Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

Interim Class Counsel

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

Additional counsel listed on signature page

IN THE UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

IN RE QUANTCAST ADVERTISING COOKIE LITIGATION

CASE NO. 2:10-cv-05484-GW-JCG

JURY DEMAND

FIRST AMENDED AND CONSOLIDATED CLASS ACTION COMPLAINT FOR:

1. Violation of Computer Fraud and Abuse Act, 18 U.S.C. §1030;
2. Violation of Computer Crime Law, Cal. Penal Code §502;
3. Violation of Invasion Of Privacy Act, Cal. Penal Code §630;
4. Violation of Consumer Legal Remedies Act, Cal. Civ. Code §1750;
5. Violation of Unfair Competition Law, Cal. Bus. and Prof. Code §17200;
6. Trespass to Personal Property/Chattel
7. Unjust Enrichment

CLASS ACTION COMPLAINT

Plaintiffs, Jennifer Aguirre; Alan Bonebrake; Alejandro Godoy; Byron Griffith; Mary Huebner; Jose Marquez; Austin Muhs; Brittany Sanchez; Edward Valdez; Gerardo Valdez ; and Kayla Valdez ("Plaintiffs"), on behalf of themselves and all other similarly situated individuals (each a "Class Member" of the putative "Class," as further described herein), by and through their attorneys, as and for their complaint and demanding trial by jury, allege as follows based on their personal knowledge as to themselves and their own acts and observations and, otherwise, upon information and belief based on the investigation of counsel, which Plaintiffs believes further investigation and discovery will support with substantial evidence.

I. NATURE OF THE CASE

1. Plaintiffs and Class Members are consumers in the United States who use their desktop and laptop computers to access websites on the Internet, and including users who configured their web browser privacy settings to deny permission for third parties to set browser cookies on their computers.

2. Quantcast Corporation ("Quantcast") is an Internet audience metrics company. Together, Quantcast and the online content-providers that deployed Quantcast's technologies, MySpace, Inc., American Broadcasting Companies, Inc., ESPN, Inc., Hulu, LLC, JibJab Media, Inc., MTV Networks, Inc., NBC Universal Inc., and Scribd ("Publishers") (collectively, the "Defendants") gained access to the computers of millions of consumers' to plant cookie-like tracking code on users' computers. With this tracking code, Defendants circumvented users' browser controls for managing web privacy and security.

3. Defendants engaged in these practices so they could monitor users, avail themselves of information about users' web-browing activities, and continue doing so for as long as Defendants' liked without being subject to users' browser privacy and security settings and cookie management utilities that limit the abili-

ties of third parties to set and read browser cookies.

4. The user information Defendants misappropriated and merged with information from Quantcast's web affiliations and data sources, included details about users' personal characteristics such as gender, age, race, number of children, education level, geographic location, and household income. Defendants used the resulting profiles to identify individual users and track them on an ongoing basis, across numerous websites, even spotting and tracking users when they accessed the web from different computers, at home and at work.

II. JURISDICTION AND VENUE

5. This Court has subject-matter jurisdiction over this action pursuant to 28 U.S.C. § 1331.

6. Venue is proper in this District under 28 U.S.C. § 1391(b) because defendants MySpace, Inc. and JibJab maintain principal executive offices and headquarters in Los Angeles County, California, and in this District.

7. Venue is also proper in this District under 28 U.S.C. § 1391(b) because Defendants' improper conduct alleged in this complaint occurred in, was directed from, and/or emanated from this judicial district.

III. PARTIES

8. Plaintiffs are individuals residing in various locations in the United States.

9. Defendant Quantcast Corporation ("Quantcast') is a Delaware corporation with headquarters at 201 Third Street, Second Floor, San Francisco, California 94103. Quantcast does business throughout the United States and, in particular, in the State of California and Los Angeles County.

10. Defendant MySpace, Inc. is a Delaware corporation that maintains its headquarters at 407 N. Maple Drive, Beverly Hills, CA 90210. Defendant MySpace is a subsidiary of News Corporation and does business throughout the United States, and in particular, does business in the State of California and in this

judicial district.

11. Defendant American Broadcasting Companies, Inc. is a Delaware corporation that maintains its headquarters at 47 W. 66th Street, New York, NY 10023. Defendant American Broadcasting Companies, Inc. is a subsidiary of The Walt Disney Company and does business throughout the United States, and in particular, does business in the State of California and in this judicial district.

12. Defendant ESPN, Inc. is a Delaware corporation that maintains its headquarters at 935 Middle Street, Bristol, CT 06010. Defendant ESPN is a subsidiary of The Walt Disney Company and does business throughout the United States, and in particular, does business in the State of California and in this judicial district.

13. Defendant Hulu, LLC ("Hulu") is a Delaware corporation with headquarters at 12312 West Olympic Boulevard, Los Angeles, California 90064. Hulu does business throughout the United States and, in particular, in the State of California and County of Los Angeles.

14. Defendant JibJab Media, Inc. is a Delaware corporation that maintains its headquarters at 228 Main Street, Suite 4, Venice, CA 90291. JibJab Media, Inc. does business throughout the United States, and in particular, does business in the State of California and in this judicial district.

15. Defendant MTV Networks, Inc. is a Delaware corporation that maintains its headquarters at 1515 Broadway, New York, NY 10036. MTV Networks, Inc. is a subsidiary of Viacom, Inc. and does business throughout the United States, and in particular, does business in the State of California and in this judicial district.

16. Defendant NBC Universal, Inc. is a Delaware corporation that maintains its headquarters at 30 Rockefeller Plaza, New York, NY 10112. NBC Universal, Inc. does business throughout the United States, and in particular, does business in the State of California and in this judicial district.

17. Defendant Scribd, Inc. is a Delaware corporation that maintains its headquarters at 539 Bryant Street, San Francisco, CA 94107. Scribd, Inc. does business throughout the United States, and in particular, does business in the State of California and in this judicial district.

IV. STATEMENT OF FACTS

A. Background

18. In 1994, in the first web browser[1] to allow for the exchange of cookie values[2] between a web server and user's computer, the browser, by default, accepted first-party websites'[3] cookies and rejected third-party cookies. "HTTP Cookies: Standards, Privacy, and Politics," David M. Kristol, 2001, available at http://arxiv.org/abs/cs/0105018 (last accessed June 22, 2010) at 9-10. Third-party cookie transactions were considered "unverifiable transactions" and a threat to users' privacy and security; users had no way of knowing in advance whether third parties might be setting cookies on their computers, for what reason, and who the third parties were. The default configuration—rejection of third-party

---

[1] A browser is software installed on a user's personal computer . . . and with which the user, by communicating through an electronic network such as the Internet, can access Web sites. *In the Matter of Netscape Communications Corporation,* Assurance of Discontinuance, Attorney General of the State of New York (June 13, 2003).

[2] A cookie is a small string of text transmitted to and from a user's computer in a communication between a server group and a particular instance of browser client software. For ease of reference in this complaint, this exchange is characterized a communication between a website and a user, or user's browser

[3] "First-party Web site" is the Web site a User affirmatively requests to visit, for example, by typing in the site's URL or by clicking on a hyperlink to the site.

In the Matter of DoubleClick Inc.: Agreement Between the Attys. Gen. of the States of Arizona, California, Connecticut, Massachusetts, Michigan, New Jersey, New Mexico, New York, Vermont, and Washington and DoubleClick Inc., Aug. 26, 2002 at 2, available at http://www.ag.ny.gov/media_center/2002/aug/aug26a_02_attach.pdf (last accessed July 29, 2010).

cookies—was retained when, in 2000, the Internet Engineering Task Force (IETF) finalized the global standard for web servers and browsers to follow in exchanging cookies. *See* "RFC 2965, HTTP State Management Mechanism" [Kristol and Montulli 2000], Internet Engineering Task Force, Oct. 7, 2000, available at http://www.ietf.org/rfc/rfc2695.txt.pdf (last accessed July 27, 2010).

19. Nascent Internet advertising companies protested the standard. The leading commercial browser vendors, Microsoft and Netscape, declined to implement it. Kristol at 21.Thus, a *de facto* standard was propagated as browser vendors engaged in mass distribution of their software: if a first-party website—the site the user expressly chose to visit—chose to display a web page that included a third-party advertisement or use a third-party-provided traffic counter, the third party gained the ability to set cookies on users' computers with no notice to those users.

20. This development cleared the way for third-party advertising companies to engage in widespread "network advertising." By assembling a client network of many websites, advertising companies could recognize, track, and profile users activities across many websites. As early as 2001, DoubleClick was delivering ads on a network of over 11,000 websites. *In re DoubleClick Inc. Privacy Litigation*, 154 F.Supp.2d 497, 500 (S.D.N.Y. 2001). By 2009, Google, which acquired DoubleClick, was serving ads on a network of millions of websites. Google Inc., SEC Form 10-K for period ending Dec. 31, 2009 at 9. In 2009, advertising accounted for 97 percent of Google's $24 billion revenue in 2009. *Id.* at 19. At the same time, it became more important to commercial entities to be able to measure advertising activity and user traffic.

21. Meanwhile, browser vendors and other companies have distributed software tools that offer users some measure of third-party cookie control. For example, users can accept or refuse to accept all or certain third-party cookies or to automatically delete them at intervals of users' choosing. These software

tools—like other software owned or licensed by users, such as Adobe Flash Player—are under the authority and control of those users.

22. One reason users employ tools to manage and delete cookies is distaste for being profiled. According to PreferenceCentral, an online ad preference management provider, 58 percent of U.S. Internet users expressed willingness to receive behaviorally targeted ads in exchange for free content. However, when told how behavioral targeting works, the number of willing users dropped to below 38 percent, and 50 percent of users stated they would elect to receive a more limited selection of free content and untargeted advertisements. "Consumer Perspectives on Online Advertising 2010," PreferenceCentral, July 7, 2010, available at http://www.preferencecentral.com/consumersurvey/results/behavioral-targeting/ (last accessed July 28, 2010).

B. Quantcast's Conduct

23. User control over third-party cookies has created challenges for advertisers and online ad networks, as well as Internet metrics companies such as Quantcast, that attempt to track and profile users over time and/or across multiple websites. For online companies that rely on cookies to track users and measure user activity, cookie deletion skews the numbers.

24. Quantcast, however, identified a way to work with the websites and content-providers deploying its technology to work around user preferences by installing, on users' computers, a tracking device that users could not easily detect, manage, or delete. In cooperation with websites, Quantcast planted its own tracking code on users' computers—but not in a cookie. Quantcast and participating website owners and operators, including the Publishers, stored tracking code as an Adobe Flash Media Player local shared object (LSO). Adobe Flash Media Player is software that enables users to view video content on their computers. Quantcast then merged the tracking results with information from other sources to arrive at metrics for the site.

25. Quantcast and the Publishers' use of this technology was independently confirmed in a report issued by academic researchers and titled, "Flash Cookies and Privacy," which found that:

a. A user visiting a Publisher site would receive a standard, browser cookie, and an identical "Flash cookie."

b. If the user deleted the browser cookie, the Flash cookie would be used to "re-spawn" the browser cookie.

c. These operations happened without any notice to the user and without any consent from the user.

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

26. In a letter to the Federal Trade Commission earlier this year, Adobe Systems Incorporated condemned the use of LSOs to back-up and re-spawn browser cookies without express user consent. Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf (last accessed July 27, 2010).

C. Plaintiffs' Experiences

27. During the Class Period, Plaintiffs visited Publisher websites.

28. Subsequently, Plaintiffs examined the contents of the local storage associated with the Adobe Flash Player application on their computers. They observed that the objects in local storage included one object labeled with the domain of the Publisher, for example "player.hulu.com" and another labeled with the domain for Quantcast, for example "www.hulu.com\com.quantserve.sol." It is Plaintiffs' belief that one or more of these objects is a tracking device used by Defendants, without authorization, to monitor and profile their Internet activities.

29. Plaintiffs did not receive notice of the installation of these devices,

did not consent to the installation of these devices, and did not want these devices to be installed on their computers.

30. Plaintiffs believe that, if they were to visit these sites again, the tracking devices would be used as substitute cookies or to re-spawn previously set cookies.

31. Plaintiffs consider information about their online activities to be in the nature of confidential, trade secret information that they protect from disclosure, including by controlling their browser settings for acceptance or rejection of cookies.

32. Plaintiffs' experiences are typical of the experiences of Class Members.

D. User Consequences

33. Defendants manipulated their "Flash cookies" in storage areas of Plaintiffs' and Class Members' computers, which were computers used in and affecting interstate commerce and communication and were therefore protected computers as defined in the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030(e)(2).

34. Defendants' actions were surreptitious and without notice and so were conducted without authorization and exceeding authorization.

35. Defendants' conduct has caused economic loss to Plaintiffs and Class Members in that, in a barter economy in which users' patronage (which is the subject of Quantcast's traffic measurement activities) is the currency with which users acquire ostensibly no-fee web services, their patronage has independent economic value.

36. In addition, inasmuch as Defendants' wrongfully acquired Plaintiffs' and Class Members' patronage, Plaintiffs and Class Members were deprived of the opportunity to contribute their patronage to web entities that did not engage in such wrongful conduct.

37. Plaintiffs and Class Members incurred the costs of repairing their computers to remediate the impaired operability caused by Defendants.

38. Further, the information misappropriated by Defendants, the "Flash cookies" copied from Plaintiffs' and Class Members' browser cookies and populated with their actual user data constitute assets with discernable values. Certainly given Defendants' conduct, Defendants associate economic value with the users' cookies. In addition, cookies even have specific valuations in criminal markets. For example, Symantec reported that, in 2007, the illicit market value of a valid Hotmail or Yahoo cookie was three dollars, though other sources have reported the prices have since dropped due to a current oversupply.

39. The aggregated loss and damage sustained by Subscribers set forth above includes economic loss with an aggregated value of at least $5,000 during a one-year period.

40. Defendants perpetrated the acts and omissions set forth in this complaint through an organized campaign of deployment, which constituted a single act.

41. Plaintiffs and Class Members sought to maintain the secrecy and confidentiality of their unique, personal, and individual information assets acquired by Defendants, which assets were trade secrets, particularly Plaintiffs' and Class Members' Internet browsing activities.

42. The means by which Defendants obtained such information, and the reasons Quantcast engaged in its campaign (user deletion of cookies) demonstrate the confidential character of such information and users' efforts to protect it.

V. CLASS ALLEGATIONS

43. Pursuant to the Federal Rules 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 Class, defined as follows:

All persons in the United States who, during the Class Period,

> used any web browsing program on any device to access one or more internet sites controlled, operated, or sponsored by Defendants or any other internet site employing any of Quantcast's technologies involving the use of HTTP "cookies" ("Cookies") or local shared objects stored in Adobe Flash Media local storage ("LSOs").

44. Excluded from the Class are Defendants, their legal representatives, assigns, and successors, and any entity in which a Defendant has a controlling interest. Also excluded is the judge to whom this case is assigned and the judge's immediate family.

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

46. The Class consists of millions of individuals and other entities, making joinder impractical.

47. The claims of Plaintiffs are typical of the claims of all other Class Members.

48. Plaintiffs will fairly and adequately represent the interests of the other Class Members. Plaintiffs have retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiffs and their counsel are committed to prosecuting this action vigorously on behalf of Class Members and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interests adverse to those of the other Class Members.

49. Absent a class action, most Class Members would find the cost of litigating their claims to be prohibitive and would have no effective remedy.

50. The class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation in that it conserves the resources of the courts and the litigants, and promotes consistency and efficiency of adjudication.

51. Defendants have acted and failed to act on grounds generally applicable to Plaintiffs and the other Class Members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members.

52. The factual and legal bases of Defendants' liability to Plaintiffs and other Class Members are the same, resulting in injury to Plaintiffs and all of the other Class Members. Plaintiffs and the other Class Members have all suffered harm and damages as a result of Defendants' wrongful conduct.

53. There are many questions of law and fact common to Plaintiffs and the Class Members and those questions predominate over any questions that may affect individual Class Members. Common questions for the Class include, but are not limited to the following, regarding Defendants' conduct described herein:

a. whether Defendants, without authorization, created and/or manipulated Adobe Flash Player local stored objects on computers to which Class Members' enjoyed rights of possession superior to those of Defendants;

b. for what purposes Defendants created and/or manipulated Adobe Flash Player local stored objects on Class Members' computers;

c. whether Defendants violated:

i. the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

ii. the California Uniform Trade Secrets Act, Civil Code § 3426;

iii. the California Computer Crime Law, Penal Code § 502;

iv. the California Unfair Competition Law, Business and Professions Code § 17200;

v. the California Consumer Legal Remedies Act, Civil Code § 1750; and

d. whether Defendants misappropriated valuable information assets of Class Members;

e. whether Defendants continue to retain valuable information assets from and about Class Members;

f. what uses of such information were exercised and continue to be exercised by Defendants; and

g. whether Defendants have been unjustly enriched.

54. The questions of law and fact common to Class Members predominate over any questions affecting only individual members, and a class action is superior to all other available methods for the fair and efficient adjudication of this controversy.

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

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

56. 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).

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

58. 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.

59. 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.

60. 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).

61. 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 a protected computers.

62. 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' and Class Members' computers by impairing the integrity of the computers.

63. 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.

64. 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.

65. Plaintiffs and Class 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."

66. Plaintiffs and Class Members 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."

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

68. 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.

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

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

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

71. Plaintiffs incorporate the above allegations by reference as if set

forth herein at length.

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

73. 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."

74. 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 Class Members; and (3) in the state in which the servers that provided the communication link between Plaintiffs and Class Members and the websites they interacted with were located.

75. 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."

76. 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."

77. 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."

78. 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."

79. 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 devise 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.

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

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

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

83. 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.

84. 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.

85. 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.

86. 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.

87. 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."

88. Plaintiffs and Class Members 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 and Class Members to injunctive relief.

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

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

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

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

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

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

Count III
Violation of the California Invasion of Privacy Act
Penal Code section 630 et seq.
Against All Defendants

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

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

97. 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 . . .

98. 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.

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

100. 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.

101. 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.

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

103. 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."

104. 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."

105. 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.

106. 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.

107. 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.

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

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

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

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

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

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

b) Defendants' representations that their services are of a particular

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

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

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

113. At this time, Plaintiffs seek only injunctive relief under this cause of action. Pursuant to California Civil Code, Section 1782, Plaintiffs will notify Defendants in writing of the particular violations of Civil Code, Section 1770 and demand that Defendants rectify the problems associated with their behavior detailed above, which acts and practices are in violation of Civil Code § 1770, though Plaintiffs contend that they have already met this notification burden by filing their original complaints.

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

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

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

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

117. By engaging in the above-described acts and practices, Defendants

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

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

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

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

need for consumers to obtain material information that enables them to safeguard their own privacy interests, including California Civil Code, Section 1798.80.

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

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

Count VI
Trespass to Personal Property / Chattels
Against All Defendants

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

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

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

126. Without Plaintiffs' and Class Members' consent, or in excess of any

consent given, Defendants knowingly and intentionally accessed Plaintiffs' and Class Members' property, thereby intermeddling with Plaintiffs' and Class Members' right to possession of the property and causing injury to Plaintiffs and the members of the Class.

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

128. Defendants undertook the following actions with respect to Plaintiffs' and Class Members' computers:

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

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

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

129. All these acts described above were acts in excess of any authority any user granted when he or she visited the Publishers' websites and none of these acts was in furtherance of users' viewing content on or utilizing the Publishers' websites. By Defendants' engaging in deception and misrepresentation, whatever authority or permission Plaintiff and Class Members may have granted to Publishers was rendered ineffective.

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

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

computers.

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

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

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

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

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

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

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

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

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

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

h) By forcing Plaintiffs and Class Members' to expend money, time,

and resources in order to remove the program installed on their computers without notice or consent.

Count VII
Unjust Enrichment

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

136. 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.

137. Defendants appreciate or have knowledge of said benefit.

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

PRAYER FOR RELIEF

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

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

2. Declare that the actions of Defendants, as set out above, violate the following:

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

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

c. California's Invasion Of Privacy Act, California Penal Code § 630;

d. California's Consumer Legal Remedies Act, Civil Code § 1750;

e. California's Unfair Competition Law, Business and Professions Code § 17200;

f. Trespass to Personal Property / Chattels;

g. Unjust Enrichment

3. As applicable to the Classes mutatis mutandis, awarding injunctive and equitable relief including, inter alia: (i) prohibiting Defendants from engaging in the acts alleged above; (ii) requiring Defendants to disgorge all of its ill-gotten gains to Plaintiffs and the other Class Members, or to whomever the Court deems appropriate; (iii) requiring Defendants to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Defendants 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 Defendants 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 Defendants;

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

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

6. Restrain Defendants, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with them from continued

access, collection, and transmission of Plaintiffs and Class Members' personal information via preliminary and permanent injunction;

7. Award Plaintiffs and the Class Members:

a. their reasonable litigation expenses and attorneys' fees;

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

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

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

e. statutory damages, including punitive damages;

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

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

Respectfully, submitted

DATED: December 3, 2010

KAMBERLAW, LLC

s/David A. Stampley

Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

Interim Counsel for the Class

Avi Kreitenberg (SBN 266571)
akreitenberg@kamberlaw.com
KamberLaw, LLP
1180 South Beverly Drive, Suite 601
Los Angeles, California 90035
Telephone: (310) 400-1050
Facsimile: (310) 400-1056

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

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

Majed Nachawati
mn@fnlawfirm.com
Fears Nachawati Law Firm
4925 Greenville Ave, Suite 715
Dallas, Texas 75206
Telephone: (214) 890-0711

Jeremy Wilson
Jeremy@wilsontrosclair.com
Kenneth P. Trosclair
pete@wilsontrosclair.com
Wilson Trosclair & Lovins, P.L.L.C.
302 N. Market St., Suite 510
Dallas, Texas 75202
Telephone: (214) 484-1930

JURY TRIAL DEMAND

Plaintiff hereby demands a trial by jury of all issues so triable.

Respectfully, submitted

DATED: December3, 2010

KAMBERLAW, LLC

s/David A. Stampley

Scott A. Kamber (*pro hac vice*)
skamber@kamberlaw.com
David A. Stampley (*pro hac vice*)
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3072
Facsimile: (212) 920-3081

Interim Counsel for the Class

Avi Kreitenberg (SBN 266571)
akreitenberg@kamberlaw.com
KamberLaw, LLP
1180 South Beverly Drive, Suite 601
Los Angeles, California 90035
Telephone: (310) 400-1050
Facsimile: (310) 400-1056

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

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

Majed Nachawati
mn@fnlawfirm.com
Fears Nachawati Law Firm
4925 Greenville Ave, Suite 715
Dallas, Texas 75206
Telephone: (214) 890-0711

Jeremy Wilson
Jeremy@wilsontrosclair.com
Kenneth P. Trosclair
pete@wilsontrosclair.com
Wilson Trosclair & Lovins, P.L.L.C.
302 N. Market St., Suite 510
Dallas, Texas 75202
Telephone: (214) 484-1930