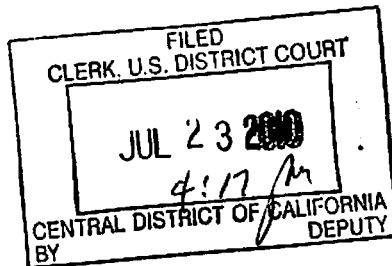


1 Joseph H. Malley  
 2 Law Office of Joseph H. Malley  
 3 1045 North Zang Blvd  
 4 Dallas, TX 75208  
 Telephone: (214) 943-6100  
 Facsimile: (214) 943-6170  
 malleylaw@gmail.com  
 5 David C. Parisi (Cal. Bar. No. 162248)  
 Parisi & Havens LLP  
 6 15233 Valleyheart Drive  
 7 Sherman Oaks, California 91403  
 Telephone: (818) 990-1299  
 8 Facsimile: (818) 501-7852  
 dparisi@parisihavens.com  
 9 Counsel for Plaintiffs



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

**CV10-05484**

12 EDWARD VALDEZ, ALAN  
 13 BONEBRAKE, BYRON GRIFFITH,  
 14 MARY HUEBNER, JOSE MARQUEZ,  
 BRITTANY SANCHEZ, GERARDO  
 15 VALDEZ, AUSTIN MUHS, and KAYLA  
 VALDEZ, Individually, on Behalf of  
 16 Themselves and Others Similarly Situated,

17 Plaintiffs,

18 v.

19 QUANTCAST CORPORATION,  
 20 MYSPACE, INC.; AMERICAN  
 BROADCASTING COMPANIES, INC.;  
 21 ESPN, INC.; HULU, LLC.; JIBJAB  
 MEDIA, INC.; MTV NETWORKS, INC.;  
 22 NBC UNIVERSAL, INC.; and SCRIBD,  
 INC.; Delaware Corporations,

23 Defendants.

CASE No.

JURY DEMAND

*60 (JCG)*

COMPLAINT FOR:

1. Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
2. Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510;
3. Violation of Video Privacy Protection Act, 18 U.S.C. § 2710;
4. Violation of California's Computer Crime Law, Penal Code § 502;
5. Violation of California's Invasion Of Privacy Act, California Penal Code § 630;
6. Violation of UCL, Bus & Prof. Code § 17200;
7. Violation of CLRA;
8. Unjust Enrichment

1 **CLASS ACTION COMPLAINT**

2 Plaintiffs, Edward Valdez, Alan Bonebrake, Byron Griffith, Mary Huebner,  
3 Jose Marquez, Brittany Sanchez, Gerardo Valdez, Austin Muhs, Kayla Valdez on  
4 behalf of themselves and all others similarly situated, by and through their  
5 attorneys, Law Office of Joseph H. Malley, P.C., and Parisi & Havens LLP, as and  
6 for their complaint, allege as follows upon information and belief, based upon,  
7 inter alia, investigation conducted by and through their attorneys, which are alleged  
8 upon knowledge, sues Defendants MySpace, Inc., Quantcast Corporation,  
9 American Broadcasting Companies, Inc., ESPN, Inc., Hulu LLC., JibJab Media,  
10 Inc., MTV Networks, Inc., NBC Universal, Inc., and Scribd, Inc. Plaintiffs’  
11 allegations as to themselves and their own actions, as set forth herein, are based  
12 upon their personal knowledge, and all other allegations are based upon  
13 information and belief pursuant to the investigations of counsel. Based upon such  
14 investigation, Plaintiffs believe that substantial evidentiary support exists for the  
15 allegations herein or that such allegations are likely to have evidentiary support  
16 after a reasonable opportunity for further investigation and/or discovery.

17 **NATURE OF THE ACTION**

18 1. Plaintiffs bring this consumer Class Action lawsuit pursuant to  
19 Federal Rules of Civil Procedure 23(a), (b)(1), (b)(2), and (b)(3), on behalf of  
20 themselves and a class of similarly situated Internet users, hereinafter referred to  
21 as the “Class Members” who were victims of unfair, deceptive, and unlawful  
22 business practices; wherein their privacy, financial interests, and computer  
23 security rights, were violated by Quantcast Corporation, (hereinafter referred to  
24 individually as “Quantcast”), and websites affiliated individually with Quantcast,  
25 referred collectively to as, “Quantcast Flash Cookie Affiliates,” and individually  
26 as: American Broadcasting Companies, Inc. (hereinafter referred to as “ABC”),  
27 ESPN, Inc. (hereinafter referred to as “ESPN”), Hulu, LLC., (hereinafter referred  
28 to as “Hulu”), JibJab Media, Inc. (hereinafter referred to as “JibJab”), MTV

1 Networks, Inc. (hereinafter referred to as “MTV”), Myspace, Inc. (hereinafter  
2 referred to as “MySpace”), NBC, Inc. (hereinafter referred to as “NBC”), and  
3 Scribd, Inc. (hereinafter referred to as “Scribd”), by setting flash cookies on their  
4 user’s computers to use as local storage within the flash media player to back up  
5 browser cookies for the purposes of restoring them later.

6 2. Quantcast Flash Cookie Affiliates acted with Quantcast, independent  
7 of one another, and knowingly authorized, directed, ratified, approved,  
8 acquiesced, or participated in the unfair and deceptive business practices made the  
9 basis of this class action, which included, but was not limited to, setting of an  
10 online tracking device which would allow access to, and disclosure of, personal  
11 information (“PI”), personal identifying information (“PII”), and/or sensitive  
12 indentifying information (“SII”). This information was derived from the Internet  
13 user’s online activities, including visits to non- Quantcast Flash Cookie Affiliates’  
14 websites, accomplished covertly, without actual notice, awareness, consent or  
15 choice of the user, obtained deceptively, for purposes not disclosed within their  
16 Terms of Service and/or Privacy Policy and used for commercial gain and  
17 nefarious purposes.

18 3. This class action does not include Quantcast affiliated corporations  
19 and websites which were not involved in setting, or allowing Quantcast to set, a  
20 flash cookie on its users’ computer hard drive to use the local storage within the  
21 user’s flash media player to back up browser cookies for the purpose of restoring  
22 them later without actual notice/awareness and consent/choice of the user.

23 4. This class action does not include Quantcast affiliated corporations  
24 and websites which provided its users adequate actual notice and awareness, that  
25 personal information would be collected, and allowed users’ choice as to how the  
26 personal information collected would be used, as it relates to information obtained  
27 by the placement of flash cookies on the users’ computer hard drive and the use of  
28 user’s local storage within their flash media player to back up browser cookies for

1 the purpose of restoring them later without actual notice/awareness and  
2 consent/choice of the user.

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

10 6. The conduct complained of includes, but is not limited to, the  
11 interception of electronic communications of Plaintiffs and Class members  
12 involving non-Quantcast Flash Cookie Affiliates, obtained in transit and  
13 temporarily stored for a limited period in their computer's electronic storage. In re  
14 Doubleclick, Inc. Privacy Litigation, 154 F. Supp.2d 497, 500 (S.D.N.Y. March  
15 28, 2001).

16 7. The conduct of Quantcast individually and in concert with the  
17 Quantcast Flash Cookie Affiliates, individually and jointly, is an unfair and  
18 deceptive practice that has been perpetrated for years, facilitated, and coordinated,  
19 by some of the world's largest websites and the network advertising industry,  
20 thereby costing the Class upwards of tens of millions of dollars. Defendants  
21 Quantcast, MySpace, ABC, ESPN, Hulu, JibJab, MTV, NBC, and Scribd  
22 (collectively) have been systematically engaged in and facilitated a covert  
23 operation of surveillance of Class members and violating one (1) or more of the  
24 following:

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

27 b. Electronic Communications Privacy Act, 18 U.S.C. § 2510 (the  
28 "ECPA"), against all Defendants;

1 c. Video Privacy Protection Act, 18 U.S.C. § 2710, (the “VPPA”)  
2 against MySpace, ABC, ESPN, HULU, JIBJAB, MTV, and NBC;

3 d. California’s Computer Crime Law, Penal Code § 502 (the  
4 “CCCL”), against all Defendants;

5 e. California’s Invasion Of Privacy Act, California Penal Code §  
6 630, against Quantcast, Myspace, Hulu, JIBJAb, and SCRIBD;

7 f. Unjust Enrichment, against all Defendants.

### 8 **JURISDICTION AND VENUE**

9 8. Venue is proper in this District under 28 U.S.C. §1391(b) and (c)  
10 against all Quantcast Flash Cookie Affiliates. A substantial portion of the events  
11 and conduct giving rise to the violations of law complained of herein occurred in  
12 this District. Defendant Hulu, LLC’s principal executive offices and headquarters  
13 are located in this District at 12312 West Olympic Boulevard, Los Angeles, CA  
14 90064; Defendant MySpace, Inc.’s principal executive offices and headquarters  
15 are located in this District at 407 N. Maple Drive, Beverly Hills, CA 90210; and  
16 Defendant JibJab, Inc.’s principal executive offices and headquarters are located  
17 in this District at 228 Main Street, Suite 4, Venice, CA 90291.

18 9. Subject matter jurisdiction exists in this Court related to this action  
19 pursuant to 28 U.S.C. § 1332. The aggregate claims of plaintiff and the proposed  
20 class members exceed the sum or value of \$5,000,000.00.

21 10. The following corporations are Delaware corporations headquartered  
22 in California. Plaintiffs assert claims on behalf of a proposed class whose  
23 members are scattered throughout the fifty states and the U.S. territories; there is  
24 minimal diversity of citizenship between proposed class members and the  
25 Defendants. The aggregate of these claims exceed the sum or value of  
26 \$5,000,000:

27 a. Quantcast;

28 b. Myspace;

- c. Hulu;
- d. JibJab;
- e. Scribd

11. This Court has personal jurisdiction over the Defendants listed in this paragraph under Cal. Code Civ. Proc. § 410.10 because each of the listed defendants maintains its corporate headquarters in, and the acts alleged herein were committed in California.

12. The following corporations are citizens of states other than California, however each of the acts upon which liability is alleged herein were committed by the corporations listed in this paragraph in the state of California:

- a. American Broadcasting Companies, Inc.
- b. ESPN, Inc.
- c. MTV Networks, Inc.
- d. NBC Universal, Inc.

13. The heart of the conduct complained of involved the communication, transmission, and interception of personally identifying information and personal private data of the class members. The mechanism to effectuate this communication, transmission and interception was devised, developed, and implemented in California.

14. This Court also has subject matter jurisdiction over all causes of action and the Defendants implicated therein pursuant to 28 U.S.C. § 1332(d), and because this action arises in part under a federal statute and this Court has jurisdiction pursuant to 18 U.S.C. § 2710(c) which confers jurisdiction in the United States District Court for actions related to the Video Privacy Protection Act.

**PARTIES**

15. Plaintiff Kayla Valdez (“K. Valdez”), is a citizen and resident of

1 Oceanside, California, (San Diego County). On information and belief, K. Valdez  
2 incorporates all allegations within this complaint. K. Valdez is a representative of  
3 the “U.S. Resident Class,” defined within the Class Allegations. At all relevant  
4 times herein, K. Valdez was an Internet user that, on one or more occasions during  
5 the class period, in the city of residence, accessed online the following named  
6 Quantcast Flash Cookie Affiliates’ websites:

- 7 a. Hulu
- 8 b. JibJab
- 9 c. MySpace

10 16. Plaintiff Jose Marquez (“Marquez”), is a citizen and resident of Rio  
11 Rancho, New Mexico, (Sandoval County). On information and belief, Marquez  
12 incorporates all allegations within this complaint. At all relevant times herein,  
13 Marquez was an Internet user that, on one or more occasions during the class  
14 period, in the city of residence, accessed online the following named Quantcast  
15 Flash Cookie Affiliates’ websites:

- 16 a. ABC
- 17 b. Hulu
- 18 c. MTV
- 19 d. NBC

20 17. Plaintiff Miriam Slater (“Slater”), is a citizen and resident of  
21 California. On information and belief, Slater incorporates all allegations within  
22 this complaint. At all relevant times herein, Slater was an Internet user that, on  
23 one or more occasions during the class period, in the city of residence, accessed  
24 certain online Quantcast Flash Cookie Affiliates’ websites. Plaintiff Edward  
25 Valdez (“E. Valdez”), is a citizen and resident of Oceanside, California, (San  
26 Diego County). On information and belief, E. Valdez incorporates all allegations  
27 within this complaint. E. Valdez is a representative of the “California Resident  
28 Class,” defined within the Class Allegations. At all relevant times herein, E.

1 Valdez was an Internet user that, on one or more occasions during the class  
 2 period, in the city of residence, accessed online the following named Quantcast  
 3 Flash Cookie Affiliates' websites:

- 4 a. MTV
- 5 b. NBC
- 6 c. Scribd

7 18. Plaintiff Gerardo Valdez ("G. Valdez"), is a citizen and resident of  
 8 Dallas, Texas, (Dallas County). On information and belief, G. Valdez incorporates  
 9 all allegations within this complaint. At all relevant times herein, G. Valdez was  
 10 an Internet user that, on one or more occasions during the class period, in the city  
 11 of residence, accessed online the following named Quantcast Flash Cookie  
 12 Affiliates' websites:

- 13 a. ESPN
- 14 b. Hulu
- 15 c. MTV

16 Cookie Name	17 Date Created/ 18 Changed	19 Size	20 Path	21 User ID	22 Domain
23 http://www.hulu.com	24 9/11/2009 9:40:16 PM	25 300	26 C:\Users\G. 27 VALDEZ\AppData\Roaming\Macromedia\Flash 28 Player\#SharedObjects\	29 2LZ 30 VE58m 31 A	32 www.hulu.com
33 BeaconServiceV2.sol	34 12/25/2009 3:59:24 PM				



1	http://www.hulu.com	9/11/2009 9:40:24 PM	72	C:\Users\G. VALDEZ\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\	2LZ VE58m	www.hulu.com
2						
3	com.quantserve.com	9/11/2009 9:40:24 PM			A	
4	e.sol					
5						
6						
7	Cookie Name	Date Created/ Changed	Size	Path	User ID	Domain
8						
9						
10	http://media.mtvnservices.com	4/19/2010 5:10:55 PM	73	C:\Documents and Settings\Owner\Application Data\Macromedia\Flash Player\#SharedObjects\	EW5 3FKS W	media.mtvnservices.com
11						
12	m	4/19/2010				
13	com.quantserve.com	5:10:55 PM				
14	e.sol					
15						
16						
17	http://media.mtvnservices.com/player/release	4/19/2010 5:10:31 PM	312	C:\Documents and Settings\Owner\Application Data\Macromedia\Flash Player\#SharedObjects\	EW5 3FKS W	media.mtvnservices.com
18						
19	m/player/release	4/19/2010				
20	se	5:27:18 PM				
21	userPrefs4.sol					
22						
23						

19. Defendant Quantcast Corporation (hereinafter “Quantcast”), is a Delaware corporation which maintains its headquarters at 201 Third St., Second Floor, San Francisco, CA 94103. Defendant Quantcast, Inc., does business throughout the United States, and in particular, does business in State of California and in this County.

1           20. Defendant MySpace, Inc. (hereinafter “MySpace”), is a Delaware  
2 corporation which maintains its headquarters at 407 N. Maple Drive, Beverly  
3 Hills, CA 90210. Defendant MySpace does business throughout the United States,  
4 and in particular, does business in State of California and in this County.

5           21. Defendant American Broadcasting Companies, Inc. (hereinafter  
6 “ABC”), is a Delaware corporation which maintains its headquarters at 47 W. 66<sup>th</sup>  
7 Street, New York, NY 10023. Defendant ABC does business throughout the  
8 United States, and in particular, does business in State of California and in this  
9 County.

10           22. Defendant ESPN, Inc. (hereinafter “ESPN”), is a Delaware  
11 corporation which maintains its headquarters at 935 Middle Street, Bristol, CT  
12 06010. Defendant ESPN does business throughout the United States, and in  
13 particular, does business in State of California and in this County.

14           23. Defendant Hulu, LLC. (hereinafter “Hulu”), is a Delaware company  
15 which maintains its headquarters at 12312 West Olympic Boulevard, Los Angeles,  
16 CA 90064. Defendant Hulu, LLC., does business throughout the United States,  
17 and in particular, does business in State of California and in this County.

18           24. Defendant JibJab Media, Inc. (hereinafter “JibJab”), is a Delaware  
19 corporation which maintains its headquarters at 228 Main Street, Suite 4, Venice,  
20 CA 90291. Defendant JibJab does business throughout the United States, and in  
21 particular, does business in State of California and in this County.

22           25. Defendant MTV Networks, Inc. (hereinafter “MTV”), is a Delaware  
23 corporation which maintains its headquarters at 1515 Broadway New York, NY  
24 10036. Defendant MTV does business throughout the United States, and in  
25 particular, does business in State of California and in this County.

26           26. Defendant NBC Universal, Inc. (hereinafter “NBC”), is a Delaware  
27 corporation which maintains its headquarters at 30 Rockefeller Plaza, New York,  
28 NY 10112. Defendant NBC does business throughout the United States, and in

1 particular, does business in State of California and in this County.

2 27. Defendant Scribd, Inc. (hereinafter “Scribd”), is a Delaware  
3 corporation which maintains its headquarters at 539 Bryant Street, San Francisco,  
4 CA 94107. Defendant NBC does business throughout the United States, and in  
5 particular, does business in State of California and in this County.

6 28. The collection of data by Defendants was wholesale and all-  
7 encompassing. Data passing from the user’s computer was observed without  
8 discrimination as to the kind, type, nature, or sensitivity of the data. Like the  
9 privacy one loses from an airport security body scanner, everything passing  
10 through the consumer’s Internet connection was intercepted by Defendants,  
11 claimed as their property, and traded as a commodity. Regardless of any  
12 representations to the contrary -- all data – whether sensitive, financial, personal,  
13 private, complete with all identifying information, was intercepted, exposing users  
14 like a “fish in a fishbowl.”

### 15 **STATEMENT OF FACTS**

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

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

25 29. This consumer class action involves a pattern of covert online  
26 surveillance. The Quantcast Flash Cookie Affiliates operated individually with  
27 Quantcast; associated in fact, targeted Internet users who visited their websites,  
28 and knowingly, without the user’s knowledge or consent,; accessed the user’s

1 computer, transmitted a program, information, code, and command, to set a  
2 tracking device within the user's flash media player. This program was set to  
3 intercept electronic communications, overriding user's security preferences, by  
4 setting a flash cookie on the user's computer hard drive to use its local storage  
5 within the flash media player to back up browser cookies for the purposes of  
6 restoring them later, if deleted by its users. This practice, also referred to as  
7 "browser cookie re-spawning," circumvented the user's intent to clear browser  
8 cookies. The objective of this scheme was the online harvesting of consumers'  
9 personal information for Defendants' use in online marketing activities. The  
10 Defendants' uniform mode of operation was as simple as it was deceptive and  
11 devious.

12 30. Quantcast Corporation is a Delaware corporation headquartered in  
13 California, and a privately owned corporation, also doing business online as  
14 "Quantserve.com;" hereinafter referred collectively to as "Quantcast," offering to  
15 advertisers and publishers a commercial access to advertise to Quantcast Flash  
16 Cookie Affiliates.

17 31. Quantcast's website, <http://www.quantcast.com>, describes its  
18 business as one that engages 220 million U.S. Internet users, providing detailed  
19 audience profiles for the advertising marketplace to learn more about what  
20 consumers are doing online. "Quantcast is currently used by 9 of the top 10 media  
21 agencies, more than half of the top publishers (by ad revenue)." While Defendant  
22 Quantcast describes itself as a media measurement and web analytics entity, in  
23 2009 Quantcast developed the "Quantcast Marketer" program which gave them  
24 "cookie access" across thousands of websites, serving billions of ad impressions  
25 daily, thus on information and belief, Quantcast has moved from simple analytics  
26 into more of a direct involvement in ad targeting.

27 32. Quantcast's "Terms of Use," dated June 17, 2009, state in part:

28 This Terms of Use Agreement (this "Agreement") describes

1 the terms and conditions on which Quantcast offers you access  
2 to the website located at [www.quantcast.com](http://www.quantcast.com).

3 33. Quantcast’s “Privacy Policy,” dated June 17, 2009, states in part:  
4 “Check the privacy policies of websites tagged with Quantcast  
5 Tags for information regarding the applicable privacy practices.

6 We use Flash cookies in connection with our Market  
7 Research Services to measure certain Flash content such as  
8 animation, games and videos.”

9 34. Quantcast Terms of Use and Privacy Policy relate only to individuals  
10 that access its website by choice, excluding any method or means involving  
11 browser hijacking, and with actual notice; thus omitting the Plaintiffs and Class  
12 members.

13 35. Quantcast does not provide the identity of all associated websites, nor  
14 do the Quantcast Flash Cookie Affiliate websites stipulate the Quantcast  
15 association.

16 36. MySpace, Inc. is a Delaware corporation, headquartered in  
17 California, and a privately owned corporation, hereinafter referred to as  
18 “MySpace,” offered as an Internet social networking platform that allows users to  
19 create unique personal profiles online.

20 37. MySpace’s website, <http://www.myspace.com>, describes its business  
21 as a “technology company connecting people through personal expression,  
22 content, and culture. MySpace empowers its global community to experience the  
23 Internet through a social lens by integrating personal profiles, photos, videos,  
24 mobile, messaging, games, and the world’s largest music community.”

25 38. MySpace conducts business, in part, as a “video tape service  
26 provider,” engaged in business, in or affecting interstate of rental, sale, and or  
27 delivery of prerecorded audio video materials.

28 39. MySpace’s “Terms of Use Agreement,” dated June 25, 2009, states

1 in part:

2 The following are examples of the kind of activity that is illegal  
3 or prohibited on the MySpace Website and through your use of  
4 the MySpace Services.

- 5 – activity that involves the use of viruses, bots, worms, or  
6 any other computer code, files or programs that interrupt,  
7 destroy or limit the functionality of any computer  
8 software or hardware, or otherwise permit the  
9 unauthorized use of or access to a computer or a  
10 computer network;
- 11 – providing or using “tracking” or monitoring functionality  
12 in connection with the MySpace Services, including,  
13 without limitation, to identify other Users’ views, actions  
14 or other activities on the MySpace Services.

- 15 40. MySpace’s “Privacy Policy,” dated February 28, 2008, states in part:  
16 “MySpace uses cookies to identify your Internet browser, store  
17 Users’ preferences, and determine whether you have installed  
18 the enabling software needed to access certain material on the  
19 MySpace Services. Data in cookies may be read to authenticate  
20 user sessions or provide services.

21 Third party advertisements displayed on MySpace  
22 Services may also contain cookies set by Internet advertising  
23 companies or advertisers (known as “third party  
24 cookies”). MySpace does not control these third party cookies  
25 and Users of the MySpace Services should check the privacy  
26 policy of the Internet advertising company or advertiser to see  
27 whether and how it uses cookies.

28 Some of the advertisements that appear on MySpace

1 Services may also be delivered to you by third party Internet  
2 advertising companies. These companies utilize certain  
3 technologies to deliver advertisements and marketing messages  
4 and to collect non-PII about your visit to or use of MySpace  
5 Services, including information about the ads they display, via a  
6 cookie placed on your computer that reads your IP address. To  
7 opt out of information collection by these companies, or to  
8 obtain information about the technologies they use or their own  
9 privacy policies, please [click here](#).”

10 41. MySpace’s Terms of Use Agreement forbids users from committing  
11 the same acts, made the basis of this action, against its computer network as was  
12 committed against the users’ computer.

13 42. MySpace does not provide the identity of all associated advertising  
14 networks nor all purposes for its involvement.

15 43. MySpace’s Privacy Policy fails to reference that flash cookies shall  
16 be used as a tracking mechanism, thus negating the possibility of a user’s privacy  
17 self help.

18 44. American Broadcasting Companies, Inc. is a Delaware corporation,  
19 headquartered in New York, and a privately owned corporation, hereinafter  
20 referred to as “ABC,” offered as an Internet website to provide consumers full-  
21 length television episodes of its shows.

22 45. ABC’s website, <http://www.abc.com>, describes its business as a  
23 provider of “information on ABC daytime and primetime network programming.  
24 Watch full episodes of your favorite ABC shows and browse exclusive online  
25 content.”

26 46. ABC conducts business, in part, as a “video tape service provider,”  
27 engaged in business, in or affecting interstate of rental, sale, and or delivery of  
28 prerecorded audio video materials.

1 47. ABC's "Terms of Service," dated May 6, 2008, states in part:  
2 The following Rules of Conduct apply to the WDIG Sites. By  
3 using the WDIG Sites, you agree that you will not Distribute  
4 any Submission that:

- 5 – is defamatory, abusive, harassing, threatening, or an  
6 invasion of a right of privacy of another person;'
- 7 – infringes or violates any right of a third party including:  
8 . . (b) right of privacy (specifically, you must not  
9 distribute another person's personal information of any  
10 kind without their express permission) or publicity;'

11 You agree that any action at law or in equity arising out  
12 of or relating to these terms of use or the WDIG Sites shall be  
13 filed, and that venue properly lies, only in state or federal courts  
14 located in the borough of Manhattan, New York, New York..

15 48. ABC's "Privacy Policy," dated August 8, 2007, states in part:  
16 "As used in this Privacy Policy, "The Walt Disney Family of  
17 Companies" refers to The Walt Disney Company and its  
18 subsidiary and affiliated entities, singly or together, including  
19 companies such as ABC and ESPN that generally do not offer  
20 their products and services under the "Disney" brand name, as  
21 well as companies that generally do offer their products and  
22 services under the "Disney" brand name. The Walt Disney  
23 Internet Group (including its subsidiaries) is a member of The  
24 Walt Disney Family of Companies, and is referred to in this  
25 Privacy Policy as "WDIG."

26 This information may include the guest's name, postal  
27 address, e-mail address and telephone number. We also may  
28 collect other types of information such as gender, age, number



1 of children, and personal interests, which we may associate  
2 with personal information.

3 Our Web sites collect information through a variety of  
4 technical methods, including cookies and Web beacons.

5 Cookies, web beacons and other technical methods may  
6 involve the transmission of information either directly to us or  
7 to another party authorized by us to collect information on our  
8 behalf.

9 These technical methods may enable us to collect and use  
10 information in a form that is personally identifiable.

11 Many advertisements are managed and placed on our  
12 Web sites by third parties. These companies are called "network  
13 advertisers." Network advertisers who place advertisements on  
14 our Web sites may use cookies and Web beacons to collect non-  
15 personally identifiable information about your visits to our Web  
16 sites and other Web sites in order to provide advertisements  
17 about goods and services of interest to you.”

18 49. ABC’s Terms of Service forbid users from committing the same acts,  
19 made the basis of this action, against its computer network as was committed  
20 against the users’ computer.

21 50. ABC does not provide the identity of all associated advertising  
22 networks nor all purposes for its involvement.

23 51. ABC’s Privacy Policy fails to reference that flash cookies shall be  
24 used as a tracking mechanism, thus negating the possibility of a user’s privacy self  
25 help.

26 52. ESPN, Inc. is a Delaware corporation, headquartered in Connecticut,  
27 and a privately owned corporation, hereinafter referred to as “ESPN,” which is a  
28 cable television network that offers an Internet website dedicated to broadcasting

1 and producing sports-related content.

2 53. ESPN's website, <http://www.espn.com>, describes its business as the  
3 "leading provider of sports on the Internet. ESPN.com provides its users, [] with  
4 late breaking news, statistics, schedules, and player updates, in addition to up-to-  
5 the minute sports scores from live events."

6 54. ESPN conducts business, in part, as a "video tape service provider,"  
7 engaged in business, in or affecting interstate of rental, sale, and or delivery of  
8 prerecorded audio video materials.

9 55. ESPN's "Terms of Service," dated May 6, 2008, states in part:

10 "The following Rules of Conduct apply to the WDIG Sites. By  
11 using the WDIG Sites, you agree that you will not Distribute  
12 any Submission that: i

13 – is defamatory, abusive, harassing, threatening, or an  
14 invasion of a right of privacy of another person;'

15 – infringes or violates any right of a third party including:

16 ... b) right of privacy (specifically, you must not

17 distribute another person's personal information of any

18 kind without their express permission) or publicity;'

19 You agree that any action at law or in equity arising out of or relating  
20 to these terms of use or the WDIG Sites shall be filed, and that venue  
21 properly lies, only in state or federal courts located in the borough of  
22 Manhattan, New York, New York.."

23 56. ESPN's "Privacy Policy," dated August 8, 2007, states in part:

24 "As used in this Privacy Policy, "The Walt Disney Family of

25 Companies" refers to The Walt Disney Company and its

26 subsidiary and affiliated entities, singly or together, including

27 companies such as ABC and ESPN that generally do not offer

28 their products and services under the "Disney" brand name, as

1 well as companies that generally do offer their products and  
2 services under the "Disney" brand name. The Walt Disney  
3 Internet Group (including its subsidiaries) is a member of The  
4 Walt Disney Family of Companies, and is referred to in this  
5 Privacy Policy as "WDIG.."

6 This information may include the guest's name, postal  
7 address, e-mail address and telephone number. We also may  
8 collect other types of information such as gender, age, number  
9 of children, and personal interests, which we may associate  
10 with personal information.

11 Our Web sites collect information through a variety of technical  
12 methods, including cookies and Web beacons.

13 Cookies, web beacons and other technical methods may involve the  
14 transmission of information either directly to us or to another party  
15 authorized by us to collect information on our behalf.

16 These technical methods may enable us to collect and use information  
17 in a form that is personally identifiable.

18 Many advertisements are managed and placed on our Web sites by  
19 third parties. These companies are called "network advertisers."

20 Network advertisers who place advertisements on our Web sites may  
21 use cookies and Web beacons to collect non-personally identifiable  
22 information about your visits to our Web sites and other Web sites in  
23 order to provide advertisements about goods and services of interest to  
24 you."

25 57. ESPN's Terms of Service forbids users from committing the same  
26 acts, made the basis of this action, against its computer network as was committed  
27 against the users' computer.

28 58. ESPN does not provide the identity of all associated advertising

1 networks nor all purposes for its involvement.

2 59. ESPN's Privacy Policy fails to reference that flash cookies shall be  
3 used as a tracking mechanism, thus negating the possibility of a user's privacy self  
4 help.

5 60. Hulu, LLC is a Delaware company, headquartered in California, and  
6 a privately owned corporation, hereinafter referred to as "Hulu," offering to  
7 consumers commercial-supported streaming video of TV shows and movies from  
8 NBC, Fox, ABC, and many other networks and studios.

9 61. Hulu's website, <http://www.hulu.com>, describes its business as an  
10 online video service that offers hit TV shows, movies and clips at hulu.com and  
11 other online destination sites — anytime in the U.S. Hulu allows users to enjoy  
12 great videos on hulu.com and on 35 other popular Web sites across the Web.

13 62. Hulu conducts business, in part, as a "video tape service provider,"  
14 engaged in business, in or affecting interstate of rental, sale, and or delivery of  
15 prerecorded audio video materials.

16 63. Hulu's "Terms of Service," dated June 26, 2009, states in part:

17 You will not access the Hulu Site or use the Hulu Services in a  
18 way that:

- 19 – uses technology or other means to access, index, frame or link  
20 to the Content or the Hulu Services that is not authorized by  
21 Hulu (including by removing, disabling, bypassing, or  
22 circumventing any content protection or access control  
23 mechanisms intended to prevent the unauthorized download,  
24 stream capture, linking, framing, reproduction, access to or  
25 distribution of the Content or Hulu Services);  
26 – involves accessing the Hulu Services through any automated  
27 means, including "robots," "spiders," or "offline readers"  
28 (other than by individually performed searches on publicly

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

accessible search engines for the sole purpose of, and solely to the extent necessary for, creating publicly available search indices — but not caches or archives — of the Hulu Services and excluding those search engines or indices that host, promote, or link primarily to infringing or unauthorized content);

– introduces viruses or any other computer code, files, or programs that interrupt, destroy, or limit the functionality of any computer software or hardware or telecommunications equipment”

64. Hulu’s “Privacy Policy,” dated June 26, 2009, states in part: “Some of the advertisements that appear in connection with the Hulu Services may be delivered to you by third party Internet advertising companies (also called "ad networks" or "network advertisers"). These companies may use cookies, web beacons and other technologies to collect non-personally identifiable information about your visits to the Hulu Site in order to deliver advertisements to you, measure their effectiveness, and personalize advertising content. Hulu does not have access to or control over cookies, web beacons or other technologies that they may use.”

65. Hulu’s Terms of Service forbids users from committing the same acts, made the basis of this action, against its computer network as was committed against the users’ computer.

66. Hulu does not provide the identity of all associated advertising networks nor all purposes for its involvement.

67. Hulu’s Privacy Policy fails to reference that flash cookies shall be used as a tracking mechanism, thus negating the possibility of a user’s privacy self help.

1           68.     JibJab Media, Inc. is a Delaware corporation, headquartered in  
2 California, and a privately owned corporation, hereinafter referred to as “JibJab,”  
3 offering to consumers flash animated videos, cartoons, movies, pictures and jokes  
4 among other. Users may upload different kind of videos.

5           69.     JibJab’s website, <http://www.jibjab.com>, describes its business as a  
6 corporation that “creates, produces and distributes entertainment content, [] audio,  
7 visual, audiovisual, text., offers users the opportunity to participate in community  
8 media applications by submitting...”

9           70.     JibJab conducts business, in part, as a “video tape service provider,”  
10 engaged in business, in or affecting interstate of rental, sale, and or delivery of  
11 prerecorded audio video materials.

12           71.     JibJab’s “Terms of Service,” dated May 27, 2009, states in part:

13           User agrees not to:

14           – interfere with or damage any of the JibJab Sites or JibJab  
15           Services, including, without limitation, through the use of  
16           viruses, cancel bots, Trojan horses, harmful code..’

17           – collect or store any information about any other user other  
18           than in the course of the permitted use of the JibJab Sites and  
19           JibJab Services..’

20           – sell or otherwise transfer any User information..’

21           THE SOLE VENUE AND JURISDICTION FOR DISPUTES  
22           ARISING FROM THIS AGREEMENT SHALL BE THE  
23           APPROPRIATE STATE OR FEDERAL COURT LOCATED  
24           IN THE LOS ANGELES COUNTY, CALIFORNIA, AND  
25           USER AND JIBJAB BOTH IRREVOCABLY AGREE TO  
26           SUBMIT TO THE JURISDICTION OF SUCH COURTS.

27           72.     JibJab’s “Privacy Policy,” dated May 27, 2009, states in part:

28           JibJab collects user submitted information such as name, email

1 address, and age.. JibJab may also collect[sic] other data either  
2 directly or via third-party sign-on services...

3 JibJab uses cookies to store user preferences, account  
4 status, traffic origination, and to record session information, for  
5 purposes including ensuring that users are not repeatedly  
6 offered the same advertisements and to customize newsletter,  
7 advertising, and Web page content based on browser type and  
8 user profile information.

9 JibJab allows 3rd party advertisers that are presenting  
10 advertisements on some of our pages to set and access their  
11 cookies on your computer. Advertisers' use of cookies is subject  
12 to their own privacy policies, not the JibJab Privacy Policy.

13 Our Web advertising partners may set cookies.

14 73. JibJab's Terms of Service forbids users from committing the same  
15 acts, made the basis of this action, against its computer network as was committed  
16 against the users' computer.

17 74. JibJab does not provide the identity of all associated advertising  
18 networks nor all purposes for its involvement.

19 75. JibJab's Privacy Policy fails to reference that flash cookies shall be  
20 used as a tracking mechanism, thus negating the possibility of a user's privacy self  
21 help.

22 76. MTV Networks, Inc. is a Delaware corporation, headquartered in  
23 New York, and a privately owned corporation, hereinafter referred to as "MTV,"  
24 offered as an Internet website in cooperation with the MTV television channel and  
25 programming service.

26 77. MTV's website, <http://www.mtv.com>, describes its business as an  
27 online video service, "And get this: we've got the actual videos -- not just snips,  
28 clips or blips, not just sneak peeks. We're talking full-on, start-to-finish music

1 videos...”

2 78. MTV conducts business, in part, as a “video tape service provider,”  
3 engaged in business, in or affecting interstate of rental, sale, and or delivery of  
4 prerecorded audio video materials.

5 79. MTV’s “Terms of Service,” dated October 19, 2009, states in part:

6 Rules Of Conduct

7 You shall not use, allow, or enable others to use the Site, or  
8 knowingly condone use of this Site by others, in any manner that is,  
9 attempts to, or is likely to:

- 10 – transmit, distribute or upload programs or material that contain  
11 malicious code, such as viruses, timebombs, cancelbots, worms,  
12 trojan horses, spyware, or other potentially harmful programs or  
13 other material or information;  
14 – collect, obtain, compile, gather, transmit, reproduce, delete, revise,  
15 view or display any material or information, whether personally  
16 identifiable or not, posted by or concerning any other person, firm  
17 or enterprise, in connection with their or your use of the Site, unless  
18 you have obtained the express, prior permission of such other  
19 person, firm or enterprise to do so.

20 80. MTV’s “Privacy Policy,” dated October 19, 2009, states in part:

21 Information Collected Through Use of Cookies and Other  
22 Tracking Technologies. The Site and/or third parties may use  
23 “cookies”, “web beacons” (also known as image tags, GIF or  
24 web bugs), "embedded scripts" and other similar tracking  
25 technologies (collectively, “Tracking Technologies”) to collect  
26 Other Information automatically as you browse the Site and the  
27 web.

28 This Site may additionally use a variety of third party



1 advertising networks, data exchanges, traffic measurement  
2 service providers, marketing analytics service providers and  
3 other third parties (collectively, “Third Party Advertising  
4 Service Providers”) to, for example, serve advertisements on  
5 the Site, facilitate targeting of advertisements and/or measure  
6 and analyze advertising effectiveness and/or traffic on the Site  
7 (“Targeting Services”).

8 Although these Third Party Advertising Service  
9 Providers do not have access to Tracking Technologies set by  
10 the Site, the Third Party Advertising Service Providers, as well  
11 as Advertisers, may themselves set and access their own  
12 Tracking Technologies on your Device if you choose to have  
13 Tracking Technologies enabled in your browser and/or they  
14 may otherwise have access to Other Information about you.

15 The use of Tracking Technologies by Third Party  
16 Advertising Service Providers and Advertisers is within their  
17 control and not ours. Even if we have a relationship with the  
18 Third Party Advertising Service Provider or Advertiser, we do  
19 not control their websites or their policies and practices  
20 regarding your Information.

21 Opting-Out of Use of Certain Other Information  
22 Collected by Tracking Technologies. With respect to the  
23 Tracking Technologies set by Third Party Advertising Service  
24 Providers and Advertisers, you have a number of options:

25 You can choose to delete the Tracking Technologies  
26 through the "Internet Options" sub-option of the "Tools"  
27 menu option of your browser or otherwise as directed by  
28 your browser’s support feature.”

1 81. MTV's Terms of Service forbids users from committing the same  
2 acts, made the basis of this action, against its computer network as was committed  
3 against the users' computer.

4 82. MTV does not provide the identity of all associated advertising  
5 networks nor all purposes for its involvement.

6 83. MTV's Privacy Policy fails to reference that flash cookies shall be  
7 used as a tracking mechanism, thus negating the possibility of a user's privacy self  
8 help.

9 84. NBC Universal, Inc. is a Delaware corporation, headquartered in  
10 New York, and a privately owned corporation, hereinafter referred to as "NBC,"  
11 offering to consumers television networks, cable channels, local stations, and  
12 motion pictures.

13 85. NBC's website, <http://www.nbc.com>, describes its business as a  
14 "leading media and entertainment company[] in the development, production and  
15 marketing of entertainment, news, and information to a global audience."

16 86. NBC conducts business, in part, as a "video tape service provider,"  
17 engaged in business, in or affecting interstate of rental, sale, and or delivery of  
18 prerecorded audio video materials.

19 87. NBC's "Terms of Service," dated September 28, 2001, states in part:

20 It is a condition of your use of the Service that you do not:

21 ...post or transmit any information, software or other material that is  
22 fraudulent or violates or infringes the rights of others, including  
23 material that violates privacy.."

24 88. NBC's "Privacy Policy," dated August 14, 2007, states in part:

25 Use of Cookies and Similar Technologies: Like many sites, we  
26 use "cookies" or other similar technologies to collect AA  
27 [aggregate and anonymous] Data.

28 For more information about these specialized cookies and

1 other technologies, and how to "opt out" of information  
2 collection by these companies, we suggest you visit  
3 [http://doubleclick.net/privacy\\_policy](http://doubleclick.net/privacy_policy) or  
4 [http://networkadvertising.org/optout\\_nonppii.asp](http://networkadvertising.org/optout_nonppii.asp).

5 89. NBC's Terms of Service forbids users from committing the same  
6 acts, made the basis of this action, against its computer network as was committed  
7 against the users' computer.

8 90. NBC does not provide the identity of all associated advertising  
9 networks nor all purposes for its involvement.

10 91. NBC's Privacy Policy fails to reference that flash cookies shall be  
11 used as a tracking mechanism, thus negating the possibility of a user's privacy self  
12 help.

13 92. Scribd, Inc. is a Delaware corporation, headquartered in California,  
14 and a privately owned corporation, hereinafter referred to as "Scribd," offering to  
15 consumers a document-sharing website which allows users to post documents in  
16 various formats and embed them into a web page.

17 93. Scribd's website, <http://www.scribd.com>, describes its business as  
18 "the largest social publishing and reading site in the world. [] for anyone to share  
19 and discover informative, entertaining and original written content on the web and  
20 mobile devices."

21 94. Scribd's "Terms of Use," dated January 12, 2010, states in part:  
22 Prohibited Conduct.

23 BY USING THE SCRIBD PLATFORM YOU AGREE NOT TO:

- 24 – ...collect, or attempt to collect, personal information about Users or  
25 third parties without their consent;'  
26 – ... use any robot, spider, scraper, or other automated means to access  
27 the Scribd Platform for any purpose...'  
28 – 'These Terms will be governed by and construed in accordance with

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 laws of the State of California, without giving effect to any principles of conflicts of law.’

– You agree that any action at law or in equity arising out of or relating to these Terms or Scribd will be filed only in the state or federal courts in and for Santa Clara County, California..”

95. Scribd’s “Privacy Policy,” dated May 19, 2009, states in part: Scribd may use both session cookies and persistent cookies. A session cookie disappears after you close your browser.

When you access the Scribd Platform or open one of our HTML emails, we may automatically record certain information from your system by using different types of tracking technology.

Scribd does not share your personally identifiable information with other organizations for their marketing or promotional uses without your prior express consent.

We may disclose User information to affiliated companies..”

96. Scribd’s Terms of Use forbids users from committing the same acts, made the basis of this action, against its computer network as was committed against the users’ computer.

97. Scribd does not provide the identity of all associated advertising networks nor all purposes for its involvement.

98. Scribd’s Privacy Policy fails to reference that flash cookies shall be used as a tracking mechanism, thus negating the possibility of a user’s privacy self help.

99. Defendants Quantcast Flash Cookie Affiliates’ privacy documents omit entirely the actual identity of its association with Quantcast, limiting the user’s awareness of, and an inability to determine accurately, the involvement of Quantcast, or locate the Quantcast website, compounded further by Quantcast

1 defining its business as a media measurement and web analytics company while  
2 the Quantcast Flash Cookie Affiliates' privacy documents refer only to  
3 associations involving advertising networks.

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

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

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

22 103. Defendants Quantcast Flash Cookie Affiliate users are unable to  
23 identify the corporate families to which these Defendant websites belong, which  
24 makes it difficult for a user to discover exactly who such associated entities are,  
25 thus their practices are deceptive. A practice is deceptive for purposes of the  
26 Federal Trade Commission Act if it involves a —material representation,  
27 omission or practice that is likely to mislead a consumer acting reasonably in the  
28 circumstances, to the consumer's detriment [FTC 1983]. The conflicting

1 statements in the privacy policies would most likely confuse or mislead a  
2 reasonable consumer. The confusion would also likely be to their detriment, as  
3 surveys indicate that users do not want companies to collect data about them  
4 without permission.

5 104. Defendants Quantcast Flash Cookie Affiliates' privacy documents  
6 discuss that the data collection practices of entities associated with their  
7 corporation are outside the coverage of the privacy policy. This appears to be an  
8 attempt to create a critical loophole used by Defendant Quantcast Flash Cookie  
9 Affiliates compounding their attempts to violate the privacy protection of their  
10 users.

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

20 106. Defendant Quantcast's privacy documents referenced the use of flash  
21 cookies, but states such is used only for audience measurement and not behavioral  
22 ad targeting. The opt-out is inconspicuous on their privacy page and appears in a  
23 small font header in the corner of the page.

24 107. Defendant Quantcast's privacy documents do not expressly state that  
25 if a Quantcast Flash Cookie Affiliate user opts-out that behavioral information  
26 will not be collected and shared but only that the Quantcast Flash Cookie Affiliate  
27 user will not receive Internet based advertising content from its "advertising  
28 delivery service;" moreover its opt-out "unique cookie value" includes identifying

1 information which means the cookie is no longer non-unique.

2 108. Defendants' privacy documents provide a false privacy protection by  
3 implying some level of protection for the user. Defendants' privacy documents  
4 intentionally are sufficiently vague so as to refrain from fully disclosing  
5 information to its users about what information is collected by the website, its  
6 associated entities, how the information is used and the purposes for the collection  
7 and use of this information; negating that its users are provided informed and  
8 meaningful online consent to these practices. Without adequate notice the  
9 potential privacy dangers are not apparent to most users, leaving them unable to  
10 exercise control over their personal information even if meaningful choice  
11 mechanisms are available.

12 109. Defendants' privacy documents require college level reading skills  
13 for comprehension. They include substantial legalese, ambiguous and obfuscated  
14 language, and are designed to confuse, disenfranchise, and mislead the users.

15 110. Defendants' privacy documents incorporate a multitude of hedging  
16 and modality markers so as to obscure their use of covert surveillance technology  
17 and data-gathering tools. They send mixed messages related to privacy controls,  
18 advising users that to exercise privacy controls would diminish or disable website.  
19 At the same time, Defendants claim that all cookies are very small and  
20 unobtrusive and pose no threat since "many websites use them."

21 111. Defendants' privacy documents fail to provide an adequate notice  
22 and choice regime, predicated on user choice, and informed by privacy policies.  
23 Defendants' privacy documents provided nuanced situations that created  
24 conditional yes or no answers to basic questions about a site's data collection and  
25 sharing practices, thus it was unclear how an average user could ever understand  
26 these practices. Choice, therefore, cannot be inferred. A notice and choice regime  
27 is favored by the FTC.

28 A U.S. Federal Trade Commission representative delivered a

1 stern indictment of current privacy laws on Monday, saying  
2 they fail to protect American consumers and instead place too  
3 much of a "burden" on them.

4 "We've put too much burden on the consumers to  
5 understand these policies."

6 "To compare the privacy policies of two companies is an  
7 almost impossible task."

8 "[T]he current 'notice and choice' model in some very  
9 basic sense isn't working ...."

10 "The goal of transparency clearly isn't being met by the  
11 way notice is being handled today."

12 McCullagh, Declan. "FTC says current privacy laws aren't working." CNET. (June  
13 22, 2010) [http://news.cnet.com/8301-13578\\_3-20008422-38.html](http://news.cnet.com/8301-13578_3-20008422-38.html)

14 112. Defendants' privacy documents fail to provide notice that they  
15 improperly collect, maintain, and disclose personal information from children  
16 under the age of 13, without parent's consent, in violation of the Children's  
17 Online Privacy Protection Act ("COPPA") by its activities made the basis of this  
18 action.

19 113. Defendants' privacy documents fail to provide notice that their data  
20 storage practices, as they relate to the term user data is stored, has no term period  
21 and is indefinite.

22 114. Defendants' privacy documents carefully attempt to parse the  
23 definitions of phrases related to their tracking activity. Their privacy documents  
24 are more nuanced than such categorized analysis allows for, omitting any direct  
25 reference to flash cookies, embedding surveillance technology into the user's  
26 computer hardware, use of user's computer hardware to store data, use of  
27 technology to allow the perpetual online tracking and surveillance of any and all  
28 online Internet activity of the Quantcast Flash Cookie Affiliate user. They also



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

8 115. Defendants’ privacy document verbiage was deceptive by design.  
 9 This deception is especially troubling when compared with the obligation imposed  
 10 upon their online visitors to download, read, and comprehend the vast amount of  
 11 documents required to protect one’s online privacy, complicated by the  
 12 cumulative effect of such task. This is accentuated by an analysis of MTV’s  
 13 privacy documents:

14 Quantcast Flash Cookie Affiliate MTV’s Privacy Documents:

15 Document:	Word Count:	Hard	Copy
16 Count			
17 Privacy Policy	11,739	18	
18 Terms of Use	12,047	16	
19 Copyright Compliance Policy	1,483	3	
20 Community Guidelines	481	1	
21 User Content Submission Agreement	6,307	8	
22 Social Project Privacy Policy	5,471	9	
23 Social Project Terms of Use	6,347	10	
24 TOTAL:	43,875	65	

25 116. In addition to downloading, reading and comprehending all of the  
 26 MTV privacy documents, its users would be required to locate the website for  
 27 Quantcast and repeat this obligation for Quantcast’s privacy documents. To  
 28 accentuate the improbability of completing this task though, Quantcast Flash

1 Cookie Affiliate website visitors were not provided any information of the identity  
 2 of Quantcast within MTV, nor any of the Quantcast Flash Cookie Affiliates’,  
 3 Terms of Service and Privacy Policy. For sake of analysis, the Quantcast Flash  
 4 Cookie Affiliate website visitors’ obligation would involve the following:

5 Quantcast Privacy Documents:

6 Document:	Word Count:	Hard Copy Count
7 Privacy Policy	2,392 4	
8 Terms of Use	2,702 5	
9 TOTAL:	5,094 9	

10 117. In addition to the MTV and Quantcast privacy documents, a user  
 11 would be obligated to review their flash media player’s privacy documents. Some  
 12 Internet users possess multiple flash media players, and many are not aware of the  
 13 identity of their flash media player nor are provided information from Defendants  
 14 as to the identity of the flash media player being apprehended for use by the  
 15 Quantcast Flash Cookie Affiliate and/or Quantcast. If a user could identify their  
 16 involved flash media player, and the identity of the corporate entity for the flash  
 17 media player, the user would have additional obligations imposed upon them to  
 18 download, read, and comprehend the flash media player’s privacy documents,  
 19 such as Adobe’s, the largest flash media player provider:

20 Adobe’s Flash Media Player Privacy Documents:

21 Document:	Word Count:	Hard	Copy
22 Count			
23 Privacy Policy	3,572	6	
24 Terms of Use	4,691	10	
25 Flash Player Help	100	1	
26 Settings Manager	1,891	4	
27 Global Privacy Settings Panel	243	1	
28 Global Storage Settings Panel	629	2	

1	Global Security Settings Panel	1,280	3
2	Global Notifications Settings Panel	114	1
3	Website Privacy Settings Panel	290	1
4	Website Storage Settings Panel	727	2
5	Display Settings	259	2
6	Local Storage Settings	1,159	3
7	Microphone Settings	370	2
8	Camera Settings	298	2
9	Privacy Settings	787	2
10	Local Storage Pop-Up Question	1,030	3
11	Privacy Pop-Up Question	648	2
12	Security Pop-up Question	823	2
13	About Updating Flash Player	749	2
14	TOTAL:	19,660	51

15 118. Quantcast Flash Cookie Affiliates’ users’ online privacy protection  
16 was premised upon imposed requirement to download, read and comprehend the  
17 accumulation of all privacy documents of Quantcast Flash Cookie Affiliate,  
18 Quantcast, and the user’s flash media player, such as Adobe, noting for analysis  
19 and emphasis, the following:

20 Defendants’ Collective Privacy Documents:

21 Document:	Word Count:	Hard	Copy
22 Count			
23 MTV- Privacy Policy	11,739		18
24 MTV- Terms of Use	12,047		16
25 MTV- Copyright Compliance Policy	1,483		3
26 MTV- Community Guidelines	481		1
27 MTV- User Content Submission Agreement	6,307		8
28 MTV- Social Project Privacy Policy	5,471		9

1	MTV- Social Project Terms of Use	6,347	10
2	Quantcast- Privacy Policy	2,392	4
3	Quantcast- Terms of Use	2,702	5
4	Adobe- Privacy Policy	3,572	6
5			
6	Adobe- Terms of Use	4,691	10
7	Adobe- Flash Player Help	100	1
8	Adobe- Settings Manager	1,891	4
9	Adobe- Global Privacy Settings Panel	243	1
10	Adobe- Global Storage Settings Panel	629	2
11	Adobe- Global Security Settings Panel	1,280	3
12	Adobe- Global Notifications Settings Panel	114	1
13	Adobe- Website Privacy Settings Panel	290	1
14	Adobe- Website Storage Settings Panel	727	2
15	Adobe- Display Settings	259	2
16	Adobe- Local Storage Settings	1,159	3
17	Adobe- Microphone Settings	370	2
18	Adobe- Camera Settings	298	2
19	Adobe- Privacy Settings	787	2
20	Adobe- Local Storage Pop-Up Question	1,030	3
21	Adobe- Privacy Pop-Up Question	648	2
22	Adobe- Security Pop-up Question	823	2
23	Adobe- About Updating Flash Player	749	2

	<b>TOTAL:</b>	<b>68,629</b>	<b>125</b>
--	---------------	---------------	------------

27 119. A millisecond was the time allotted to an online visitor opening a  
28 Quantcast Flash Cookie Affiliates' webpage, before a flash cookie was embedded

1 within their computer and data collected immediately, without their awareness,  
2 knowledge or consent to such actions. Such occurred without the benefit of being  
3 provided adequate time to access, read, and attempt to comprehend the Terms of  
4 Service/Use and Privacy Policy for Quantcast Flash Cookie Affiliates’ website,  
5 Quantcast’s, and the website of the user’s flash media player. While only the most  
6 technically savvy online users were familiar with cookies, a finite amount of  
7 individuals even knew about flash cookies, let alone could possibly comprehend  
8 the technical aspects of flash cookies inherent within the 68,629 words and 125  
9 hard copy pages.

10 120. To put matters in perspective, a Herculean task would be required,  
11 and equate in word count to reading, in a millisecond, either the United States  
12 Constitution eleven (11) times, Plaintiffs’ complaint twice (based on 35,765  
13 words), one (1) of the following novels: The Great Gatsby by F. Scott Fitzgerald;  
14 The Catcher in the Rye by J. D. Salinger; The Adventures of Tom Sawyer by  
15 Mark Twain; Of Mice and Men by John Steinbeck, or your choice between one  
16 (1) of George Orwell’s novels Animal Farm, or more appropriately, Nineteen  
17 Eighty-Four:

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

26 A. Traditional Online Advertising

27 “Contrary to what many marketers claim, most adult Americans  
28 (66%) do not want marketers to tailor advertisements to their interests.

1           Moreover, when Americans are informed of three common ways that  
2           marketers gather data about people in order to tailor ads, even higher  
3           percentages - between 73% and 86% - say they would not want such  
4           advertising.”

5           Turow, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy  
6           and Hennessy, Michael, Americans Reject Tailored Advertising and  
7           Three Activities that Enable It (September 29, 2009).

8           <http://ssrn.com/abstract=1478214>

9           121. Although a comprehensive description of the online advertising  
10          industry is unnecessary to address the allegations raised in this complaint, a  
11          rudimentary grasp of traditional online advertising, the Internet’s architecture, and  
12          browser engineering is important.

13          122. Originally advertising on websites evolved based upon the business  
14          model used by the newspaper industry, in that they relied on traditional  
15          advertising in order to provide content to their subscribers at a reduced rate for the  
16          cost of the content. Subscribers would read the content and advertisers hoped their  
17          ad would attract the reader.

18          123. Commercial websites, such as Quantcast Flash Cookie Affiliates  
19          MySpace, ABC, ESPN, Hulu, JibJab, MTV, NBC, and Scribd, use online  
20          advertising in order to promote content to the consumers without charge and  
21          require online advertising to support this objective. Commercial websites, known  
22          as “publishers” allow portions of their web page to be sold to online advertising  
23          networks, which act as an intermediary between “publishers” and the  
24          “advertisers.”

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

1 by a media service.

2 125. Web advertisements provided by “third-party ad servers” inject their  
3 advertisements into hosting web pages. The web page upon which an  
4 advertisement will appear reserves a blank space in the page's layout with a URL  
5 containing a third-party advertising server address. Whenever that page is  
6 displayed, the user's web browser will read the page, discover the URL address of  
7 the advertising server, and request a web page asset from it. This could be an  
8 image, flash animation, video, or other resource from the third-party server. When  
9 the advertising asset is received by the browser, it will be inserted into the page to  
10 appear in the reserved location and become part of the delivered page.

11 126. Publishers desiring to identify and track users while they were on  
12 their site; embed “first party” tracking devices, “session cookies,” used to  
13 facilitate a user’s activities within the selected website while actively on that site,  
14 and “persistent cookies,” which exist beyond the period of the initial website  
15 session and provides tracking technology while a users visits all websites.

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

25 128. Online advertising companies created a network of publishers linked  
26 by a common ad server. Third-party cookies feed into the clickstream data of the  
27 consumer by the publisher and/or advertising network providing the ability to  
28 monitor the consumer’s online activity.

1           129. Defendants Quantcast’s involvement in the network advertising  
2 industry relates in whole, or part, to media measurement and web analytics,  
3 analyzing Internet websites in order to obtain usage statistics relating to their  
4 online users.

5           130. The online advertising industry sought to maximize the benefit of ad  
6 placement by developing two (2) advertising models to analyze consumer’s  
7 interest: “Contextual Advertising” and “Behavioral Advertising.”

8           131. Contextual Advertising matched ads to the content of the webpage  
9 the consumer was viewing. For example, if the consumer was visiting a car site,  
10 which was within the advertising network of sites, car ads would be placed on that  
11 site for the consumer to view.

12           132. Behavioral Advertising analyzed the consumer’s interest over a  
13 period of time, attempting to gauge a pattern of behavior relating to online  
14 searches. If the consumer was visiting multiple car sites over a period of time, and  
15 then searched for a sports site, car ads would appear on the sports site.

16           133. Behavioral targeting involves the collection of information about a  
17 consumer’s online activities in order to deliver advertising targeted to their  
18 potential upcoming purchases. It is conducted by companies that are generically  
19 identified as advertising networks. By observing the web activities of millions of  
20 consumers, advertising networks can closely match advertising to potential  
21 customers. The clear intent of behavioral targeting is to track consumers over  
22 time, to build up digital dossiers of their interests and shopping activities, tagging  
23 consumers with a unique identifier used to aggregate their web activity.

24           134. “Online behavioral tracking” as defined by the Federal Trade  
25 Commission defines such as “tracking consumers’ online activities over time ...  
26 in order to deliver advertising that is targeted to the individual consumer’s  
27 interests. This definition is not intended to include ‘first party’ advertising, where  
28 no data is shared with third parties, or contextual advertising, where an ad is based



1 on a single visit to a web page or single search query.” Federal Trade  
2 Commission, FTC Staff Revises Online Behavioral Advertising Principles  
3 (February 2009), online: <http://www.ftc.gov/opa/2009/02/behavad.shtm>.

4 135. The ultimate goal for online advertising networks became to obtain a  
5 complete digital dossier of all consumers, including all data pertaining to their  
6 sensitive information, personal identifying information and non-personal  
7 identifying information; however growing awareness of privacy risks led to an  
8 increase in blocking cookies.

9 136. Online advertisements, targeted or otherwise, were disfavored by  
10 consumers. As software programs that filtered online activity and deleted browser  
11 cookies developed in sophistication and availability, the consumer gained control  
12 over advertising strategies and advertiser attempts at data collection. Without the  
13 ability to maintain the accurate collection of user data, online advertising,  
14 contextual or behavioral, was not accurate. This diminished the effectiveness of  
15 cookies for behavioral targeting, so that other methods needed to be developed to  
16 further the objective of advertising network’s covert surveillance. The answer to  
17 the network advertising industry’s dilemma would come from an unlikely source,  
18 flash media products. Starting in 2006, the improvement to, and evolution of flash  
19 media products, would provide an unforeseen and indirect benefit to the network  
20 advertising industry. The exploitation of a user’s web browser and the flash media  
21 development provided the mechanism.

22 **B. The Internet and Web Browsers**

23 “People should have dominion over their computers ... The current,  
24 don’t ask, don’t tell” in online tracking and profiling has to end.”

25 FTC Chairman Jon Leibowitz, November 5, 2007.

26 137. The World-Wide-Web (WWW, or simply, “the web”), is a subset of  
27 the Internet, a computer network that allows users on one computer to access  
28 information stored on other computers through a world-wide network.

1           138. Computer networks are composed of individual computers connected  
2 together to share information consisting of a vast, decentralized collection of  
3 documents containing text, visual images, audio clips, and other informative  
4 media. Computers known as “servers” store web documents and make them  
5 available over the Internet through a set of standard operating and transmission  
6 protocols that define and structure the Web's operation and organization.

7           139. The Internet connects hundreds of thousands of independent  
8 networks into a vast global "network of networks," which has been simplified and  
9 commercialized for mass-market use, all speaking the same computer language,  
10 the Internet Protocol (IP). Every computer connected to the Internet has an IP  
11 address, a unique numeric identifier that can be “static”, i.e. unchanging, or may  
12 be “dynamically” assigned, such that your computer’s address changes with each  
13 new Internet session. This means that every new Internet connection means a new  
14 IP address. This address is essential to identify a PC on the Internet. The server  
15 only knows the address to which it should send the data requested, not the person  
16 who exists behind the address.

17           140. More sophisticated networking protocols may be "layered" on top of  
18 the IP protocol, enabling different types of Internet communications. For instance,  
19 World Wide Web (Web) communications are transmitted via the HyperText  
20 Transfer Protocol (HTTP) and e-mails via the Simple Mail Transport Protocol  
21 (SMTP).

22           141. These additional protocols use their own types of addresses, apart  
23 from IP addresses. For example, to download a webpage, you need its Web  
24 address, known as a Uniform Resource Locator (URL) (e.g., <http://www.abc.org>).  
25 To exchange e-mails, both the sender and recipient need e-mail addresses (e.g.,  
26 [user@emailprovider.com](mailto:user@emailprovider.com)). Web sites are groups of related documents that reside  
27 on one or more servers. Uniform Resource Locators or ("URLs") are addresses  
28 that indicate the precise location of specific Web documents on a server.

1           142. Web page persistence occurs by having a unique address or Uniform  
2 Resource Locator (URL) for each Web page, which is displayed in the address bar  
3 at the top of your browser as you browse the web. For example,  
4 <http://www.abc.org> is a simple URL pointing to a specific Web page. Every user  
5 that types in that URL in their browser header will be taken to the exact same  
6 page.

7           143. URLs can be used to uniquely identify individual users and allow  
8 stateful sessions, but unless a user bookmarks the URL containing their unique  
9 identifier, there is no way for the site to associate the same unique identifier with  
10 the same user on subsequent visits.

11           144. Consumers access the Internet through an Internet service provider  
12 (“ISP”). Whether the ISP offers Internet connectivity through dial-up; DSL  
13 (typically Asymmetric Digital Subscriber Line, ADSL); broadband wireless; cable  
14 modem; fiber to the premises (FTTH); or Integrated Services Digital Network  
15 (ISDN), the ISP is the ‘gateway’ through which all consumer communications  
16 must pass in order to take advantage of the benefits of the Internet. All email sent  
17 by the consumer is routed through the ISP in order to be delivered to its ultimate  
18 recipient. All web-based interactions similarly are routed from the user’s  
19 computer through the ISP and passed along to the relevant website. All  
20 communications from any website to the consumer must pass through the ISP.  
21 Anything that the consumer does that involves the Internet passes through the  
22 conduit that the ISP provides.

23           145. The web is built on a very simple, but powerful premise. All material  
24 on the web is formatted in a general, uniform format called HTML (Hypertext  
25 Markup Language), and all information requests and responses conform to a  
26 similarly standard protocol. When someone accesses a server on the Web, the  
27 user’s Web browser will send an information request to that website’s computer.  
28 This computer is called a web server. The web server will respond to the request

1 to that website's computer. There, the user's browser will display the received  
2 information on the user's screen.

3 146. Web servers respond to each client request without relating that  
4 request to previous requests. There was no need to remember what other pages the  
5 user had requested because the requests were for static pages. But if you've used a  
6 Web-based email system like Gmail, Hotmail, Yahoo! Mail, etc., you know that  
7 once you log in, the service remembers who you are as you click from message to  
8 message. When a website can keep track of a user as they move from page to page  
9 within a site it is called a "stateful session." The website doesn't necessarily need  
10 to know anything about the user, it just needs to be able to distinguish that  
11 particular user from all other users. If you leave the site before buying anything  
12 and then go back an hour later, it's possible that the site will have completely  
13 forgotten about you. In that case, the unique identifier persists during your  
14 "session" on the site, but it doesn't persist between sessions.

15 147. Although web browsers display whole scrollable pages, each of the  
16 many different pieces used to compose a single page — the text, pictures, photos,  
17 diagrams, animations, advertisements and so on — actually exist on the Internet as  
18 individual web page "assets," or individual web page assets are anything web  
19 pages display or use, such as the page's textual content, page layout and  
20 formatting information, executable scripts, images, animations, videos,  
21 advertisements, and so on.

22 148. A web browser's "operation model" is simple and straightforward; it  
23 is just a series of individual queries and replies. The key concept is that individual  
24 page assets exist separately on remote servers, and each must be requested  
25 separately by the web browser. Since each individual page asset must be  
26 separately requested from remote web servers, pages are literally built-up and  
27 assembled by requesting, receiving, and accumulating many separate assets onto a  
28 single page.

1           149. The main “body” of the page is first retrieved from a remote web  
2 server. After receiving the page's text, the web browser searches for all references  
3 to additional assets contained on the page and sends out a second wave of requests  
4 for each of the page's additional assets.

5           150. Web browser queries are composed of a series of lines of  
6 information, with each line containing a “name” and a “value.” Not all queries  
7 contain all of the same items. Some may contain additional “name:value pairs,”  
8 and you can probably infer much of the intent from the names and values  
9 themselves.

10           151. Modern web browsers and browser plug-ins provide a rich set of  
11 interfaces for web sites to store information on end-users' systems. This data is  
12 used for credentials (username/passwords and equivalents), tracking users, storing  
13 preferences (interface customizations, volume controls), site data (security  
14 questions, images, cached data), identifying tokens, or other data. User's desire to  
15 control tracking data (and other data third-parties store on their systems) has lead  
16 to a number of browser features, but the effectiveness of these tools is difficult for  
17 the average consumer to gauge, and provide a wealth of user data for online  
18 behavioral targeted advertising.

19           152. Web pages that contain links to files which the web browser can't  
20 play or display, such as no sound or animation files, required a plug-in or a helper  
21 application, such as a flash media player; however this widely accepted and  
22 trusted add-on provided a “hiding place” on the user’s computer for Defendants to  
23 perpetuate their covert surveillance of user’s online activities. Defendants would  
24 need initially to gain unauthorized access to the Quantcast Flash Cookie Affiliate  
25 users’ flash media technology, requiring the use not of browser cookies, but an  
26 emerging technology, flash cookies.

### 27           C. Browser Cookies

28                   The World Wide Web is an exciting new marketplace for

1 consumers. It offers easy access not only to a vast array of  
2 goods and services, but also to rich sources of information that  
3 enable consumers to make better-informed purchasing  
4 decisions. It also offers the convenience of shopping from the  
5 office or home. This information-rich medium also serves as a  
6 source of vast amounts of personal information about  
7 consumers. Commercial Web sites collect personal information  
8 explicitly through a variety of means, including registration  
9 pages, user surveys, and online contests, application forms, and  
10 order forms. Web sites also collect personal information  
11 through means that are not obvious to consumers, such as  
12 “cookies.”

13 <http://www.ftc.gov/reports/privacy3/history.shtm>

14 153. In the mid-1990s, technology was developed that enabled a small text  
15 file to be deposited on a hard drive of an individual computer. The text file itself  
16 typically occupied less than four kilobytes of memory, and was referred to as a  
17 “cookie.”

18 154. A "cookie" is a small text file that a website sends to a visitor's  
19 computer. Originally, the purpose of cookies was to give a website a means to  
20 tell that a "click" it received was from the same user that had clicked on a previous  
21 page, or to retain information such as which zip code to use in displaying weather  
22 reports to a user. . The cookie text files themselves consist of strings of “name-  
23 value” pairs that reduce to code various pieces of information about an  
24 individual’s computer, the browsing choices a person makes while accessing a  
25 website and any additional information a person discloses during a particular visit.  
26 While some cookies may contain minimal information, others may record a wide  
27 array of user-profiling information, IP numbers, shopping cart contents, user IDs,  
28 user-selected preferences, serial numbers, frequencies of contact with companies,

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

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

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

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

21 158. Cookie setting by advertising networks occurs as follow:

- 22 a) User visits a Quantcast Flash Cookie Affiliate website that includes a  
23 banner or script of the Defendant Quantcast advertising network. The  
24 visit then creates a new cookie and assigns a previously unused  
25 unique id, i.e. 12345. The cookie content (whether flash or http or  
26 both could now be id=12345). The database of the advertising  
27 network would now contain an entry 12345 with content time and  
28 date of access, website visited, category of product that was displayed

1 if applicable, language setting of the browser, ip address, location of  
2 user, etc.

3 b) User later visits another site that includes the same advertising  
4 network. The cookie value 12345 is therefore sent to that site. The site  
5 now retrieves the info in its database under the id 12345 and maybe  
6 displays another more relevant ad according to what it knows and  
7 amends the database with the new information, same than above.

8 159. 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.google.com could be shared with  
10 calendar.google.com). These are called first-party cookies because they're set by  
11 the site displayed in the address bar of the Web browser. Third-party cookies, on  
12 the 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.

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



1 specify a date, the cookie is removed once the user quits his or her browser. As a  
2 result, specifying a date is a way for making a cookie survive across sessions. For  
3 this reason, cookies with an expiration date are called persistent.

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

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

12 163. Clickstream data may include basic information, such as the type of  
13 computer an individual used to access the Internet, the kind of Internet browser  
14 utilized and the identification of each site or page visited. In addition, were an  
15 individual to disclose certain information during the visit, the clickstream data  
16 may also include more personalized details, such as passwords, e-mail addresses,  
17 credit card numbers, name, address, date of birth, gender, or zip code. Centralized  
18 website servers, however, simply lack the capacity to store and sift through the  
19 vast amounts of clickstream data generated by every visitor to a site. In an effort  
20 to sidestep the need for centralized data storage, "cookies," were developed as a  
21 means for a website to collect and store clickstream data on the hard drive of each  
22 visitor's computer. By accessing, reading and editing the cookies that a website  
23 stores on an individual's computer, a website can maintain detailed records about  
24 a particular individual over a period of time.

25 164. The session context encapsulates the total time a visitor is on the site.  
26 The nature of HTTP protocol is that is connections are not maintained. Once all  
27 the content for a page request is transferred, the connection is terminated. When a  
28 visitor first enters a site, they are given a unique id in a cookie. When they return

1 within a fixed amount of time, the cookie is returned, making it possible for the  
2 server to identify them as the same visitor. This technique is useless if a visitor's  
3 browser has cookie support turned off.

4 165. Used in combination with cookies, a web beacon is an often-  
5 transparent graphic image, usually no larger than 1 pixel x 1 pixel, that is placed  
6 on a website or in an e-mail that is used to monitor the behavior of the user  
7 visiting the website or sending the e-mail. Alternative names are bug, web bug,  
8 action tag, tracking bug, tracking pixel, pixel tag, 1×1 gif, and clear gif. When the  
9 HTML code for the Web beacon points to a site to retrieve the image, at the same  
10 time it can pass along information such as the IP address of the computer that  
11 retrieved the image, the time the Web beacon was viewed and for how long, the  
12 type of browser that retrieved the image and previously set cookie values.

13 166. The bug is one of the ingredients of the page, just like other images  
14 and text, except it is very small and/or clear such that it is effectively invisible.  
15 Web pages and graphical e-mails use presentation code that tells your computer  
16 what to do when a page is opened. This code usually contains the text of the page,  
17 but it typically also contains a number of instructions that cause your computer to  
18 ask either the website's server or another server to send you further content, such  
19 as an image. Web bugs are images retrieved in this way. The action of calling the  
20 material from another server allows the event to be counted. They are a  
21 convenient way of gathering statistics and managing cookies within a complex  
22 network.

23 167. Web bugs also use the HTML IFrame, style, script, input link,  
24 embed, object, and other tags to track usage. Whenever the user opens the page  
25 with a graphical browser or e-mail reader, the image or other information is  
26 downloaded. This download requires the browser to request the image from the  
27 server storing it, allowing the server to take notice of the download. As a result,  
28 the organization running the server is informed when the HTML page has been

1 viewed.

2 168. Web bugs are typically used by third parties to monitor the activity of  
3 customers at a site. Turning off a browser's cookies can prevent some web bugs  
4 from tracking a customer's specific activity. The website logs will still record a  
5 page request from the customer's IP address, but unique information associated  
6 with a cookie cannot be recorded.

7 169. Cookies exist because the underlying HTTP protocol is “stateless”—  
8 each request from your browser is completely separate from the next one, so the  
9 server needs a way to keep track of what request belongs to what visitor. By  
10 storing a small bit of information in a cookie, the web site can determine that your  
11 page view belongs to your user account. The browser feature that allows a website  
12 to store “**state**” on the user can be abused for tracking, and co-operative tracking  
13 by websites, and is essentially impossible to defend against.

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

27 **D. Web Browser Security**

28 171. Computers are used for everything from banking and investing to

1 shopping and communicating with others through email or chat programs.

2 Although online communications may not be considered “top secret,” online users  
3 do not want third parties reading their email, or examining personal information  
4 stored on their computer (such as financial statements), or downloading software,  
5 such as flash cookies, without their knowledge or consent.

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

13 173. Web browser security is the process of preventing and detecting  
14 unauthorized use of a computer. Prevention measures help stop unauthorized users  
15 (also known as “intruders”) from accessing any part of a computer system.  
16 Detection helps to determine whether or not someone attempted to break into a  
17 system, if they were successful, and what they may have done.

18 174. Attackers focus on exploiting client-side systems through various  
19 vulnerabilities, using these vulnerabilities to take control of a computer,  
20 downloading software, stealing information, and destroying a user’s files. A low-  
21 cost way attackers do this is by exploiting vulnerabilities in web browsers.

22 175. The security threat from software attacks on vulnerable web browsers  
23 is increased by many factors, such as: configuring web browsers to increase  
24 functionality, or web sites requiring users to enable features or install additional  
25 software. Users unaware of how to configure their web browsers in any manner,  
26 let alone securely, are vulnerable to having unscrupulous entities exploit the user’s  
27 computer due to their lack of knowledge in this area.

28 176. Most computers are sold with a web browser installed; however the

1 operating system is not setup up in a secure default configuration. The software is  
2 installed by the computer manufacturer, operating system maker, Internet service  
3 provider, or by the retail store.

4 177. Multiple web browsers may be installed on a computer. Software  
5 applications on a computer, such as email clients or document viewers, may use a  
6 different browser than the one a user normally uses to access the web. Also,  
7 certain file types may be configured to open with a different web browser. Using  
8 one web browser for manually interacting with web sites does not mean other  
9 applications will automatically use the same browser. For this reason, it is  
10 important to securely configure each web browser that may be installed on a  
11 computer. One advantage to having multiple web browsers is that one browser can  
12 be used for only sensitive activities such as online banking, and the other can be  
13 used for general purpose web browsing.

14 178. With some web browsers, users have the option of turning off or  
15 deleting their cookies. When this happens, web servers are unable to track users or  
16 set up customized content for users. If the website requires login or registration  
17 information, it can correlate personally identifiable information (PII) with  
18 browsing behavior.

19 179. Spyware, Adware, Trojans, Worms, Keyloggers, Toolbar Hijackers,  
20 and other harmful programs are all tracking programs that secretly install onto  
21 user's computer. Once infected with these malicious programs, privacy and  
22 personal information are at risk. Spyware, as well as other malicious programs,  
23 can go from dangerous, stealing your passwords and credit card information, to  
24 simply annoying you with their excessive popups. These malicious programs can  
25 track your surfing habits, abuse your Internet connection by sending this data to a  
26 third party, profile your shopping preferences, hijack your browser, and alter  
27 important system files – all without your knowledge or permission.

28 180. Within the last decade, software developers have produced a

1 substantial number of cookie cleaners which provide additional protection from  
2 unwanted cookies being set by websites; furthermore browser developers have  
3 added a multitude of options for cookie management.

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

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

22 183. The Advanced tab contains settings that apply to all of the security  
23 zones. Disabling the Enable third-party browser extensions option, limiting tool  
24 bars and Browser Helper Objects (BHOs), provide greater privacy controls. A  
25 user may evaluate the originating site to determine whether they wish to accept or  
26 deny the cookie, and what action to take (allow or block, with the option to  
27 remember the decision for all future cookies from that web site).

28 184. The Privacy tab contains settings for cookies. The Advanced button

1 and Override automatic cookie handling allows a user to select Prompt for added  
2 protection from both first and third-party cookies. This will prompt a user each  
3 time a site tries to place a cookie on their machine.

4 185. The Security tab lists the various security zones that Internet Explorer  
5 uses. For each of these zones, a user can customize their Custom Level of  
6 protection. The Internet zone is where all sites initially start out. The security  
7 settings for this zone apply to all the web sites that are not listed in the other  
8 security zones. By selecting the High security setting, several features, including  
9 ActiveX, Active scripting, and Java will be disabled. With these features disabled,  
10 the browser will be more secure.

11 186. The Trusted sites zone is a security zone for sites that a user thinks  
12 are safe to visit, and can be trusted not to contain malicious content. For a more  
13 fine-grained control over what features are allowed in the zone, a user clicks the  
14 Custom Level button to control the specific security options that apply to the  
15 current zone.

16 187. When a browser is set in private browsing mode (during a private  
17 browsing "session"), the web browser stores several types of information only  
18 temporarily. Once the session ends, the browser will delete that data, including the  
19 record of online visits to websites in the browser's history, cookies, and cached  
20 image files. This keeps browsing session private from other people that may use  
21 the same computer. This contrasts with normal browsing, where the browser  
22 remembers history that can be used even after restarting the browser. Private  
23 browsing allows users to browse the web without storing any browsing history on  
24 the user's computer.

25 188. Blocking third party cookies is difficult. One defense is to disable  
26 third-party cookies, thereby limiting the types of information they can collect and  
27 associate with personally identifiable information. However, not all browsers have  
28 this functionality. Furthermore, blocking third-party cookies does not remove the

1 web bug itself, since it is part of the web page and not the cookie, and has the  
2 capability to track navigation data using IP address as an identifier. In cases where  
3 a user maintains a static IP, that may be all that is necessary match a profile to an  
4 individual user.

5 189. Flash media players, such as the Macromedia flash media player  
6 (Adobe), operate outside the boundaries of a user's browser and flash content acts  
7 independently, relying on a security model within itself.

8 "How do I use the Settings Manager to manage third-party content  
9 storage settings?

10 The Flash Player Settings Manager lets you manage privacy settings,  
11 storage settings, security settings, and automatic notification settings  
12 by clicking the tabs. Your first experience with Flash Player settings  
13 might have been while visiting a site with Flash content, when a pop-  
14 up menu asked you questions about privacy or storage space, or by  
15 right-clicking on content to see the Settings option in the context  
16 menu. Selecting the Help icon or clicking the Advanced button within  
17 the Settings dialog box in Flash Player opens a browser to the Settings  
18 Manager on Adobe.com, or you can access the Settings Manager  
19 directly.

20 The third-party content setting can be found in the Global Storage  
21 Settings panel in the Settings Manager. You can prevent all third  
22 parties from storing information on your computer by deselecting the  
23 "Allow third-party Flash content option." If you disable all third-party  
24 content storage, Flash Player will not allow information to be read or  
25 written by Flash content unless the address of the content matches the  
26 address displayed in your browser's address bar. Flash Player  
27 remembers your setting and blocks third-party content storage for all  
28 sites you visit.



1 Conclusion

2 Like browser cookies, Flash Player local shared objects are used to  
3 create great web experiences for users, but they might be misused by  
4 some advertisers and websites.”

5 <http://www.adobe.com/products/flashplayer/articles/thirdpartyiso/>

6 190. Within the flash environment, “flash cookies,” properly known as  
7 “local shared objects,” emerged as a tracking device, due to the culmination of a  
8 few factors, including but not limited to: individual’s awareness of privacy  
9 implications from their use of the Internet, development of the flash media player  
10 and LSO; new industry developing software to protect online user’s privacy,  
11 improvements to the web browser, storage limitation of user data, and the demise  
12 of the benefits of using cookies due to performance problems related to response  
13 times.

14 191. HTTP requests require all associated cookies that have been set for  
15 that domain and path to be sent collectively, thus such factors as the http header  
16 request and cookie size delays the response time to download the webpage  
17 resulting in significant effects on abandonment, and reduced overall traffic.  
18 Excluding a reduction of cookie size, the advertising industry sought a means to  
19 conduct covert surveillance while gaining the ability to ignore user’s privacy  
20 preferences. Flash media players, and local stored objects provided the means to  
21 this end.

22 E. Flash Player- Cookies-LSO

23 192. [http://www.ftc.gov/os/comments/privacyroundtable/544506-](http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf)  
24 [00085.pdf](http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf)

25 A Brief History of Flash Player

26 193. In 1995, the Web was all about text. There was no easy way to create  
27 rich and engaging graphics and animation for display in Web browsers. The  
28 creators of FutureSplash, the ancestor of today’s Flash Player, had originally

1 created a graphics technology for pen computing tablets, but this technology was  
2 ahead of its time. The team looked for other ways to distribute this technology. In  
3 1996, Netscape introduced a browser technology that allowed developers to  
4 extend the browser and FutureSplash was brought to the Web via this technology.  
5 The first big success of the new technology came in August of 1996, when  
6 Microsoft used FutureSplash to create the most TV-like experience on the Internet  
7 at that time with MSN. This was quickly followed by Disney’s use of  
8 FutureSplash for the animation and user interface for the Disney Daily Blast.

9       194. Macromedia acquired FutureSplash in 1996 and released it as  
10 Macromedia Flash 1.0. Over the next few years, Macromedia added innovative  
11 new capabilities, such as sound, simple scripting to create interactive Web  
12 experiences, and video. The technology gained in popularity for websites, casual  
13 games, and rich media advertising.

14       195. As Flash Player increased in sophistication, so did the content built  
15 using Flash technology. In 2002, Macromedia launched Flash Player 6 and coined  
16 the term “rich Internet application” (RIA) to describe a more robust Web  
17 application that could be deployed across different types of browsers and  
18 operating systems, and that offered users, including enterprises, a more  
19 compelling and interactive experience than was previously unavailable on the  
20 Web. In December 2005, Adobe acquired Macromedia and continued the  
21 development of Flash Player to offer richer experiences on the web.

22       196. Today, over 75 percent of online videos viewed worldwide are  
23 delivered using the Flash technology, making it the No.1 platform for video on the  
24 web. According to an Adobe internal survey, over 70 percent of web-based games  
25 are built using flash technology. One flash game developer did his own research  
26 into the space in July 2007 and found more than 14,000 games spread across  
27 30,000 game portals with hundreds of new games launching every month.

28       Local Storage in Flash Player

1           197. To build a platform that could support the development of robust  
2 applications, a number of new capabilities were added to flash player. The  
3 addition of local storage was a feature designed to support RIAs. Web  
4 applications require the ability to store information so that once the application is  
5 closed by the user, the information (such as user preferences) can be retrieved the  
6 next time the user loads the application. This information is stored locally on the  
7 user's computer, and is available only to the domain that stored it.

8           198. Local storage allows websites with applications built to run in Flash  
9 player to store data associated with those applications on the user's computer for  
10 use when the user revisits that site. Many websites use this feature to save  
11 information such as the user's work, online game progress or high scores, login  
12 data, and/or preferences. Local storage can improve the browsing experience by  
13 eliminating the need for users to reenter information each time they visit a site.

14           199. Local storage can store simple text as well as more complex data.  
15 Local storage, by itself, cannot do anything to or with the data on a computer. The  
16 storage is just a container to hold information such as user preferences which the  
17 web developer deems appropriate to help make the user experience easy, intuitive,  
18 and consistent with the user's expectations in context.

19           200. There are many use cases for local storage. The following are some  
20 of the most common ones:

- 21           • Application preferences – The ability for an application to remember a  
22 user's choices made while visiting a Website. These can range from a  
23 convenience feature to a critical aspect of the application.

24           For example, many video websites will use Local Storage to store the  
25 volume preference for the video playback experience. Once a user  
26 adjusts the volume setting, it is remembered so that the user does not  
27 need to reset it when moving from one video to the next or upon  
28 future visits to the same video site. By using Local Storage for this

1 purpose, the user experience becomes faster because the user is not  
2 required to first create a user account that would then be used to  
3 associate the user with user-specific volume setting.

4 Without the ability to store preferences, more sophisticated  
5 applications would not be able to provide the quality Web experience  
6 users have come to expect. For example, if the user did not have the  
7 ability to store his choice of a custom dictionary in an online word  
8 processor, he would need to select it each time he visited the site. As  
9 another example, other websites or Web applications that use Flash  
10 Player may allow the user to configure or customize her own user  
11 interface. That information can be stored in local storage and used by  
12 the application the next time the user visits the site, as the user would  
13 expect.

- 14 • Caching – Many online applications consist of a large number of files  
15 and data that need to be downloaded during each visit, to load user  
16 preferences, such as language preferences or other user-specific  
17 application data. By storing this data in Local Storage, the local data  
18 can be used instead of requesting it from the server every time the  
19 application is loaded. This optimization results in a faster start-up time  
20 for the user when she visits the site.
- 21 • Saved Data – Applications generally need to “maintain state” for the  
22 user, so the application can be returned to the same point where the  
23 user left it. Games are a good example of this and are one of the most  
24 recognizable types of content that run in Flash Player. Many large-  
25 scale games are designed to be played across multiple sessions or  
26 visits. In most games, Local Storage is updated regularly with the  
27 progress. Thus, the user can leave the game, return to it at a later time,  
28 and continue from where he left off, just as he would expect.

- Temporary Data – Web applications and websites that don't require the reloading of a page or that don't require the user to navigate the page through links have become common, yet, the browser navigation model has struggled to keep up. As a result, using the browser navigation (e.g. the "Forward" and "Back" buttons) may accidentally take the user away from a site or an application she was using. Most often, once the Web page is gone, so is the unsaved data in the application. Many Flash applications address this problem by storing temporary data in Local Storage so that the user can return and continue where she left off.

For example, many users employ online photo editing sites to manage images before sharing them with friends. What happens when a user makes changes to an image, but accidentally hits the browser's "Back" button before saving the changes? Often, those changes will be lost. By using Local Storage, the application can save all the changes the user made so that she can pick up where she left off instead of requiring her to start from scratch.

201. The flash player is software for viewing animations and movies using computer programs such as a web browser. Flash player is a widely distributed proprietary multimedia and application player created by Macromedia and now developed and distributed. Flash player runs SWF files that can be created by the flash authoring tool, or by a number of other Macromedia and third party tools.

202. Flash refers to both a multimedia authoring program and the flash player that uses vector and raster graphics, a native scripting language called ActionScript and bidirectional streaming of video and audio. Strictly speaking, flash is the authoring environment and flash player is the virtual machine used to run the flash files, but in colloquial language these have become mixed: "Flash" can mean either the authoring environment, the player, or the application files.

1           203. The Flash Player was originally designed to display 2-dimensional  
2 vector animation, but has since become suitable for creating rich Internet  
3 applications and streaming video and audio. It uses vector graphics to minimize  
4 file size and create files that save bandwidth and loading time. Flash is a common  
5 format for games, animations, and GUIs embedded into web pages.

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

13           205. Flash cookies are not transferred from the client back to the server  
14 like HTTP cookies. Instead, downloaded Flash objects that run locally in the web  
15 browser [locally stored/run objects] read and write these cookie like files. Using  
16 JavaScript, this data can be pulled out of the Flash objects and then used like any  
17 other data by the web application. It is not necessary to have any visible signs that  
18 a Flash object is running on a given page. In fact, it would be difficult to reliably  
19 detect if an application were using flash cookies.

20           206. When you drill down in each domain's directory, you will eventually  
21 find a "SOL" file. This file contains the data that is stored and used as the flash  
22 cookie.

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

27           208. Functionally, client storage areas are quite different from cookies.  
28 DOM Storage doesn't transmit values to the server with every request as cookies

1 do, nor does the data in a local storage area ever expire. And unlike cookies, it is  
2 easy to access individual pieces of data using a standard interface that has growing  
3 support among browser vendors. If objects are stored in a Local Object Repository  
4 then these are available to specific actions but not to all the actions. But if these  
5 objects are stored in one or more Shared Object Repositories then multiple actions  
6 or tests can use them.

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

16       210. Flash LSO cookies properties:

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

- 1 • Shared folders allow cross-browser tracking
- 2 • There is currently no mechanism to force a shared-object to "expire".
- 3 Browser cookies have an expiration mechanism built in.
- 4 User can only disable local shared-object by disallowing a particular
- 5 site to write to the user's hard drive. This can be done in the
- 6 Macromedia player Setting window.

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

15 212. The flash cookie setting process is a system, method and computer  
16 readable medium configured to track Internet users as they browse web-sites when  
17 cookies are disabled or deleted. A web-site receives a request for content from the  
18 computing-device. After obtaining information about the computing-device, the  
19 tracking-server assesses the request for content from the computing-device. If the  
20 computing-device has an available flash plug-in, the tracking-server transmits a  
21 flash applet to the computing-device. The flash applet is configured to: determine  
22 whether a unique flash identifier has been assigned to the computing-device,  
23 generate the unique flash identifier if no unique flash identifier has already been  
24 assigned to the computing-device, transmit the unique flash identifier to a tracking  
25 server, and store the unique flash identifier in local flash storage. The process also  
26 stores a cookie at the computing-device when no flash plug-in is available.

27 213. While the flash media industry was developing the tools required to  
28 accommodate the needs of its users, these same innovations became an "attractive



1 nuisance” to those in the advertising industry. Such entities, including the  
2 Defendants, rather than taking the lawful and ethical path to building businesses  
3 that respect the privacy rights of Internet users, have sought their fortunes by  
4 brazenly exploiting digital technology. This has been compounded by the FTC’s  
5 policy of self-regulation of the advertising industry, a policy akin to: “the fox  
6 guarding the hen house.” Using the leverage of the Internet, the Defendants  
7 reduced the flash media industry’s innovations to the level of a mere spy tool. The  
8 Defendants’ brazen disregard of privacy rights fundamentally threatens not just  
9 Plaintiffs and Class members but the economic underpinnings of one of the most  
10 important sections of the United States economy. Although “the fox has raided the  
11 hen house,” the basis of this class action shall let it be known: the “chickens have  
12 come home to roost.”

13 **F. Flash Cookies, Privacy, and the “Elephant in the Room”**

14 “If users don't want to be tracked and there is a problem with tracking,  
15 then we should regulate tracking, not regulate cookies.”

16 Ashkan Soltani

17 Singel, Ryan. “You Deleted Your Cookies? Think Again.” Wired.  
18 (August 10, 2009) [http://www.wired.com/epicenter/2009/08/you-  
19 deleted-your-cookies-think-again/](http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/)

20 **1. Elephant in the Hard Drive CIRCA: 2005**

21 Cohn, Michael. “Flash Player Worries Privacy Advocates”  
22 InternetWeek. (April 15, 2005)

23 [http://www.informationweek.com/news/showArticle.jhtml?articleI  
24 D=160901743](http://www.informationweek.com/news/showArticle.jhtml?articleID=160901743)

25 “Macromedia's Flash media player is raising concerns among  
26 privacy advocates for its little-known ability to store computer  
27 users' personal information and assign a unique identifier to their  
28 machines.

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

Macromedia emphasized that Flash only stores personal information if computer users elect to fill in the information on a website.

While websites are supposed to safeguard the personal information they gather according to the dictates of their privacy policies, many sites, nevertheless, share customer information widely.”

Wegert, Tessa. “The Web Cookie is crumbling- and marketers feel the fallout” The Globe and Mail. (July 21, 2005)

<http://www.theglobeandmail.com/news/technology/article891541.ace>

“A recent study by international research advisory organization JupiterResearch has found that nearly 60 per cent of American Internet users have deleted cookies from their primary computers, with 39 per cent doing so on a monthly basis. According to the report, as more and more people block or delete cookies, it could cause the long-term measurement of consumer Web surfing behaviour to be "severely compromised.”

"The attitude is there is something wrong with [cookies], when really they are benign," he says.

Jeff Fox, senior project editor with Consumer Reports Magazine, agrees. "Cookies aren't spybots hanging around people's computers," he says. "They are passive data files. Their only problem is that there's nothing to stop marketers in the future from associating anonymous information with personal information."

JupiterResearch analyst Mr. Peterson says that besides making things easier for marketers and research companies, there are spinoff benefits for Web surfers if they stop deleting cookie files.

"Cookies are just designed to help marketers make better

1 websites," he maintains.

2 The Internet marketing industry hopes Internet users will bite.”

3 2. “Elephant is Out of the Room” CIRCA: 2009

4 “We find that more than 50 percent of the sites in our sample are  
5 using flash cookies to store information about the user. Some are  
6 using it to ‘respawn’ or re-instantiate HTTP cookies deleted by the  
7 user. Flash cookies often share the same values as HTTP cookies,  
8 and are even used on government websites to assign unique values  
9 to users. Privacy policies rarely disclose the presence of Flash  
10 cookies, and user controls for effectuating privacy preferences are  
11 lacking.”

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

15 “The following are my questions (in bold) and Mrs. Rasmussen’s  
16 responses verbatim. Flash Local Shared Objects (LSOs) have been  
17 around for a long-time and I have been aware of their use as a  
18 “backup” for browser cookies for reset and other calculations for a  
19 few years. What made you write your letter to the FTC now? Was  
20 there a specific event or occurrence?

21 The topic of respawning browser cookies using Flash local storage  
22 was publicized after research conducted by UC Berkeley on the  
23 subject was published in August 2009. The topic was also raised at  
24 the FTC’s First Privacy Roundtable in December, so when the  
25 FTC announced that its Second Roundtable would focus on  
26 Technology and Privacy, we felt it was the appropriate opportunity  
27 for Adobe to describe the problem and state our position on the  
28 practice.”

1 Peterson, Eric. "My Interview with Adobe Chief Privacy Officer"  
2 Web Analytics Demystified. (April 2010)  
3 [http://blog.webanalyticsdemystified.com/weblog/2010/04/my-](http://blog.webanalyticsdemystified.com/weblog/2010/04/my-interview-with-adobe-chief-privacy-officer.html)  
4 [interview-with-adobe-chief-privacy-officer.html](http://blog.webanalyticsdemystified.com/weblog/2010/04/my-interview-with-adobe-chief-privacy-officer.html)

5 3. "Flash Cookies and Privacy"- Berkeley Study

6 214. A study released by researchers at the University of California,  
7 Berkeley and other universities, submitted to the federal government for  
8 consideration as part of a new policy on the use of tracking technologies, revealed  
9 the details of a consumer online privacy invasion of such epidemic proportions  
10 that the FTC finally took notice of the advertising networks' deceptive practices.

11 Ashkan Soltani et al., "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 A.Introduction:

14 In 2005, United Virtualities (UV), an online advertising company,  
15 exclaimed, "All advertisers, websites and networks use [HTTP]  
16 cookies for targeted advertising, but cookies are under attack." The  
17 company announced that it had, "developed a backup ID system  
18 for cookies set by web sites, ad networks and advertisers, but  
19 increasingly deleted by users. UV's 'Persistent Identification  
20 Element' (PIE) is tagged to the user's browser, providing each with  
21 a unique ID just like traditional cookie coding. However, PIEs  
22 cannot be deleted by any commercially available antispysware, mal-  
23 ware, or adware removal program. They will even function at the  
24 default security setting for Internet Explorer."

25 United Virtualities' PIE leveraged a feature in Adobe's Flash MX:  
26 the "local shared object," also known as the "flash cookie."

27 Erasing HTTP cookies, clearing history, erasing the cache, or  
28 choosing a delete private data option within the browser does not

1 affect Flash cookies. Even the ‘Private Browsing’ mode recently  
2 added to most browsers such as Internet Explorer 8 and Firefox 3  
3 still allows Flash cookies to operate fully and track the user.

4 We surveyed the top 100 websites to determine which were using  
5 Flash cookies, and explored the privacy implications. We  
6 examined these sites’ privacy policies to see whether they  
7 discussed Flash cookies.

8 From a privacy perspective, this is problematic, because in  
9 addition to storing user settings, many sites stored the same values  
10 in both HTTP and Flash cookies, usually with telling variable  
11 names indicating they were user ids or computer guids (globally  
12 unique identifiers). We found that top 100 websites are using Flash  
13 cookies to “respawn,”<sup>1</sup> or recreate deleted HTTP cookies. This  
14 means that privacy-sensitive consumers who “toss” their HTTP  
15 cookies to prevent tracking or remain anonymous are still being  
16 uniquely identified online by advertising companies. Few websites  
17 disclose their use of Flash in privacy policies...”

18 A Flash cookie can be set when a websites embeds first party or  
19 third party Flash content on a page. For instance, a website may  
20 include animated Flash banner advertisements served by a  
21 company that leases the advertising space or they may embed a  
22 hidden SWF used solely to provide metrics on the user. Thus,  
23 merely visiting some websites (without actually clicking on an  
24 advertisement or video) can cause Flash data from a third party  
25 advertiser to be stored on the user’s computer, often unbeknownst  
26 to the user. [How done? Tricks?]

27 B.Results and Discussion:

- 28 • We encountered Flash cookies on 54 of the top 100 sites. These 54

1 sites set a total of 157 Flash shared objects files yielding a total of  
2 281 individual Flash cookies. Ninety-eight of the top 100 sites set  
3 HTTP cookies (only wikipedia and wikimedia.org lacked HTTP  
4 cookies in our tests). These 98 sites set a total of 3,602 HTTP  
5 cookies. Thirty-one of these sites carried a TRUSTe Privacy Seal.  
6 Of these 31, 14 were employing Flash cookies.

- 7 • We found that taking the privacy-conscious step of deleting HTTP  
8 cookies to prevent unique tracking could be circumvented through  
9 “respawning.” The Flash cookie value would be rewritten in the  
10 standard HTTP cookie value, thus subverting the user’s attempt to  
11 prevent tracking.
- 12 • We also found HTTP cookie respawning across domains.
- 13 • “The NAI (Network Advertising Initiative) is a cooperative of  
14 online marketing and analytics companies committed to building  
15 consumer awareness and establishing responsible business and  
16 data management practices and standards.” Since some of the sites  
17 using Flash cookies also belong to the NAI, we tested the  
18 interaction of Flash cookies with the NAI opt-out cookie.
- 19 • We found that persistent Flash cookies were still used when the  
20 NAI opt-out cookie for QuantCast was set. Upon deletion of  
21 cookies, the Flash cookie still allowed a respawn of the QuantCast  
22 HTML cookie (see Figures 4-7). It did not respawn the opt-out  
23 cookie. Thus, user tracking is still present after individuals opt out.
- 24 • Adobe Flash settings files (those in the Macromedia.com folder)  
25 were set by Flash player in visits to 89 of the top 100 sites. A total  
26 of 201 settings files were present among these 89 sites. This is  
27 relevant, because each settings file is stored in its own directory,  
28 labeled by domain. This creates a type of history file parallel to the

1 one created by the browser.

- 2 • However, the Flash history is not deleted when browser controls  
3 are used to erase information about sites previously visited. This  
4 means that users may falsely believe that they have fully cleared  
5 their history when using the standard browser tools.
- 6 • We searched the privacy policies of the top 100 sites, looking for  
7 terms such as “Flash,” “PIE,” or “LSO.” Only 4 mentioned the use  
8 of Flash as a tracking mechanism. Given the different storage  
9 characteristics of Flash cookies, without disclosure of Flash  
10 cookies in a privacy policy, it is unclear how the average user  
11 would even know of the technology. This would make privacy  
12 self-help impossible except for sophisticated users.
- 13 • When disabling third party content, we found that 84 of the sites  
14 had no functionality issues after third-party Flash content was  
15 disabled. Sixteen sites stored some type of Flash data.

#### 16 G. Overlapping Values

17 “QuantCast changed its code and updated its servers Tuesday  
18 afternoon after Wired.com published a story about the research,  
19 according to spokeswoman Christina Cubeta.”

20 “Quantcast no longer restores deleted cookies using values stored in  
21 Flash,” Cubeta said, describing the behavior as an “unintended effect”  
22 of trying to have better web-traffic measurement.”

23 Singel, Ryan. “Flash Cookie Researchers Spark Quantcast Change”  
24 Wired. (August 12, 2009)

25 [http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-  
26 spark-quantcast-change/#ixzz0nepIEDIb](http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-spark-quantcast-change/#ixzz0nepIEDIb)

27 215. The “Flash Cookies and Privacy,” study attempted to infer the  
28 potential use of flash cookies by examining the variable name for each cookie i.e.

1 volume, userid, user, referred to as a “unique identifier;” however without access  
2 to the Defendants’ server and database, such flash cookie forensics to determine  
3 whether the flash cookie is benign or not, cannot be definitive.

4 216. “Flash cookie forensics” related to the expiration date of cookie  
5 information and the entropy of the information contained in the cookie provides  
6 limited information. If the entropy is low (e.g. content is “volume =5”) then it can  
7 be assumed to be a legitimate setting to be saved. If the entropy is high (e.g.  
8 “userId = b56574ce78d2f110b1gd522”) then it is more likely than not a tracking  
9 id connected to a background database of user information, i.e. a user goes to a  
10 website wherein the algorithm locates a normal cookie stored by an advertising  
11 network, then the algorithm searched for repeating keys. Every character (at least  
12 in a charset like ASCII) counts one byte, thus counting the number of characters  
13 in “id=344499284532” which are 15 and in “volume\_level=98,  
14 language=English” which are 32.

15 217. The analysis of both HTTP and flash cookies for key identifiers  
16 revealed undisputable correlations including overlapping values.

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

21 “Of the top 100 websites, 31 had at least one overlap between a HTTP  
22 and Flash cookie. For instance, a website might have an HTTP cookie  
23 labeled “uid” with a long value such as 4a7082eb-775d6-d440f-dbf25.  
24 There were 41 such matches on these 31 sites. Most Flash cookies  
25 with matching values were served by third-party advertising networks.  
26 That is, upon a visit to a top 100 website, a third party advertising  
27 network would set both a third party HTTP cookie and a third party  
28 Flash cookie.”



1           218. Researchers were able to identify a high number of cookies similarly  
2 labeled such as: “user ID.” These cookies stored unique identifiers which allowed  
3 user tracking; however unlike HTTP cookies used for tracking these cookies had  
4 overlapping values. This respawning was because the flash cookies, provided by  
5 Quantcast, had the same data values as the HTTP cookies, provided by the  
6 Quantcast Flash Cookie Affiliates, so in effect the flash cookies acted as a back-up  
7 on the computer systems once the HTTP cookies had been removed. If users  
8 simply deleted cookies without clearing the browser cache, the identifiers in the  
9 deleted browser cookies still returned to the cookies, more than likely, using  
10 information stored in the cache.

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

16                   Moscaritolo, Angela. “ Top Websites using Flash cookies to track user  
17 behavior.” SC Magazine. (August 11, 2009)

18                   <http://www.scmagazineus.com/top-websites-using-flash-cookies-to-track-user-behavior/article/141486/>

20           Defendants implanted identical code in the Plaintiffs and Class members’  
21 computers resulting in a uniform action to set redundant unique identifiers  
22 used to identify and track users overlapping values, as evident by the  
23 computer logs from Class representative Edward Valdez:

24           220. “userPrefs.sol” would be HTTP cookies set by a Quantcast Flash  
25 Cookie Affiliate MTV on 10/22/2009, with a size of 434, using a “shared object”  
26 path, so as to store users’ preferences, such as volume control.

27           221. “com.quantserve.sol,” set by Defendant Quantcast, in concert with  
28 Defendant MTV (media.mtvnservices.com/player/release) on 10/28/2009, with a

size of 72, provides the tracking mechanism.

Cookie Name	Date Created/ Changed	Size	Path	User ID	Domain
<a href="http://media.mtvnservices.com/player/release">http://media.mtvnservices.com/player/release</a> userPrefs.sol	10/22/2009 9:26:09 PM 11/5/2009 12:03:06 PM	434	C:\Users\Owner\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\	N2AMUEDE	media.mtvnservices.com
<a href="http://media.mtvnservices.com/com.quantserve">http://media.mtvnservices.com/com.quantserve</a> rve.sol	10/28/2009 10:16:12PM 10/28/2009 10:16:12 PM	72	C:\Users\Owner\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\	N2AMUEDE	media.mtvnservices.com

222. Such issues, taken individually, would be of limited consequence, but analyzed collectively, with an overlapping value set by a common domain, provided a record of Defendants’ activity, located on Plaintiffs and Class members’ hard drive, and permanent documentation that Defendants cannot control or delete.

223. The identical “userID” “N2AMUEDE,” evidences that Quantcast Flash Cookie Affiliates acted independently and in concert with Quantcast to set tracking devices.

224. The identical “domain” “media.mtvnservices.com,” provided the Defendants data management capabilities without limitation of the “same-origin security policy.” This is an invitation for cross-site mayhem involving crossdomain.xml. Using actionscript dynamic applications have broad capabilities to load code and data over the Internet. Entities allowed to bypass the web

1 browser's same-origin security policy allows one domain to read data or code  
2 hosted on another.

3 **H. "flashcookie", "/movies/mymovie.swf" (VPPA Defendants)**

4 225. Flash media player does not require permission from the user for  
5 flash content, i.e. movies/video to store data locally, thus permission to access  
6 content from the same origin that the user has provided permission, grants broader  
7 powers, such as to any content allowed by the crossdomain.xml file, in addition to  
8 the use of identical domain by Defendant Quantcast and Defendants Quantcast  
9 Flash Cookie Affiliates.

10 226. Flash cookie data regarding audio visual material downloaded from  
11 VPPA Defendants' websites, and viewed by Plaintiffs and Class members was  
12 saved within their LSO. While the localpath content helps to organize this option,  
13 it was possible without it by storing all user data in one (1) LSO readable by any  
14 page on that domain.

15 [http://kb2.adobe.com/cps/161/tn\\_16194.html](http://kb2.adobe.com/cps/161/tn_16194.html)

16 **Creating the Shared Object**

17 "Create a Shared Object with the getLocal method of Shared Object.

18 The movie above sets a variable (myLocalSO) and assigns a Shared  
19 Object with the name of "flashcookie" with the following

20 **ActionScript:**

21 `//create the local Shared Object myLocal_so =`  
22 `sharedobject.getLocal("flashcookie");`

23 If a Shared Object with the name "flashcookie" does not already exist,  
24 then the Macromedia Flash Player will create a Shared Object with  
25 that name.

26 An optional parameter called localPath can also be specified for the  
27 Shared Object. This localPath parameter allows some control over  
28 where the Shared Object is stored on the client machine. This path

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

match or be contained within the URL that the SWF came from. Therefore, if the movie that creates the Shared Object on the client machine is at `http://www.mydomain.com/movies/mymovie.swf` then the `localPath` parameter can be set to `http://www.mydomain.com/movies/mymovie.swf`, `/movies`, or `/movies/mymovie.swf`.

The code would look like this:

```
myLocal_so =  
sharedobject.getLocal("flashcookie", "/movies/mymovie.swf");
```

This is useful when more than one local Shared Object is used on a site. For instance, all movies from a certain domain can access a user name stored in a local Shared Object created at the root level (set the `localPath` to `"/"`) while other information specific to an individual movie can be stored in a Shared Object whose `localPath` parameter is specific to that movie (set the `localPath` to `"/movies/mymovie.swf"`). Set the value of the Shared Object Information is stored in the Shared Object by assigning attributes to the `data` property of the Shared Object. In the above movie, the user name entered in the text field is stored in the Shared Object by assigning a `name` attribute to the `data`

Cookie Name	Date Created/ Changed	Size	Path	User ID	Domain
-------------	-----------------------	------	------	---------	--------

property of the local shared object and setting it equal to the contents of the text field as follows:

1		10/12/2009	60	C:\Users\Owner\AppData	N2A	media.mtvu.com\[[IM
2	<a href="http://media.mtvu.com">http://media.mtvu.com</a>	4:33:28 PM		Data\Roaming\Macro	MUE	PORT]]\media.mtvns
3	<a href="http://media.mtvu.com">a.mtvu.co</a>	10/28/2009		media\Flash	DE	ervices.com
4	<a href="http://media.mtvu.com">m/[[IMPO</a>	10:14:43 PM		Player\#SharedObject		
5	<a href="http://media.mtvu.com">RT]]/medi</a>			s\		
6	<a href="http://media.mtvnservices.com">a.mtvnserv</a>					
7	<a href="http://media.mtvnservices.com">ices.com/p</a>					
8	<a href="http://media.mtvnservices.com">layer/rea</a>					
9	<a href="http://media.mtvnservices.com">se DownS</a>					
10	<a href="http://media.mtvnservices.com">hiftHistory</a>					
11	<a href="http://media.mtvnservices.com">.sol</a>					

//set the variable "name" equal to the text property //of the  
 textfield"userName" myLocal\_so.data.name = userName.text;

//increase the variable counter by one for each visit  
 myLocal\_so.data.counter++;

The data is written to the Shared Object when the movie is removed  
 from the Macromedia Flash Player. To write the data immediately the  
 methodflushcan be used as follows:

myLocal\_so.flush();

Return the value of the Shared Object When a user returns to the page  
 the Shared Object is read and its values are displayed.

userName.text = myLocal\_so.data.name; numVisits.text = "You have  
 been here " + myLocal\_so.data.counter +" times."

Because the Shared Object "flashcookie" has already been created on  
 the client machine,myLocalSO =

sharedobject.getLocal("flashcookie");will get the data from the Shared  
 Object, which can be used to display the user name and number of  
 visits.”

1           227. Such vulnerabilities provided the Defendants the method and means  
2 to perpetrate its scheme, made the basis of this action, which will include  
3 anticipated discovery, related in part, to additional flash cookies forensics located  
4 on Class representative Edward Valdez’s computer:

5           I. Personal Identifying Information

6                   “We see that people are getting more and more privacy aware lately,  
7 which is important as cookie use is spiraling out of control. While this  
8 increases the demand for cookie managing software, browsers  
9 supporting the new web standard HTML5 will, in the further future,  
10 definitely bring a change; and in my opinion render Flash useless. On  
11 the other hand, new plug-ins will emerge and with a tighter coupling  
12 of online and offline information, could make keeping one's privacy  
13 more and more difficult.”

14                   Jenkins, George. “A Conversation with Jens Muller, CTO at Maxa  
15 Research.” I’ve Been Mugged. (June 10, 2010)

16                   [http://ivebeenmugged.typepad.com/my\\_weblog/2010/06/interview-  
17 jens-muller.html](http://ivebeenmugged.typepad.com/my_weblog/2010/06/interview-jens-muller.html)

18           228. Defendants’ interception of electronic communications, while  
19 Plaintiffs and Class members visited non-Quantcast Flash Cookie Affiliate  
20 websites, provided personal identifying information. A user’s actions on two  
21 websites that work with the same advertising network - like logging into a social  
22 network in one site and buying a book in another – can be cross-referenced by  
23 Defendants to learn more about the user and create a profile about his or her  
24 online habits. This would allow any entity with access to that LSO to know of the  
25 viewing interests and habits of the user. The names of the audio visual materials  
26 viewed can be stored in clean text in the LSO, in addition to, user ID, and any  
27 additional user data, albeit allegedly anonymized.

28           229. Some Quantcast Flash Cookie Affiliates required users that registered

1 as a member to provide their name and email address, but most required date of  
2 birth, gender, and zip code, thus providing Quantcast access to uniquely  
3 indentifying personal information of Quantcast Flash Cookie Affiliate users. There  
4 are well reported occurrences of de-anonymization of databases including, but not  
5 limited to: the “Massachusetts Data Release,” wherein The Massachusetts Group  
6 Insurance Commission release of state hospital records was re-anonymized by  
7 using 1990 census data that showed 87% (216 million of 248 million) of the  
8 United States population reported characteristics that made them uniquely  
9 identifiable using only three pieces of data: 5-digit ZIP, gender, date of birth, fifty-  
10 three percent of the U.S. population could be uniquely identified using only  
11 gender, location (city, town, or municipality), and date of birth, and at the county  
12 level approximately 18% of the U.S. population could be uniquely identified. L.  
13 Sweeney. Uniqueness of Simple Demographics in the U.S. Population, LIDAP-  
14 WP4. Carnegie Mellon University, Laboratory for International Data Privacy,  
15 Pittsburgh, PA: 2000 (available at

16 <http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html>)

17 230. “In our analysis of anonymized data from around half a million  
18 distinct browsers, 84% had unique configurations. Among browsers that had Flash  
19 or Java installed, 94% were unique, and only 1% had fingerprints that were seen  
20 more than twice. However, our experiment only studied a limited number of  
21 variables, and the companies that offer specialized fingerprinting services are  
22 likely to use a wider and therefore more powerful range of measurements.”

23 <https://panopticlick.eff.org/browser-uniqueness.pdf>

24 **J. Flash Cookie Vulnerability**

25 “Thoughts on Flash,” Steve Jobs (April 2010)  
26 Symantec recently highlighted Flash for having one of the worst  
27 security records in 2009. We also know first hand that Flash is the  
28 number one reason Macs crash.

1 <http://www.apple.com/hotnews/thoughts-on-flash/>

2 231. Symantec Global Internet Security Threat Report Trends for 2009  
3 Volume XV, Published April 2010

4 Of the top-attacked vulnerabilities that Symantec observed in 2009,  
5 four of the top five being exploited were client-side vulnerabilities  
6 that were frequently targeted by Web-based attacks (table 2). Two of  
7 these vulnerabilities were in Adobe.

- 8 • National Cyber Alert System Technical Cyber Security Alert TA10-  
9 159A Adobe Flash, Reader, and Acrobat Vulnerability Original  
10 release date: June 08, 2010 Last revised: June 11, 2010 Source: US-  
11 CERT <http://www.us-cert.gov/cas/techalerts/TA10-159A.html>

12 Overview

13 According to Adobe, there is a vulnerability in Adobe Flash. This  
14 vulnerability affects Flash Player, Reader, Acrobat, and possibly other  
15 products that support Flash. A remote attacker could exploit this  
16 vulnerability to execute arbitrary code.”

#### 17 K. Defendants’ Business Practices

18 Signaling frustration over privacy issues, Americans are inclined  
19 toward strict punishment of information offenders. 70% suggest that a  
20 company should be fined more than the maximum amount suggested  
21 (\$2,500) “if a company purchases or uses someone’s information  
22 illegally.

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

26 232. Defendant Quantcast’s activities with Quantcast Flash Cookie  
27 Affiliates occurred throughout the United States. They have secretly obtained  
28 personal and private information from Plaintiffs and the Class - a course of action



1 and a body of information that is protected from interception, access, and  
2 disclosure by federal law.

3 233. Defendants used, interfered with, and intermeddled with Class  
4 members' ownership of their personal property, namely, their computers, by,  
5 directly or indirectly, secretly depositing cookies on their computers, secretly  
6 accessing their computers to obtain information contained in and enabled by the  
7 cookie, and secretly collecting personal data and information regarding each Class  
8 members' Internet surfing habits contained in electronic storage on his/her  
9 computer.

10 234. At all relevant times, Defendants' advertising technology has  
11 contained secret information-gathering capacities that were not disclosed to or  
12 known by Plaintiffs or the Class and which permitted Defendants to  
13 surreptitiously, in an unauthorized manner, and for tortious and unlawful  
14 purposes, intercept and access Plaintiffs' and the Class members' personal and  
15 private information, monitor their Internet activity, and create detailed personal  
16 profiles based on such information.

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

26 236. Defendants have used those cookies and other surreptitious data-  
27 collection methods to secretly intercept and access computer users' personal data  
28 and web browsing habits and have transmitted this information to Defendants for

1 their own commercial benefit.

2 237. Defendants collected and/or disclosed covered information of Class  
3 members about all or substantially all of their online activity, including across  
4 websites.

5 238. Defendant Quantcast did not only engage in online tracking and  
6 profiling activities, but further boasts on its website that due to the depth and  
7 breadth of the online profiles of Internet users that it surreptitiously compiles and  
8 creates, it is able to create detailed, user-specific behavioral profiles of the Internet  
9 users.

10 239. Defendant Quantcast's profiling, and tracking technologies, coupled  
11 with its behavioral data compilation tools, allowed Internet website publishers and  
12 advertisers to target Class members based on personal profiling and data  
13 collection technology.

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

28 241. Defendants failed to disclose that its applied technologies also

1 provide Defendants with the ability to surreptitiously intercept, access, and collect  
2 electronic communications and information from unsuspecting Internet users –  
3 including Plaintiffs and the Class. This sensitive information may include such  
4 things as what the web user looked at and what he/she bought, the materials  
5 he/she read, details about his/her financial situation, his/her sexual preference,  
6 health conditions and even more specific information like his/her name, home  
7 address, e-mail address and telephone number.

8         242. Defendants intercepted Class members' electronic communications  
9 for the purpose of committing a tortious or criminal act, and violated the  
10 constitutional rights of Plaintiffs and Class members.

11         243. Defendants failed to post clearly and conspicuously on their website,  
12 including but not limited to the following:

- 13             a. The identity of the covered entity collecting the covered information.
- 14             b. A description of any covered information collected by the covered  
15             entity.
- 16             c. How the covered entity collects covered information.
- 17             d. The specific purposes for which the covered entity collects and uses  
18             covered information.
- 19             e. How the covered entity stores covered information.
- 20             f. How the covered entity may merge, link, or combine covered  
21             information collected about the individual with other information  
22             about the individual that the covered entity may acquire from  
23             unaffiliated parties.
- 24             g. How long the covered entity retains covered information in  
25             identifiable form.
- 26             h. How the covered entity disposes of or renders anonymous covered  
27             information after the expiration of the retention period.
- 28             i. The purposes for which covered information may be disclosed, and

1 the categories of unaffiliated parties who may receive such  
2 information for each such purpose.

- 3 j. The choice and means the covered entity offers individuals to limit or  
4 prohibit the collection and disclosure of covered information, in  
5 accordance with this section.
- 6 k. The means by and the extent to which individuals may obtain access  
7 to covered information that has been collected by the covered entity in  
8 accordance with this section.
- 9 l. A means by which an individual may contact the covered entity with  
10 any inquiries or complaints regarding the covered entity's handling of  
11 covered information.
- 12 m. The process by which the covered entity notifies individuals of  
13 material changes to its privacy notice.
- 14 n. A hyperlink to or a listing of the Federal Trade Commission's online  
15 consumer complaint form or the toll-free telephone number for the  
16 Commission's Consumer Response Center.

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

20 245. In no case as alleged in this complaint, was adequate, informed notice  
21 provided to any class member of the true nature and function of the Defendant's  
22 service.

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

26 247. In no case was the collection of all Internet communication data of  
27 the consumer halted or affected in any way. All data was still collected. The 'opt  
28 out' only affected what advertisements the consumer was shown. Thus, the

1 provision of the opportunity for opting out was, itself, totally misleading.

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

10 249. Defendants did not obtain consent from Plaintiffs and Class members  
11 for any collection or use of their data and was not allowed to decline consent at  
12 the time such statement was presented to the Class members.

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

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

22 252. Defendant intentionally accessed Plaintiffs and Class members'  
23 computers without authorization or exceeded authorized access to obtain  
24 information from protected computers involved in interstate communications.

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

28 254. At all relevant times, Plaintiffs and Class Members' personal and

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

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

14 256. Defendants intentionally intercepted, endeavored to intercept, or  
15 procured another person to intercept or endeavor to intercept the electronic  
16 communication of Plaintiffs and Class members.

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

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

27 259. Defendants caused harm and damages to Plaintiffs and Class  
28 members' computers finite resources, depleted and exhausted its memory, thus

1 causing an actual inability to use it for its intended purposes, and significant  
2 unwanted CPU activity, disk usage, and network traffic resulting in instability  
3 issues, such as applications freezing, failure to boot, and system-wide crashes.

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

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

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

20 263. Defendants harmed Plaintiffs and Class members by its actions which  
21 included, but were not limited to, the following:

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

1 information.

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

10 L. All Eyes On Flash

11 265. “All Eyes on Privacy at FTC Event” (January 29, 2010):

12 “At the Federal Trade Commission's second public discussion about  
13 online privacy in Berkeley, California yesterday, panelists discussed  
14 the ways that digital-era technologies impact individuals' privacy and  
15 what can be done about it, the San Francisco Chronicle reports.  
16 Experts explored Flash cookies, behavioral advertising, data  
17 matching, inadvertent sharing and other topics, and proposed solutions  
18 such as stricter regulations, greater oversight of third-party application  
19 developers and mandatory notice requirements.”

20 266. “Congressman Close to Introducing Privacy Bill” (January 29, 2010):

21 “Representative Rick Boucher (D-VA) is close to introducing a  
22 privacy bill to the House of Representatives that is focused on opt-  
23 in/opt-out requirements for collecting data from Internet users. Our  
24 goal in doing this is to enhance the confidence that Internet users have  
25 that their experience on the Web is secure. [Bill is without a private  
26 cause of action.]

27 [https://www.privacyassociation.org/publications/2010\\_01\\_29\\_congressman\\_close\\_to\\_introducing\\_privacy\\_bill/](https://www.privacyassociation.org/publications/2010_01_29_congressman_close_to_introducing_privacy_bill/)  
28



1 267. Adobe's Comments:

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

5 [http://www.ftc.gov/os/comments/privacyroundtable/544506-](http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf)  
6 [00085.pdf](http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf)

7 When asked to choose what, if anything should be a company's  
8 single punishment beyond fines if it uses a person's information  
9 illegally, 38% of Americans answer that the company should fund  
10 efforts to help people protect privacy. But over half of Americans  
11 adults are far tougher: 18% choose that the company should be put  
12 out of business and 35% select that executives who are responsible  
13 should face jail time.

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

## 18 **CLASS ALLEGATIONS**

### 19 **Allegations as to Class Certification**

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

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

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

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

12          269. The class action period, (the “Class Period”), pertains to the date, two  
13          years preceding the date of this filing to the date of this filing, that a person  
14          residing in the United States, that accessed a Quantcast Flash Cookie Affiliate  
15          website, and a flash cookie was set on their computer to use its local storage  
16          within the flash media player to back up browser cookies for the purposes of  
17          restoring them later.

18          270. Pursuant to Federal Rule of Civil Procedure 23(a), (b)(1), (b)(2), and  
19          (b)(3), Plaintiffs bring this class action, on behalf of themselves and the following  
20          classes with respect to Plaintiffs’ claims for violation of the:

- 21           a) Computer Fraud and Abuse Act (CFAA),
- 22           b) Electronic Communications Privacy Act (ECPA),
- 23           c) California’s Computer Crime Law, (CCCL),
- 24           d) Civil Conspiracy, and
- 25           e) Unjust Enrichment against ALL DEFENDANTS:

26                   All persons residing in United States who, during the period of  
27                   July 1, 2008 to July 1, 2010 (the “Class Period”), accessed a  
28                   Quantcast Flash Cookie Affiliate website and a flash cookie was

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

set on their computer to use its local storage within the flash media player to back up browser cookies for the purposes of restoring them later.

(hereinafter referred to as “CFAA/ ECPA/CCCL Subclass.”)

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

- a) Video Privacy Protection Act
- b) California’s Computer Crime Law (CCCL),
- c) California’s Invasion of Privacy Act, against DEFENDANT

QUANTCAST, ALONE:

All persons residing in United States who, during the period of July 1, 2008 to July 1, 2010 (the “Class Period”), accessed a Quantcast Flash Cookie Affiliate website and a flash cookie was set on their computer to use its local storage within the flash media player to back up browser cookies for the purposes of restoring them later.

(hereinafter referred to as “Quantcast Subclass.”)

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

Video Privacy Protection Act (“VPPA”), against DEFENDANTS MYSPACE, ABC, ESPN, HULU, JIBJAB, MTV, NBC, AND DOES 1-20 (hereinafter referred to as “VPPA Defendants”):

All persons residing in United States who, during the period of July 1, 2008 to July 1, 2010 (the “Class Period”), accessed one or more of the VPPA Defendants’ website and a flash cookie

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

was set on their computer to use its local storage within the flash media player to back up browser cookies for the purposes of restoring them later.

(hereinafter referred to as “VPPA Subclass”)

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

- a) California’s Invasion of Privacy Act, against DEFENDANTS MYSFACE, HULU, JIBJAB, SCRIBD, and DOES 21-50 (hereinafter referred to as California Defendants):

All persons residing in United States who, during the period of July 1, 2008 to July 1, 2010 (the “Class Period”), accessed one or more of the California Defendants’ website and a flash cookie was set on their computer to use its local storage within the flash media player to back up browser cookies for the purposes of restoring them later.

(hereinafter referred to as “California Defendants Subclass”)

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

- a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- b) Electronic Communications Privacy Act, 18 U.S.C. § 2510;
- c) Video Privacy Protection Act, 18 U.S.C. § 2710;
- d) California’s Computer Crime Law, Penal Code § 502;
- e) California Invasion Of Privacy Act, California Penal Code § 630;
- f) Civil Conspiracy;
- g) Unjust Enrichment

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

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

11           277. Plaintiffs reserve the right to revise these class definitions of the  
12 classes based on facts they learn during discovery.

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

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

- 26           a) What was the extent of Quantcast and Quantcast Flash Cookie  
27           Affiliates' business practice of setting a flash cookie on a user's  
28           computer to use its local storage within the flash media player to

1 back up browser cookies for the purpose of restoring them later  
2 and how did it work?

- 3 b) What information did Quantcast and Quantcast Flash Cookie  
4 Affiliates' collect from its business practices of setting a flash  
5 cookie on a user's computer to use its local storage within the flash  
6 media player to back up browser cookies for the purpose of  
7 restoring them later, and what did it do with that information?
- 8 c) Whether Quantcast Flash Cookie Affiliate users, by virtue of their  
9 visitation to Quantcast Flash Cookie Affiliate's website, had pre-  
10 consented to the operation of Quantcast and Quantcast Flash  
11 Cookie Affiliates' business practices of setting a flash cookie on a  
12 user's computer to use its local storage within the flash media  
13 player to back up browser cookies for the purpose of restoring  
14 them later;
- 15 d) Was there adequate notice, or any notice, of the operation of  
16 Quantcast and Quantcast Flash Cookie Affiliates' business  
17 practices of setting a flash cookie on a user's computer to use its  
18 local storage within the flash media player to back up browser  
19 cookies for the purpose of restoring them later provided to  
20 Quantcast and Quantcast Flash Cookie Affiliates' users?
- 21 e) Was there reasonable opportunity to decline the operation of  
22 Quantcast and Quantcast Flash Cookie Affiliates' business  
23 practices of setting a flash cookie on a user's computer to use its  
24 local storage within the flash media player to back up browser  
25 cookies for the purpose of restoring them later provided to  
26 Quantcast and Quantcast Flash Cookie Affiliates' users?
- 27 f) Did Quantcast and Quantcast Flash Cookie Affiliates' business  
28 practices of setting a flash cookie on a user's computer to use its

1 local storage within the flash media player to back up browser  
2 cookies for the purpose of restoring them later disclose, intercept,  
3 and transmit personally identifying information, or sensitive  
4 identifying information, or personal information?

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

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

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

26 j) Did the operation, function, and/or implementation of Quantcast  
27 and Quantcast Flash Cookie Affiliates' business practices of  
28 setting a flash cookie on a user's computer to use its local storage

1 within the flash media player to back up browser cookies for the  
2 purpose of restoring them later violate the Electronic  
3 Communications Privacy Act, 18 U.S.C. § 2510?

4 k) Did the operation, function, and/or implementation of Quantcast  
5 and VPPA Defendants' business practices of setting a flash cookie  
6 on a user's computer to use its local storage within the flash media  
7 player to back up browser cookies for the purpose of restoring  
8 them later violate the Video Privacy Protection Act, 18 U.S.C. §  
9 2710?

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

16 m) Did the operation, function, and/or implementation of Quantcast  
17 and Quantcast Flash Cookie Affiliates' business practices of  
18 setting a flash cookie on a user's computer to use its local storage  
19 within the flash media player to back up browser cookies for the  
20 purpose of restoring them later violate the California Invasion of  
21 Privacy Act, California Penal Code § 630?

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

28 1. Are the Defendants Quantcast and/or Quantcast Flash Cookie



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

- Affiliates liable under a theory of civil conspiracy for violations of the statutes listed herein?
2. Are the Defendants Quantcast and/or Quantcast Flash Cookie Affiliates liable under a theory of unjust enrichment for violations of the statutes listed herein?
  3. Whether Quantcast and Quantcast Flash Cookie Affiliates participated in and/or committed or is responsible for violation of law(s) complained of herein;
  4. Are Class members entitled to damages as a result of the implementation of Quantcast and Quantcast Flash Cookie Affiliates' marketing scheme, and, if so, what is the measure of those damages?
  5. Whether Plaintiffs and members of the Class have sustained damages as a result of Defendants' conduct, and, if so, what is the appropriate measure of damages;
  6. Whether Plaintiffs and members of the Class are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and
  7. Whether Plaintiffs and members of the Class are entitled to punitive damages, and, if so, in what amount.

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

281. Adequacy of Representation: Plaintiffs will fairly and adequately protect the interests of the members of the Class. Plaintiffs have retained counsel highly experienced in complex consumer class action litigation, and Plaintiffs

1 intend to prosecute this action vigorously. Plaintiffs have no adverse or  
2 antagonistic interests to those of the Class.

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

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

- 19       a) the prosecution of separate actions by individual Class members  
20       would create a risk of inconsistent or varying adjudication with  
21       respect to individual Class members that would establish  
22       incompatible standards of conduct for the Defendants;
- 23       b) the prosecution of separate actions by individual Class members  
24       would create a risk of adjudications with respect to them that  
25       would, as a practical matter, be dispositive of the interests of other  
26       Class members not parties to the adjudications, or substantially  
27       impair or impede their ability to protect their interests; and/or  
28       c) Defendants have acted or refused to act on grounds generally

1 applicable to the Class thereby making appropriate final  
2 declaratory and/or injunctive relief with respect to the members of  
3 the Class as a whole.

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

8 285. Quantcast Flash Cookie Affiliates websites. The claims asserted  
9 herein are based on Federal law and California law, which is applicable to all  
10 Class members throughout the United States.

11 286. Adequate notice can be given to Class members directly using  
12 information maintained in Defendants' records, or through notice by publication.

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

## 17 **Count I**

### 18 **Violation of the Computer Fraud and Abuse Act**

19 **18 U.S.C. § 1030 et. seq.**

20 **Against All Defendants**

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

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

25 290. The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, referred to as  
26 "CFAA," regulates fraud and relates activity in connection with computers, and  
27 makes it unlawful to intentionally access a computer used for interstate commerce  
28 or communication, without authorization or by exceeding authorized access to

1 such a computer, thereby obtaining information from such a protected computer,  
2 within the meaning of U.S.C. § 1030(a)(2)(C).

3 291. Defendants violated 18 U.S.C. § 1030 by intentionally accessing a  
4 Plaintiffs' computer, without authorization or by exceeding access, thereby  
5 obtaining information from such a protected computer.

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

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

15 294. Plaintiffs' computers are "protected computer[s]...which are used in  
16 interstate commerce and/or communication" within the meaning of 18 U.S.C. §  
17 1030(e)(2)(B).

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

21 296. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly  
22 causing the transmission of a command embedded within their webpages,  
23 downloaded to Plaintiffs' computers, which are protected computers as defined in  
24 18 U.S.C. § 1030(e)(2)(B). By accessing, collecting, and transmitting Plaintiffs'  
25 viewing habits, Defendants intentionally caused damage without authorization to  
26 those Plaintiffs' computers by impairing the integrity of the computers.

27 297. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(ii) by intentionally  
28 accessing Plaintiffs' and Class members' protected computers without

1 authorization, and as a result of such conduct, recklessly caused damage to  
2 Plaintiffs' and Class members' computers by impairing the integrity of data and/or  
3 system and/or information.

4 298. Defendants violated 18 U.S.C. § 1030(a)(5)(A)(iii) by intentionally  
5 accessing Plaintiffs' and Class members' protected computers without  
6 authorization, and as a result of such conduct, caused damage and loss to Plaintiffs  
7 and Class members.

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

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

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

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

25 303. Plaintiffs and Class members have additionally suffered loss by  
26 reason of these violations, including, without limitation, violation of the right of  
27 privacy.

28 304. Defendants' unlawful access to Plaintiffs' computers and electronic

1 communications has caused Plaintiffs irreparable injury. Unless restrained and  
2 enjoined, Defendants will continue to commit such acts. Plaintiffs' remedy at law  
3 is not adequate to compensate it for these inflicted and threatened injuries,  
4 entitling Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C.  
5 § 1030(g).

## 6 **COUNT II**

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

#### 8 **18 U.S.C. §2510**

#### 9 **Against All Defendants**

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

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

14 307. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §  
15 2510, referred to as "ECPA," regulates wire and electronic communications  
16 interception and interception of oral communications, and makes it unlawful for  
17 a person to "willfully intercept[], endeavor[] to intercept, or procure[] any other  
18 person to intercept or endeavor to intercept, any wire, oral, or electronic  
19 communication," within the meaning of 18 U.S.C. § 2511(1).

20 308. Defendants violated 18 U.S.C. § 2511 by intentionally acquiring  
21 and/or intercepting, by device or otherwise, Plaintiffs' and Class members'  
22 electronic communications, without knowledge, consent, or authorization.

23 309. The contents of data transmissions from and to Plaintiffs' and Class  
24 Members' personal computers constitute "electronic communications" within the  
25 meaning of 18 U.S.C. §2510.

26 310. Plaintiffs are "person[s] whose ... electronic communication is  
27 intercepted ... or intentionally used in violation of this chapter" within the  
28 meaning of 18 U.S.C. § 2520.

1           311. Defendants violated 18 U.S.C. § 2511(1)(a) by intentionally  
2 intercepting, endeavoring to intercept, or procuring any other person to intercept  
3 or endeavor to intercept Plaintiffs’ electronic communications.

4           312. Defendants violated 18 U.S.C. § 2511(1)(c) by intentionally  
5 disclosing, or endeavoring to disclose, to any other person the contents of  
6 Plaintiffs’ electronic communications, knowing or having reason to know that the  
7 information was obtained through the interception of Plaintiffs’ electronic  
8 communications.

9           313. Defendants violated 18 U.S.C. § 2511(1)(d) by intentionally using, or  
10 endeavoring to use, the contents of Plaintiffs’ electronic communications,  
11 knowing or having reason to know that the information was obtained through the  
12 interception of Plaintiffs’ electronic communications.

13           314. Defendants’ intentional interception of these electronic  
14 communications without Plaintiffs’ or Class Members’ knowledge, consent, or  
15 authorization was undertaken without a facially valid court order or certification.

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

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

23           317. The Electronic Communications Privacy Act of 1986, 18 USC  
24 §2520(a) provides a civil cause of action to “any person whose wire, oral, or  
25 electronic communication is intercepted, disclosed, or intentionally used” in  
26 violation of the ECPA.

27           318. Defendants are liable directly and/or vicariously for this cause of  
28 action. Plaintiffs therefore seek remedy as provided for by 18 U.S.C. §2520,

1 including such preliminary and other equitable or declaratory relief as may be  
2 appropriate, damages consistent with subsection (c) of that section to be proven at  
3 trial, punitive damages to be proven at trial, and a reasonable attorney's fee and  
4 other litigation costs reasonably incurred.

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

8 320. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to  
9 preliminary, equitable, and declaratory relief, in addition to statutory damages of  
10 the greater of \$10,000 or \$100 a day for each day of violation, actual and punitive  
11 damages, reasonable attorneys' fees, and Defendants' profits obtained from the  
12 above-described violations. Unless restrained and enjoined, Defendants will  
13 continue to commit such acts. Plaintiffs' remedy at law is not adequate to  
14 compensate it for these inflicted and threatened injuries, entitling Plaintiffs to  
15 remedies including injunctive relief as provided by 18 U.S.C. § 2510.

16  
17 **Count III**

18 **Violations of the Video Privacy Protection Act**

19 **18 U.S.C. § 2710**

20 **Against MySpace, ABC, ESPN, Hulu, JibJab, MTV, and NBC (hereinafter**  
21 **"VPPA Defendants")**

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

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

26 323. The Video Privacy Protection Act, 18 U.S.C. § 2710, referred to as  
27 "VPPA," regulates disclosure of video tape rental or sale records.

28 324. The Video Privacy Protection Act, 18 U.S.C. § 2710, makes it



1 unlawful for a video service provider to “knowingly disclose[s] personally  
2 identifiable information concerning any consumer of such provider.”

3 325. The VPPA Defendants violated 18 U.S.C. § 2710 by knowingly  
4 disclosing Plaintiffs’ and Class Members’ personally identifiable information to  
5 Quantcast.

6 326. As defined in 18 U.S.C. § 2710(a)(3), “personally identifiable  
7 information” “identifies a person as having requested or obtained specific video  
8 materials or services from a video tape service provider.”

9 327. As defined in 18 U.S.C. § 2710(a)(4), a “video tape service provider”  
10 is “any person, engaged in the business, in or affecting interstate or foreign  
11 commerce, of rental, sale or delivery of prerecorded video cassette tapes or similar  
12 audiovisual materials.”

13 328. Each of the VPPA Defendants is a “video tape service provider”  
14 within the meaning of 18 U.S.C. § 2710(a)(4) because each VPPA Defendant is a  
15 person, engaged in the business, in or affecting interstate or foreign commerce, of  
16 rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual  
17 materials as defined by the Act.

18 329. Each of the VPPA Defendants violated 18 U.S.C. § 2710(b)(1) by  
19 knowingly disclosing personally identifiable information concerning each user to  
20 Quantcast without the consent of the user. Each of the VPPA Defendants  
21 knowingly consented to the operation of the marketing program on their website  
22 and affirmatively incorporated special script that activated the marketing program  
23 and its communications to Quantcast when the website was visited by the user.

24 330. Each of the VPPA Defendants violated 18 U.S.C. § 2710(b)(1) by  
25 knowingly providing personally identifiable information within the meaning of 18  
26 U.S.C. § 2710(a)(3) as the information communicated to Quantcast includes  
27 information which identifies a person as having requested or obtained specific  
28 audiovisual materials or services from a VPPA Defendant.



1 referred to as “CCCL” regulates “tampering, interference, damage, and  
2 unauthorized access to lawfully created computer data and computer systems.”

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

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

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

17 341. Pursuant to California Penal Code § 502(b)(8), “Injury means any  
18 alteration, deletion, damage, or destruction of a computer system, computer  
19 network, computer program, or data caused by the access, or the denial of access  
20 to legitimate users of a computer system, network, or program.”

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

1 other fashion usurp the normal operation of the computer, computer system, or  
2 computer network.”

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

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

12 345. Defendants have violated California Penal Code § 502(c)(3) by  
13 knowingly and without permission, using and causing to be used Plaintiffs’  
14 computer services.

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

18 347. Defendants have violated California Penal Code § 502(c)(5) by  
19 knowingly and without permission, disrupting or causing the disruption of  
20 Plaintiffs’ computer services or denying or causing the denial of computer  
21 services to Plaintiffs.

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

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

28 350. Defendants have violated California Penal Code § 502(c)(8) by

1 knowingly introducing a computer contaminant into the Plaintiffs' computer,  
2 computer system and/or computer network to obtain data regarding Plaintiffs'  
3 electronic communications.

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

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

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

18 354. As a direct and proximate result of Defendants' unlawful conduct  
19 within the meaning of California Penal Code § 502, Defendants have caused loss  
20 to Plaintiffs in an amount to be proven at trial. Plaintiffs are also entitled to  
21 recover their reasonable attorneys' fees pursuant to California Penal Code §  
22 502(e).

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

25 356. Plaintiffs and Class Members have suffered irreparable and  
26 incalculable harm and injuries from Defendant's violations. The harm will  
27 continue unless Defendant is enjoined from further violations of this section.  
28 Plaintiffs and Class Members have no adequate remedy at law.



1           conspires with any person or persons to unlawfully do, or permit, or  
2           cause to be done any of the acts or things mentioned above in this  
3           section, is punishable . . .

4           362.    On information and belief, each Plaintiff, and each Class Member,  
5           during one or more of their interactions on the Internet during the Class Period,  
6           communicated with one or more web entities based in California, or with one or  
7           more entities whose servers were located in California.

8           363.    Communications from the California web-based entities to Plaintiffs  
9           and Class Members were sent from California. Communications to the California  
10          web-based entities from Plaintiffs and Class Members were sent to California.

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

14          365.    Plaintiffs and Class Members did not consent to any of the  
15          Defendants’ actions in using the contents of their communications with such  
16          California-based entities.

17          366.    Defendants are not a “ public utility engaged in the business of  
18          providing communications services and facilities . . .”

19          367.    The actions alleged herein by the Defendants were not undertaken:  
20          “for the purpose of construction, maintenance, conduct or operation of the  
21          services and facilities of the public utility.”

22          368.    The actions alleged herein by the Defendants were not undertaken in  
23          connection with: “the use of any instrument, equipment, facility, or service  
24          furnished and used pursuant to the tariffs of a public utility.

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

28          370.    The Defendants directly participated in the interception, reading,

1 and/or learning the contents of the communications between plaintiffs, Class  
2 Members and California-based web entities.

3 371. Alternatively, and of equal violation of the California Invasion of  
4 Privacy Act, the Defendants aided, agreed with, and/or conspired with Quantcast  
5 to unlawfully do, or permit, or cause to be done all of the acts complained of  
6 herein.

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

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

## 17 **COUNT VI**

### 18 **Violations of the Unfair Competition Law (“UCL”)California** 19 **Business and Professions Code § 17200, et seq.**

20 374. Plaintiffs incorporate the foregoing allegations as if fully set forth  
21 herein.

22 375. In violation of California Business and Professions Code § 17200 et  
23 seq., Defendant’s conduct in this regard is ongoing and includes, but is not limited  
24 to, unfair, unlawful and fraudulent conduct.

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



1 fees.

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

9 378. Defendant's business acts and practices are also unlawful in that they  
10 violate the California Consumer Legal Remedies Act, California Civil Code,  
11 Sections 1647, et seq., 1750, et seq., and 3344, California Penal Code,  
12 section 502, and Title 18, United States Code, Section 1030. Defendant is  
13 therefore in violation of the "unlawful" prong of the UCL.

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

28 380. In addition, Defendant's modus operandi constitutes a sharp practice

1 in that Defendant knew, or should have known, that consumers care about the  
2 status of personal information and email privacy but were unlikely to be aware of  
3 the manner in which Defendant failed to fulfill its commitments to respect  
4 consumers' privacy. Defendant is therefore in violation of the "unfair" prong of  
5 the UCL.

6 381. Defendant's acts and practices were fraudulent within the meaning of  
7 the UCL because they are likely to mislead the members of the public to whom  
8 they were directed.

9 382. Plaintiffs, on behalf of themselves and on behalf of each member of  
10 the Class, seek individual restitution, injunctive relief, and other relief allowed  
11 under the UCL as the Court deems just and proper.

## 12 **COUNT VII**

### 13 **Violations of the Consumer Legal Remedies Act** 14 **("CLRA")California Civil Code § 1750, et seq.**

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

17 g. In violation of Civil Code section 1750, et seq. (the "CLRA"),  
18 Defendant has engaged and is engaging in unfair and deceptive acts and practices  
19 in the course of transactions with Plaintiffs, and such transactions are intended to  
20 and have resulted in the sales of services to consumers. Plaintiffs and the Class  
21 Members are "consumers" as that term is used in the CLRA because they sought  
22 or acquired Defendant's good or services for personal, family, or household  
23 purposes. Defendant's past and ongoing acts and practices include but are not  
24 limited to:

25 h. Defendant's representations that its services have  
26 characteristics, uses, and benefits that they do not have, in violation of Civil Code  
27 § 1770(a)(5);

28 i. Defendant's representations that its services are of a particular

1 standard, quality and grade but are of another standard quality and grade, in  
2 violation of Civil Codes § 1770(a)(7); and

3 j. Defendant's advertisement of services with the intent not to  
4 sell those services as advertised, in violation of Civil Code § 1770(a)(9).

5 k. Defendant's violations of Civil Code § 1770 have caused  
6 damage to Plaintiffs and the other Class Members and threaten additional injury if  
7 the violations continue. This damage includes the losses set forth above.

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

13 385. If Defendant fails to respond adequately to Plaintiff's above-  
14 described demand within 30 days of Plaintiff's notice, pursuant to California Civil  
15 Code, Section 1782(b), Plaintiffs will amend the complaint to request damages  
16 and other relief, as permitted by Civil Code, Section 1780.

### 17 **Count VIII**

#### 18 **Unjust Enrichment**

#### 19 **Against All Defendants**

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

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

24 388. A benefit has been conferred upon all Defendants by Plaintiffs and  
25 the Class. On information and belief, Defendants, directly or indirectly, have  
26 received and retain information regarding online communications and activity of  
27 Plaintiffs, and Defendants have received and retain information regarding specific  
28 purchase and transactional information that is otherwise private, confidential, and

1 not of public record, and/or have received revenue from the provision of such  
2 information.

3 389. Defendants appreciate or have knowledge of said benefit.

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

9 **PRAYER FOR RELIEF**

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

- 12 A. Certify this case as a class action on behalf of the Classes defined above,  
13 appoint Plaintiffs as class representatives, and appoint Plaintiff's counsel as  
14 class counsel;
- 15 B. Declare that the actions of Quantcast and Quantcast Flash Cookie Affiliates,  
16 as set out above, violate the following:
- 17 a) Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
  - 18 b) Electronic Communications Privacy Act, 18 U.S.C. § 2510;
  - 19 c) Video Privacy Protection Act, 18 U.S.C. § 2710;
  - 20 d) California's Computer Crime Law, Penal Code § 502;
  - 21 e) California Invasion Of Privacy Act, California Penal Code § 630;
  - 22 f) Civil Conspiracy;
  - 23 g) Unjust Enrichment
- 24 C. As applicable to the Classes mutatis mutandis, awarding injunctive and  
25 equitable relief including, inter alia: (i) prohibiting Quantcast and Quantcast  
26 Flash Cookie Affiliates from engaging in the acts alleged above; (ii)  
27 requiring Quantcast and Quantcast Flash Cookie Affiliates to disgorge all of  
28 its ill-gotten gains to Plaintiffs and the other Class Members, or to

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

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

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

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

21 G. Award Plaintiffs and the Classes:

- 22 a) their reasonable litigation expenses, costs of court, and attorneys'  
23 fees;
- 24 b) pre- and post-judgment interest, to the extent allowable;
- 25 c) restitution, disgorgement and/or other equitable relief as the Court  
26 deems proper;
- 27 d) compensatory damages sustained by Plaintiffs and all others similarly  
28 situated as a result of Defendants' unlawful acts and conduct;

- 1 e) statutory damages, including punitive damages;  
2 f) permanent injunction prohibiting Defendants from engaging in the conduct  
3 and practices complained of herein;  
4 H. For such other and further relief as this Court may deem just and proper.

5  
6 DATED this 23th day of July 2010.



7  
8 By: David Parisi

9 Joseph H. Malley (*pro hac vice* pending)  
10 Law Office of Joseph H. Malley  
11 1045 North Zang Blvd  
12 Dallas, TX 75208  
13 Telephone: (214) 943-6100  
14 Facsimile: (214) 943-6170  
malleylaw@gmail.com

15 David Parisi (Cal. Bar. No. 162248)  
16 Parisi & Havens LLP  
17 15233 Valleyheart Drive  
18 Sherman Oaks, California 91403  
19 Telephone: (818) 990-1299  
Facsimile: (818) 501-7852  
dparisi@parisihavens.com

20  
21  
22  
23  
24  
25  
26  
27  
28

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

JURY TRIAL DEMAND

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

Respectfully submitted,

DATED this 23 th day of July 2010.



By: David C. Parisi

Joseph H. Malley (*pro hac vice* pending)  
Law Office of Joseph H. Malley  
1045 North Zang Blvd  
Dallas, TX 75208  
Telephone: (214) 943-6100  
Facsimile: (214) 943-6170  
malleylaw@gmail.com

David C. Parisi (Cal. Bar. No. 162248)  
Parisi & Havens LLP  
15233 Valleyheart Drive  
Sherman Oaks, California 91403  
Telephone: (818) 990-1299  
Facsimile: (818) 501-7852  
dparisi@parisihavens.com





**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): \_\_\_\_\_

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	California Counties Outside of this District: San Diego County Other States: Texas; New Mexico

(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
Los Angeles	California Counties outside of this district: San Francisco; Palo Alto; San Carlos Other States: New York; Connecticut; Washington

(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	

\* 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 July 23, 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))

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

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

EDWARD VALDEZ; See attachment A for additional  
plaintiffs

CASE NUMBER

PLAINTIFF(S)

**CV10-05484** *GW (JCGX)*

v.

QUANTCAST CORPORATION; See attachment A  
for additional defendants

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: 23 JUL 2010

By: *Shelene Hursey*  
Deputy Clerk

(Seal of the Court)

[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:**

ALAN BONEBRAKE; BYRON GRIFFITH; MARY HUEBNER; JOSE MARQUEZ; BRITTANY SANCHEZ; GERARDO VALDEZ; AUSTIN MUHS; and KAYLA VALDEZ, *individually, on behalf of themselves and others similarly situated,*

**Additional Defendants:**

MYSFACE, INC.; AMERICAN BROADCASTING COMPANIES, INC.; ESPN, INC.; HULU, LLC.; JIBJAB MEDIA, INC.; MTV NETWORKS, INC.; NBC UNIVERSAL, INC.; and SCRIBD, INC.; *Delaware Corporations,*

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

UNITED STATES DISTRICT COURT  
CENTRAL DISTRICT OF CALIFORNIA

EDWARD VALDEZ; See attachment A for additional  
plaintiffs

PLAINTIFF(S)

v.

QUANTCAST CORPORATION; See attachment A  
for additional defendants

DEFENDANT(S).

CASE NUMBER

CV10-05484 EW (JCGX)

SUMMONS

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.

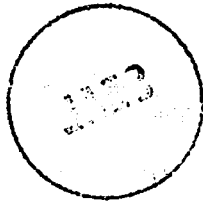
Clerk, U.S. District Court

Dated: 23 JUL 2010

By: [Signature]  
Deputy Clerk  
(Seal of the Court)

[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)].

100-100000



100-100000

**ATTCHMENT A**

Attachment to Summons

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

**Additional Plaintiffs:**

ALAN BONEBRAKE; BYRON GRIFFITH; MARY HUEBNER; JOSE MARQUEZ; BRITTANY SANCHEZ; GERARDO VALDEZ; AUSTIN MUHS; and KAYLA VALDEZ, *Individually, on Behalf of themselves and Others Similarly Situated,*

**Additional Defendants:**

MYSFACE, INC.; AMERICAN BROADCASTING COMPANIES, INC.; ESPN, INC.; HULU, LLC.; JIBJAB MEDIA, INC.; MTV NETWORKS, INC.; NBC UNIVERSAL, INC.; and SCRIBD, INC.; *Delaware Corporations,*