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

I (a) PLAINTIFFS (Check box if you are representing yourself ☐)
EDWARD VALDEZ, ALAN BONEBRAKE, BYRON GRIFFITH, MARY HUEBNER, JOSE MARQUEZ, BRITTANY SANCHEZ, GERARDO VALDEZ, AUSTIN MUHS, and KAYLA VALDEZ

DEFENDANTS
QUANTCAST CORPORATION; MYSPACE, INC.; AMERICAN BROADCASTING COMPANIES, INC.; ESPN, INC.; HULU, LLC.; JIBJAB MEDIA, INC.; MTV NETWORKS, INC.; NBC UNIVERSAL, INC.; SCRIBD, INC.

(b) Attorneys (Firm Name, Address and Telephone Number. If you are representing yourself, provide same.)
David C. Parisi, Suzanne Havens Beckman, Parisi & Havens LLP, 15233 Valleyheart Drive, Sherman Oaks, California 91403, (818) 990-1299

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an X in one box only.)

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☑ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES - For Diversity Cases Only
(Place an X in one box for plaintiff and one for defendant.)

	PTF	DEF		PTF	DEF
Citizen of This State	☑ 1	☐ 1	Incorporated or Principal Place of Business in this State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated and Principal Place of Business in Another State	☐ 5	☑ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. ORIGIN (Place an X in one box only.)

☑ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify): ☐ 6 Multi-District Litigation ☐ 7 Appeal to District Judge from Magistrate Judge

V. REQUESTED IN COMPLAINT: **JURY DEMAND:** ☑ Yes ☐ No (Check 'Yes' only if demanded in complaint.)

CLASS ACTION under F.R.C.P. 23: ☑ Yes ☐ No ☐ **MONEY DEMANDED IN COMPLAINT: $**_____

VI. CAUSE OF ACTION (Cite the U.S. Civil Statute under which you are filing and write a brief statement of cause. Do not cite jurisdictional statutes unless diversity.)
Violation of: (1) 18 U.S.C. § 1030; (2) 18 U.S.C. § 2510; (3) 18 U.S.C. § 2710; (4) California Penal Code § 502; (5) California Penal Code § 630.

VII. NATURE OF SUIT (Place an X in one box only.)

OTHER STATUTES
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce/ICC Rates/etc.
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 810 Selective Service
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 875 Customer Challenge 12 USC 3410
- ☑ 890 Other Statutory Actions
- ☐ 891 Agricultural Act
- ☐ 892 Economic Stabilization Act
- ☐ 893 Environmental Matters
- ☐ 894 Energy Allocation Act
- ☐ 895 Freedom of Info. Act
- ☐ 900 Appeal of Fee Determination Under Equal Access to Justice
- ☐ 950 Constitutionality of State Statutes

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loan (Excl. Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Fed. Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury-Med Malpractice
- ☐ 365 Personal Injury-Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 463 Habeas Corpus-Alien Detainee
- ☐ 465 Other Immigration Actions

TORTS PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

CIVIL RIGHTS
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/Accommodations
- ☐ 444 Welfare
- ☐ 445 American with Disabilities - Employment
- ☐ 446 American with Disabilities - Other
- ☐ 440 Other Civil Rights

PRISONER PETITIONS
- ☐ 510 Motions to Vacate Sentence Habeas Corpus
- ☐ 530 General
- ☐ 535 Death Penalty
- ☐ 540 Mandamus/ Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition

FORFEITURE / PENALTY
- ☐ 610 Agriculture
- ☐ 620 Other Food & Drug
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 630 Liquor Laws
- ☐ 640 R.R. & Truck
- ☐ 650 Airline Regs
- ☐ 660 Occupational Safety /Health
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Mgmt. Relations
- ☐ 730 Labor/Mgmt. Reporting & Disclosure Act
- ☐ 740 Railway Labor Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Empl. Ret. Inc. Security Act

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS-Third Party 26 USC 7609

FOR OFFICE USE ONLY: Case Number: CV10-05484

AFTER COMPLETING THE FRONT SIDE OF FORM CV-71, COMPLETE THE INFORMATION REQUESTED BELOW.

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 PLAINTIFF(S) v. QUANTCAST CORPORATION; See attachment A for additional defendants DEFENDANT(S).	CASE NUMBER CV10-05484 GW (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: _____
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:

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

ATTACHMENT A
Attachment to Summons

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: _____
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:

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

ATTACHMENT A
Attachment to Summons

Joseph H. Malley
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

Counsel for Plaintiffs

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

EDWARD VALDEZ, 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,

Plaintiffs,

v.

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

Defendants.

CASE No. CV10-05484 GAF (JCGx)

JURY DEMAND

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

CLASS ACTION COMPLAINT

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

NATURE OF THE ACTION

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

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

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

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

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

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

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

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

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

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

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

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

d. California's Computer Crime Law, Penal Code § 502 (the "CCCL"), against all Defendants;

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

f. Unjust Enrichment, against all Defendants.

JURISDICTION AND VENUE

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

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

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

a. Quantcast;

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 n 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

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

a. Hulu
b. JibJab
c. MySpace

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

a. ABC
b. Hulu
c. MTV
d. NBC

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

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

a. MTV

b. NBC

c. Scribd

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

a. ESPN

b. Hulu

c. MTV

Cookie Name	Date Created/ Changed	Size	Path	User ID	Domain
http://www.hulu.com BeaconServiceV2.sol	9/11/2009 9:40:16 PM 12/25/2009 3:59:24 PM	300	C:\Users\G. VALDEZ\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\	2LZVE58A	www.hulu.com

http://www.hulu.com com.quantserve.sol	9/11/2009 9:40:24 PM 9/11/2009 9:40:24 PM	72	C:\Users\G. VALDEZ\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\	2LZVE58A	www.hulu.com
Cookie Name	Date Created/ Changed	Size	Path	User ID	Domain
http://media.mtvnservices.com com.quantserve.sol	4/19/2010 5:10:55 PM 4/19/2010 5:10:55 PM	73	C:\Documents and Settings\Owner\Application Data\Macromedia\Flash Player\#SharedObjects\	EW53FKSW	media.mtvnservices.com
http://media.mtvnservices.com/player/release userPrefs4.sol	4/19/2010 5:10:31 PM 4/19/2010 5:27:18 PM	312	C:\Documents and Settings\Owner\Application Data\Macromedia\Flash Player\#SharedObjects\	EW53FKSW	media.mtvnservices.com

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.

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

21. Defendant American Broadcasting Companies, Inc. (hereinafter "ABC"), is a Delaware corporation which maintains its headquarters at 47 W. 66th Street, New York, NY 10023. Defendant ABC does business throughout the United States, and in particular, does business in State of California and in this County.

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

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

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

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

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

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

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

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

STATEMENT OF FACTS

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

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

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

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

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

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

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

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

the terms and conditions on which Quantcast offers you access to the website located at www.quantcast.com.

33. Quantcast's "Privacy Policy," dated June 17, 2009, states in part: "Check the privacy policies of websites tagged with Quantcast Tags for information regarding the applicable privacy practices.

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

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

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

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

37. MySpace's website, http://www.myspace.com, describes its business as a "technology company connecting people through personal expression, content, and culture. MySpace empowers its global community to experience the Internet through a social lens by integrating personal profiles, photos, videos, mobile, messaging, games, and the world's largest music community."

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

39. MySpace's "Terms of Use Agreement," dated June 25, 2009, states

in part:

> The following are examples of the kind of activity that is illegal or prohibited on the MySpace Website and through your use of the MySpace Services.
>
> - activity that involves the use of viruses, bots, worms, or any other computer code, files or programs that interrupt, destroy or limit the functionality of any computer software or hardware, or otherwise permit the unauthorized use of or access to a computer or a computer network;
> - providing or using "tracking" or monitoring functionality in connection with the MySpace Services, including, without limitation, to identify other Users' views, actions or other activities on the MySpace Services.

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

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

Some of the advertisements that appear on MySpace

> Services may also be delivered to you by third party Internet advertising companies. These companies utilize certain technologies to deliver advertisements and marketing messages and to collect non-PII about your visit to or use of MySpace Services, including information about the ads they display, via a cookie placed on your computer that reads your IP address. To opt out of information collection by these companies, or to obtain information about the technologies they use or their own privacy policies, please click here."

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

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

43. MySpace'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.

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

45. ABC's website, http://www.abc.com, describes its business as a provider of "information on ABC daytime and primetime network programming. Watch full episodes of your favorite ABC shows and browse exclusive online content."

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

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

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

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

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

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

> of children, and personal interests, which we may associate with personal information.
>
> Our Web sites collect information through a variety of technical methods, including cookies and Web beacons.
>
> Cookies, web beacons and other technical methods may involve the transmission of information either directly to us or to another party authorized by us to collect information on our behalf.
>
> These technical methods may enable us to collect and use information in a form that is personally identifiable.
>
> Many advertisements are managed and placed on our Web sites by third parties. These companies are called "network advertisers." Network advertisers who place advertisements on our Web sites may use cookies and Web beacons to collect non-personally identifiable information about your visits to our Web sites and other Web sites in order to provide advertisements about goods and services of interest to you."

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

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

51. ABC'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.

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

and producing sports-related content.

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

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

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

> "The following Rules of Conduct apply to the WDIG Sites. By using the WDIG Sites, you agree that you will not Distribute any Submission that: i
>
> - is defamatory, abusive, harassing, threatening, or an invasion of a right of privacy of another person;'
> - infringes or violates any right of a third party including: ... b) right of privacy (specifically, you must not distribute another person's personal information of any kind without their express permission) or publicity;'
>
> You agree that any action at law or in equity arising out of or relating to these terms of use or the WDIG Sites shall be filed, and that venue properly lies, only in state or federal courts located in the borough of Manhattan, New York, New York.."

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

> "As used in this Privacy Policy, "The Walt Disney Family of Companies" refers to The Walt Disney Company and its subsidiary and affiliated entities, singly or together, including companies such as ABC and ESPN that generally do not offer their products and services under the "Disney" brand name, as

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

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

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

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

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

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

57. ESPN’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.

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

networks nor all purposes for its involvement.

59. ESPN'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.

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

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

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

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

> You will not access the Hulu Site or use the Hulu Services in a way that:
>
> – uses technology or other means to access, index, frame or link to the Content or the Hulu Services that is not authorized by Hulu (including by removing, disabling, bypassing, or circumventing any content protection or access control mechanisms intended to prevent the unauthorized download, stream capture, linking, framing, reproduction, access to or distribution of the Content or Hulu Services);
>
> – involves accessing the Hulu Services through any automated means, including "robots," "spiders," or "offline readers" (other than by individually performed searches on publicly

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.

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

69. JibJab's website, http://www.jibjab.com, describes its business as a corporation that "creates, produces and distributes entertainment content, [] audio, visual, audiovisual, text.., offers users the opportunity to participate in community media applications by submitting…"

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

71. JibJab's "Terms of Service," dated May 27, 2009, states in part:

> User agrees not to:
>
> – interfere with or damage any of the JibJab Sites or JibJab Services, including, without limitation, through the use of viruses, cancel bots, Trojan horses, harmful code..'
>
> – collect or store any information about any other user other than in the course of the permitted use of the JibJab Sites and JibJab Services..'
>
> – sell or otherwise transfer any User information..'
>
> THE SOLE VENUE AND JURISDICTION FOR DISPUTES ARISING FROM THIS AGREEMENT SHALL BE THE APPROPRIATE STATE OR FEDERAL COURT LOCATED IN THE LOS ANGELES COUNTY, CALIFORNIA, AND USER AND JIBJAB BOTH IRREVOCABLY AGREE TO SUBMIT TO THE JURISDICTION OF SUCH COURTS.

72. JibJab's "Privacy Policy," dated May 27, 2009, states in part:

> JibJab collects user submitted information such as name, email

> address, and age.. JibJab may also collects[sic] other data either directly or via third-party sign-on services…
>
> JibJab uses cookies to store user preferences, account status, traffic origination, and to record session information, for purposes including ensuring that users are not repeatedly offered the same advertisements and to customize newsletter, advertising, and Web page content based on browser type and user profile information.
>
> JibJab allows 3rd party advertisers that are presenting advertisements on some of our pages to set and access their cookies on your computer. Advertisers' use of cookies is subject to their own privacy policies, not the JibJab Privacy Policy.
>
> Our Web advertising partners may set cookies.

73. JibJab'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.

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

75. JibJab'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.

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

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

videos..."

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

79. MTV's "Terms of Service," dated October 19, 2009, states in part:

> Rules Of Conduct
>
> You shall not use, allow, or enable others to use the Site, or knowingly condone use of this Site by others, in any manner that is, attempts to, or is likely to:
>
> – transmit, distribute or upload programs or material that contain malicious code, such as viruses, timebombs, cancelbots, worms, trojan horses, spyware, or other potentially harmful programs or other material or information;
>
> – collect, obtain, compile, gather, transmit, reproduce, delete, revise, view or display any material or information, whether personally identifiable or not, posted by or concerning any other person, firm or enterprise, in connection with their or your use of the Site, unless you have obtained the express, prior permission of such other person, firm or enterprise to do so.

80. MTV's "Privacy Policy," dated October 19, 2009, states in part:

> Information Collected Through Use of Cookies and Other Tracking Technologies. The Site and/or third parties may use "cookies", "web beacons" (also known as image tags, GIF or web bugs), "embedded scripts" and other similar tracking technologies (collectively, "Tracking Technologies") to collect Other Information automatically as you browse the Site and the web.
>
> This Site may additionally use a variety of third party

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

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

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

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

> You can choose to delete the Tracking Technologies through the "Internet Options" sub-option of the "Tools" menu option of your browser or otherwise as directed by your browser's support feature."

81. MTV'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.

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

83. MTV'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.

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

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

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

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

> It is a condition of your use of the Service that you do not:
> ...post or transmit any information, software or other material that is fraudulent or violates or infringes the rights of others, including material that violates privacy.."

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

> Use of Cookies and Similar Technologies: Like many sites, we use "cookies" or other similar technologies to collect AA [aggregate and anonymous] Data.
>
> For more information about these specialized cookies and

other technologies, and how to "opt out" of information collection by these companies, we suggest you visit http://doubleclick.net/privacy_policy or http://networkadvertising.org/optout_nonppii.asp.

89. NBC'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.

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

91. NBC'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.

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

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

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

Prohibited Conduct.

BY USING THE SCRIBD PLATFORM YOU AGREE NOT TO:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

A U.S. Federal Trade Commission representative delivered a

> stern indictment of current privacy laws on Monday, saying they fail to protect American consumers and instead place too much of a "burden" on them.
>
> "We've put too much burden on the consumers to understand these policies."
>
> "To compare the privacy policies of two companies is an almost impossible task."
>
> "[T]he current 'notice and choice' model in some very basic sense isn't working ...."
>
> "The goal of transparency clearly isn't being met by the way notice is being handled today."

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

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

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

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

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

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

Quantcast Flash Cookie Affiliate MTV's Privacy Documents:

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

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

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

Quantcast Privacy Documents:

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

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

Adobe's Flash Media Player Privacy Documents:

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

Global Security Settings Panel	1,280	3
Global Notifications Settings Panel	114	1
Website Privacy Settings Panel	290	1
Website Storage Settings Panel	727	2
Display Settings	259	2
Local Storage Settings	1,159	3
Microphone Settings	370	2
Camera Settings	298	2
Privacy Settings	787	2
Local Storage Pop-Up Question	1,030	3
Privacy Pop-Up Question	648	2
Security Pop-up Question	823	2
About Updating Flash Player	749	2
TOTAL:	19,660	51

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

Defendants' Collective Privacy Documents:

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

MTV- Social Project Terms of Use	6,347	10
Quantcast- Privacy Policy	2,392	4
Quantcast- Terms of Use	2,702	5
Adobe- Privacy Policy	3,572	6
Adobe- Terms of Use	4,691	10
Adobe- Flash Player Help	100	1
Adobe- Settings Manager	1,891	4
Adobe- Global Privacy Settings Panel	243	1
Adobe- Global Storage Settings Panel	629	2
Adobe- Global Security Settings Panel	1,280	3
Adobe- Global Notifications Settings Panel	114	1
Adobe- Website Privacy Settings Panel	290	1
Adobe- Website Storage Settings Panel	727	2
Adobe- Display Settings	259	2
Adobe- Local Storage Settings	1,159	3
Adobe- Microphone Settings	370	2
Adobe- Camera Settings	298	2
Adobe- Privacy Settings	787	2
Adobe- Local Storage Pop-Up Question	1,030	3
Adobe- Privacy Pop-Up Question	648	2
Adobe- Security Pop-up Question	823	2
Adobe- About Updating Flash Player	749	2
TOTAL:	68,629	125

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

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

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

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

A. Traditional Online Advertising

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

> Moreover, when Americans are informed of three common ways that marketers gather data about people in order to tailor ads, even higher percentages - between 73% and 86% - say they would not want such advertising."
>
> Turow, Joseph, King, Jennifer, Hoofnagle, Chris Jay, Bleakley, Amy and Hennessy, Michael, Americans Reject Tailored Advertising and Three Activities that Enable It (September 29, 2009). http://ssrn.com/abstract=1478214

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

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

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

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

by a media service.

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

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

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

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

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

130. The online advertising industry sought to maximize the benefit of ad placement by developing two (2) advertising models to analyze consumer's interest: "Contextual Advertising" and "Behavioral Advertising."

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

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

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

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

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

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

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

B. The Internet and Web Browsers

> "People should have dominion over their computers … The current, don't ask, don't tell" in online tracking and profiling has to end." FTC Chairman Jon Leibowitz, November 5, 2007.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

C. Browser Cookies

The World Wide Web is an exciting new marketplace for

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

http://www.ftc.gov/reports/privacy3/history.shtm

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

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

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

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

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

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

158. Cookie setting by advertising networks occurs as follow:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

viewed.

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

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

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

D. Web Browser Security

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

shopping and communicating with others through email or chat programs. Although online communications may not be considered "top secret," online users do not want third parties reading their email, or examining personal information stored on their computer (such as financial statements), or downloading software, such as flash cookies, without their knowledge or consent.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

> "How do I use the Settings Manager to manage third-party content storage settings?
>
> The Flash Player Settings Manager lets you manage privacy settings, storage settings, security settings, and automatic notification settings by clicking the tabs. Your first experience with Flash Player settings might have been while visiting a site with Flash content, when a pop-up menu asked you questions about privacy or storage space, or by right-clicking on content to see the Settings option in the context menu. Selecting the Help icon or clicking the Advanced button within the Settings dialog box in Flash Player opens a browser to the Settings Manager on Adobe.com, or you can access the Settings Manager directly.
>
> The third-party content setting can be found in the Global Storage Settings panel in the Settings Manager. You can prevent all third parties from storing information on your computer by deselecting the "Allow third-party Flash content option." If you disable all third-party content storage, Flash Player will not allow information to be read or written by Flash content unless the address of the content matches the address displayed in your browser's address bar. Flash Player remembers your setting and blocks third-party content storage for all sites you visit.

Conclusion

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

http://www.adobe.com/products/flashplayer/articles/thirdpartylso/

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

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

E. Flash Player- Cookies-LSO

192. http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf

A Brief History of Flash Player

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

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

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

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

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

Local Storage in Flash Player

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

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

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

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

- Application preferences – The ability for an application to remember a user's choices made while visiting a Website. These can range from a convenience feature to a critical aspect of the application.
  For example, many video websites will use Local Storage to store the volume preference for the video playback experience. Once a user adjusts the volume setting, it is remembered so that the user does not need to reset it when moving from one video to the next or upon future visits to the same video site. By using Local Storage for this

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

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

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

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

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

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

206. When you drill down in each domain’s directory, you will eventually find a “SOL” file. This file contains the data that is stored and used as the flash cookie.

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

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

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

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

210. Flash LSO cookies properties:

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

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

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

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

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

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

F. Flash Cookies, Privacy, and the "Elephant in the Room"

> "If users don't want to be tracked and there is a problem with tracking, then we should regulate tracking, not regulate cookies."
> Ashkan Soltani
> Singel, Ryan. "You Deleted Your Cookies? Think Again." Wired. (August 10, 2009) http://www.wired.com/epicenter/2009/08/you-deleted-your-cookies-think-again/

1. Elephant in the Hard Drive CIRCA: 2005

- Cohn, Michael. "Flash Player Worries Privacy Advocates" InternetWeek. (April 15, 2005) http://www.informationweek.com/news/showArticle.jhtml?articleID=160901743

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

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.ece

"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

websites," he maintains.

The Internet marketing industry hopes Internet users will bite."

2. "Elephant is Out of the Room" CIRCA: 2009

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

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

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

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

Peterson, Eric. “My Interview with Adobe Chief Privacy Officer” Web Analytics Demystified. (April 2010) http://blog.webanalyticsdemystified.com/weblog/2010/04/my-interview-with-adobe-chief-privacy-officer.html

3. “Flash Cookies and Privacy”- Berkeley Study

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

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

A. Introduction:

- In 2005, United Virtualities (UV), an online advertising company, exclaimed, “All advertisers, websites and networks use [HTTP] cookies for targeted advertising, but cookies are under attack.” The company announced that it had, “developed a backup ID system for cookies set by web sites, ad networks and advertisers, but increasingly deleted by users. UV’s ‘Persistent Identification Element’ (PIE) is tagged to the user's browser, providing each with a unique ID just like traditional cookie coding. However, PIEs cannot be deleted by any commercially available antispyware, mal-ware, or adware removal program. They will even function at the default security setting for Internet Explorer.”
- United Virtualities’ PIE leveraged a feature in Adobe’s Flash MX: the “local shared object,” also known as the “flash cookie.”
- Erasing HTTP cookies, clearing history, erasing the cache, or choosing a delete private data option within the browser does not

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

- We surveyed the top 100 websites to determine which were using Flash cookies, and explored the privacy implications. We examined these sites' privacy policies to see whether they discussed Flash cookies.
- From a privacy perspective, this is problematic, because in addition to storing user settings, many sites stored the same values in both HTTP and Flash cookies, usually with telling variable names indicating they were user ids or computer guids (globally unique identifiers). We found that top 100 websites are using Flash cookies to "respawn,"1 or recreate deleted HTTP cookies. This means that privacy-sensitive consumers who "toss" their HTTP cookies to prevent tracking or remain anonymous are still being uniquely identified online by advertising companies. Few websites disclose their use of Flash in privacy policies…"
- A Flash cookie can be set when a websites embeds first party or third party Flash content on a page. For instance, a website may include animated Flash banner advertisements served by a company that leases the advertising space or they may embed a hidden SWF used solely to provide metrics on the user. Thus, merely visiting some websites (without actually clicking on an advertisement or video) can cause Flash data from a third party advertiser to be stored on the user's computer, often unbeknownst to the user. [How done? Tricks?]

B.Results and Discussion:

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

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

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

one created by the browser.

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

G. Overlapping Values

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

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

Singel, Ryan. "Flash Cookie Researchers Spark Quantcast Change" Wired. (August 12, 2009)

http://www.wired.com/epicenter/2009/08/flash-cookie-researchers-spark-quantcast-change/#ixzz0nepIEDlb

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

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

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

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

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

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

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

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

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

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

221. “com.quantserve.sol,” set by Defendant Quantcast, in concert with 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
http://media.mtvnservices.com/player/release 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
http://media.mtvnservices.com com.quantserve.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

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

H. “flashcookie","/movies/mymovie.swf” (VPPA Defendants)

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

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

http://kb2.adobe.com/cps/161/tn_16194.html

Creating the Shared Object

“Create a Shared Object with the getLocal method of Shared Object. The movie above sets a variable (myLocalSO) and assigns a Shared Object with the name of "flashcookie" with the following ActionScript:

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

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

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

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 tohttp://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:

http://media.mtvu.com/[[IMPORT]]/media.mtvnservices.com/player/release DownShiftHistory.sol	10/12/2009 4:33:28 PM 10/28/2009 10:14:43 PM	60	C:\Users\Owner\AppData\Roaming\Macromedia\Flash Player\#SharedObjects\	N2AMUEDE	media.mtvu.com\[[IMPORT]]\media.mtvnservices.com

//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."

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

I. Personal Identifying Information

> "We see that people are getting more and more privacy aware lately, which is important as cookie use is spiraling out of control. While this increases the demand for cookie managing software, browsers supporting the new web standard HTML5 will, in the further future, definitely bring a change; and in my opinion render Flash useless. On the other hand, new plug-ins will emerge and with a tighter coupling of online and offline information, could make keeping one's privacy more and more difficult."
>
> Jenkins, George. "A Conversation with Jens Muller, CTO at Maxa Research." I've Been Mugged. (June 10, 2010) http://ivebeenmugged.typepad.com/my_weblog/2010/06/interview-jens-muller.html

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

229. Some Quantcast Flash Cookie Affiliates required users that registered

as a member to provide their name and email address, but most required date of birth, gender, and zip code, thus providing Quantcast access to uniquely indentifying personal information of Quantcast Flash Cookie Affiliate users. There are well reported occurrences of de-anonymization of databases including, but not limited to: the "Massachusetts Data Release," wherein The Massachusetts Group Insurance Commission release of state hospital records was re-anonymized by using 1990 census data that showed 87% (216 million of 248 million) of the United States population reported characteristics that made them uniquely identifiable using only three pieces of data: 5-digit ZIP, gender, date of birth, fifty-three percent of the U.S. population could be uniquely identified using only gender, location (city, town, or municipality), and date of birth, and at the county level approximately 18% of the U.S. population could be uniquely identified. L. Sweeney. Uniqueness of Simple Demographics in the U.S. Population, LIDAP-WP4. Carnegie Mellon University, Laboratory for International Data Privacy, Pittsburgh, PA: 2000 (available at http://privacy.cs.cmu.edu/dataprivacy/papers/LIDAP-WP4abstract.html)

230. "In our analysis of anonymized data from around half a million distinct browsers, 84% had unique configurations. Among browsers that had Flash or Java installed, 94% were unique, and only 1% had fingerprints that were seen more than twice. However, our experiment only studied a limited number of variables, and the companies that offer specialized fingerprinting services are likely to use a wider and therefore more powerful range of measurements." https://panopticlick.eff.org/browser-uniqueness.pdf

J. Flash Cookie Vulnerability

"Thoughts on Flash," Steve Jobs (April 2010)

> Symantec recently highlighted Flash for having one of the worst security records in 2009. We also know first hand that Flash is the number one reason Macs crash.

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

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

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

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

> Overview
>
> According to Adobe, there is a vulnerability in Adobe Flash. This vulnerability affects Flash Player, Reader, Acrobat, and possibly other products that support Flash. A remote attacker could exploit this vulnerability to execute arbitrary code."

K. Defendants' Business Practices

> Signaling frustration over privacy issues, Americans are inclined toward strict punishment of information offenders. 70% suggest that a company should be fined more than the maximum amount suggested ($2,500) "if a company purchases or uses someone's information illegally.

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

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

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

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

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

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

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

their own commercial benefit.

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

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

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

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

241. Defendants failed to disclose that its applied technologies also

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

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

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

a. The identity of the covered entity collecting the covered information.
b. A description of any covered information collected by the covered entity.
c. How the covered entity collects covered information.
d. The specific purposes for which the covered entity collects and uses covered information.
e. How the covered entity stores covered information.
f. How the covered entity may merge, link, or combine covered information collected about the individual with other information about the individual that the covered entity may acquire from unaffiliated parties.
g. How long the covered entity retains covered information in identifiable form.
h. How the covered entity disposes of or renders anonymous covered information after the expiration of the retention period.
i. The purposes for which covered information may be disclosed, and

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

j. The choice and means the covered entity offers individuals to limit or prohibit the collection and disclosure of covered information, in accordance with this section.

k. The means by and the extent to which individuals may obtain access to covered information that has been collected by the covered entity in accordance with this section.

l. A means by which an individual may contact the covered entity with any inquiries or complaints regarding the covered entity's handling of covered information.

m. The process by which the covered entity notifies individuals of material changes to its privacy notice.

n. A hyperlink to or a listing of the Federal Trade Commission's online consumer complaint form or the toll-free telephone number for the Commission's Consumer Response Center.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

information.

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

L. All Eyes On Flash

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

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

266. "Congressman Close to Introducing Privacy Bill" (January 29, 2010):

> "Representative Rick Boucher (D-VA) is close to introducing a privacy bill to the House of Representatives that is focused on opt-in/opt-out requirements for collecting data from Internet users. Our goal in doing this is to enhance the confidence that Internet users have that their experience on the Web is secure. [Bill is without a private cause of action.]
>
> https://www.privacyassociation.org/publications/2010_01_29_congressman_close_to_introducing_privacy_bill/

267. Adobe's Comments:

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

http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf

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

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

CLASS ALLEGATIONS

Allegations as to Class Certification

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

a) U.S. Resident Class: All persons residing in the United States that accessed a 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.

b) California Resident Class: All persons residing in California that 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. All California Resident Class members are also members of the U.S. Resident Class.

c) Injunctive Class: All persons after the date of the filing of this complaint, residing in the United States, that accessed a 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.

269. The class action period, (the "Class Period"), pertains to the date, two years preceding the date of this filing to the date of this filing, that a person residing in the United States, that 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.

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

a) Computer Fraud and Abuse Act (CFAA),

b) Electronic Communications Privacy Act (ECPA),

c) California's Computer Crime Law, (CCCL),

d) Civil Conspiracy, and

e) Unjust Enrichment against ALL DEFENDANTS:

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 "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

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 MYSPACE, 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.

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

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

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

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

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

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

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

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

d) Was there adequate notice, or any notice, of the operation of Quantcast and Quantcast Flash Cookie Affiliates' business practices of setting a flash cookie on a user's computer to use its local storage within the flash media player to back up browser cookies for the purpose of restoring them later provided to Quantcast and Quantcast Flash Cookie Affiliates' users?

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

f) Did Quantcast and Quantcast Flash Cookie Affiliates' business practices of setting a flash cookie on a user's computer to use its

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

c) Defendants have acted or refused to act on grounds generally

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

284. The claims asserted herein are applicable to all persons throughout the United States that 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.

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

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

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

Count I

Violation of the Computer Fraud and Abuse Act

18 U.S.C. § 1030 et. seq.

Against All Defendants

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT II

Violations of the Electronic Communications Privacy Act

18 U.S.C. §2510

Against All Defendants

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Count III

Violations of the Video Privacy Protection Act

18 U.S.C. § 2710

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

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

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

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

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

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

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

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

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

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

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

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

331. Each of the VPPA Defendants violated 18 U.S.C. § 2710(e) by failing to destroy Plaintiffs' and Class Members' personally identifiable information no later than one year from the date the information is no longer necessary for the purpose for which it was collected.

332. The Video Privacy Protection Act, 18 U.S.C. § 2710(c), provides a civil cause of action to any person aggrieved by a violation of its disclosure rules to bring a civil action for damages in a federal court.

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

334. Each incident in which a VPPA Defendant provided personally identifiable information regarding a VPPA Defendant class member as having requested or obtained specific video materials or services from a VPPA Defendant is a separate and distinct violation of the VPPA, subject to the remedies provided under the VPPA, and specifically pursuant to 18 U.S.C. § 2710(c). Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiffs' remedy at law is not adequate to compensate it for these inflicted and threatened injuries, entitling Plaintiffs to remedies including injunctive relief as provided by 18 U.S.C. § 2710.

Count IV

Violation of California's Computer Crime Law ("CCCL")

California Penal Code § 502

Against All Defendants

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

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

337. The California Computer Crime Law, California Penal Code § 502,

referred to as "CCCL" regulates "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems."

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

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

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

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

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

other fashion usurp the normal operation of the computer, computer system, or computer network."

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Count V

Violation of the California Invasion of Privacy Act

Penal Code section 630 et seq.

Against Quantcast, MySpace, Hulu, JibJab, Scribd,(hereinafter "California Defendants")

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

COUNT VI

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

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

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

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

fees.

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

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

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

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

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

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

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

COUNT VII

Violations of the Consumer Legal Remedies Act

("CLRA")California Civil Code § 1750, et seq.

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

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

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

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

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

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

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

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

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

Count VIII

Unjust Enrichment

Against All Defendants

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

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

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

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

389. Defendants appreciate or have knowledge of said benefit.

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

PRAYER FOR RELIEF

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

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiffs as class representatives, and appoint Plaintiff's counsel as class counsel;

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

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

C. As applicable to the Classes mutatis mutandis, awarding injunctive and equitable relief including, inter alia: (i) prohibiting Quantcast and Quantcast Flash Cookie Affiliates from engaging in the acts alleged above; (ii) requiring Quantcast and Quantcast Flash Cookie Affiliates to disgorge all of its ill-gotten gains to Plaintiffs and the other Class Members, or to

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

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

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

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

G. Award Plaintiffs and the Classes:

a) their reasonable litigation expenses. costs of court, and attorneys' fees;

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

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

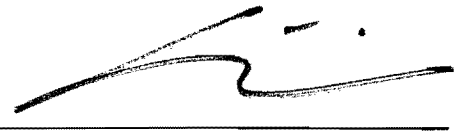
d) compensatory damages sustained by Plaintiffs and all others similarly situated as a result of Defendants' unlawful acts and conduct;

e) statutory damages, including punitive damages;

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

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

DATED this 23th day of July 2010.



By: David 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

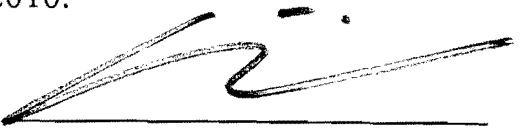
David Parisi (Cal. Bar. No. 162248)
Parisi & Havens LLP
15233 Valleyheart Drive
Sherman Oaks, California 91403
Telephone: (818) 990-1299
Facsimile: (818) 501-7852
dparisi@parisihavens.com

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