JEFFREY H. REEVES, SBN 156648
JReeves@gibsondunn.com
JOSHUA A. JESSEN, SBN 222831
JJessen@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
3161 Michelson Drive
Irvine, California 92612-4412
Telephone: (949) 451-3800
Facsimile: (949) 451-4220

S. ASHLIE BERINGER, SBN 263977
ABeringer@gibsondunn.com
GIBSON, DUNN & CRUTCHER LLP
1881 Page Mill Road
Palo Alto, CA 94304-1211
Telephone: (650) 849-5300
Facsimile: (650) 849-5333

Attorneys for Defendant
SPECIFIC MEDIA, INC.

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

IN RE SPECIFIC MEDIA FLASH COOKIES LITIG.

Case No. SACV 10-01256 GW (JCGx)

Honorable George H. Wu

DEFENDANT SPECIFIC MEDIA, INC.'S NOTICE OF MOTION AND MOTION TO DISMISS FIRST AMENDED, CONSOLIDATED CLASS ACTION COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES IN SUPPORT THEREOF

HEARING:
Date: March 17, 2011
Time: 8:30 a.m.
Place: Courtroom 10

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE THAT on March 17, 2011, at 8:30 a.m., or as soon thereafter as the matter may be heard, in Courtroom 10 of the above-entitled court, located at 312 N. Spring Street, Los Angeles, CA 90012, Defendant Specific Media, Inc. ("Specific Media") will and hereby does move the Court pursuant to Rules 12(b)(1), 9(b), and 12(b)(6) of the Federal Rules of Civil Procedure for an Order dismissing Plaintiffs' First Amended, Consolidated Class Action Complaint *with prejudice*. Specific Media understands that Plaintiffs will oppose this Motion.

The basis for the Motion is threefold:

First, Plaintiffs have failed to plausibly allege any injury in fact. Accordingly, they lack standing to prosecute this action on behalf of themselves or the putative class, and the Complaint therefore must be dismissed for lack of subject matter jurisdiction pursuant to Federal Rule of Civil Procedure 12(b)(1).

Second, the Complaint sounds in fraud, but Plaintiffs have failed to plead any of the required particulars – the "who, what, when, where, and how" of the alleged fraud. The Complaint therefore must be dismissed pursuant to Federal Rule of Civil Procedure 9(b).

Third, the Complaint fails to state a claim upon which relief can be granted. Simply stated, the seven statutory and common law claims asserted in the Complaint were not intended to cover – and do not cover – the conduct alleged in the Complaint. The Complaint therefore must be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6).

This Motion is based upon this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, the [Proposed] Order filed concurrently herewith, the records and files in this action, and any other matters of which this Court may take judicial notice.

This Motion is made following the conference of counsel pursuant to Local Rule 7-3, which took place on February 10, 2010.

Dated: February 17, 2010

Respectfully submitted,

JEFFREY H. REEVES
S. ASHLIE BERINGER
JOSHUA A. JESSEN
GIBSON, DUNN & CRUTCHER LLP

By: *<u>/s/ Jeffrey H. Reeves</u>*
Jeffrey H. Reeves

Attorneys for Defendant SPECIFIC MEDIA, INC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

Rules

Treatises

Constitutional Provisions

I. INTRODUCTION

This putative class action is a transparent attempt by opportunistic plaintiffs' lawyers to shake down a law-abiding company (Defendant Specific Media, Inc.) by asserting legal claims that (1) on their face do not apply to the conduct alleged in Plaintiffs' First Amended, Consolidated Class Action Complaint (the "Complaint"), and (2) are predicated on conduct – specifically, the alleged practice of "respawning" browser cookies through the use of "Flash cookies" for the purpose of serving relevant advertisements to specific computers – that, even if accepted as true, did not harm a single person in any way whatsoever. The Court should not countenance such a lawsuit and should dismiss the Complaint for three separate and independent reasons.

First, despite Plaintiffs' conclusory assertion that the use of Flash cookies to re-spawn browser cookies has somehow harmed Plaintiffs and members of the proposed class, the Complaint fails to identify a single instance in which a single person (including but not limited to the named Plaintiffs) lost even one dollar – or was specifically harmed in any other way – as a result of Specific Media's alleged conduct. Accordingly, Plaintiffs have failed to allege any injury in fact, and they therefore lack standing to maintain a lawsuit under Article III of the U.S. Constitution, which requires their Complaint to be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(1).

Second, the Complaint is replete with references to Specific Media's alleged "deceptive acts and practices," "fraudulent" practices, "false advertising," "deception and concealment," and "deception and misrepresentation." Complaint, ¶¶ 82, 87, 91, 98 & 99. Accordingly, the Complaint sounds in fraud and is subject to Federal Rule of Civil Procedure 9(b)'s heightened pleading standards. Those heightened pleading standards mandate that Plaintiffs provide the specific details of the alleged fraud – the who, what, when, where, and how – which the Complaint manifestly fails to do.

Finally, even if the Complaint could pass Rule 12(b)(1) and 9(b) muster (which it cannot), the Complaint fails to state a claim upon which relief can be granted. Simply stated, Plaintiffs are attempting to rely largely upon statutes and common law claims that are directed to destructive computer crimes, such as hacking and wiretapping, and that were never intended to cover – and plainly do not cover – the type of conduct that Plaintiffs allege here. Other courts have rejected similar attempts by other plaintiffs' lawyers to expand these claims to cover standard Internet tracking technologies such as cookies, and this Court should do the same.

II. FACTUAL BACKGROUND

A. Representative Plaintiffs and Proposed Class

The named plaintiffs in this case are seven "individuals residing in various locations in the United States": Genevieve La Court; Deirdre Harris; Cahill Hooker; Bill Lathrop; Judy Stough; E.H., a minor, by and through parent Jeff Hall; and Stefen Kaufman. Compl. ¶ 3. Without setting forth any details, the Complaint asserts in a single, conclusory sentence that "Plaintiffs are persons who have set the privacy and security controls on their browsers to block third-party cookies and/or who periodically delete third-party cookies."[1] *Id.* ¶ 21. The Complaint also alleges that each of the named Plaintiffs had a "Flash cookie" installed on his or her computer by Specific Media and that each "did not receive notice of the installation of such devices, did not consent to the installation of such devices, and did not want such devices to be installed on their computers." *Id.* ¶ 24. Plaintiffs purport to bring this action on behalf of the following Class:

> All persons residing in the United States who, during the Class Period, used any web browsing program on any device to access web pages during which time and related to which Specific Media stored Adobe Flash local shared objects (LSOs) [a.k.a. "Flash cookies"] on such persons' computers.

[1] A web browser or Internet browser is a software application for retrieving, presenting, and traversing information resources on the World Wide Web. Common browsers include Microsoft Internet Explorer, Mozilla Firefox, Apple Safari, and Google Chrome. "Cookies" are discussed *infra*.

Id. ¶ 35. Critically, unlike the named plaintiffs who allegedly deleted or blocked third-party cookies and allege that they (i) did not receive notice of, (ii) did not consent to, and (iii) did not want Flash cookies installed on their computers, the proposed Class contains none of these limitations.[2]

The Complaint does not allege that any of the named Plaintiffs lost money or was in any way harmed by Specific Media's alleged conduct. Indeed, the Complaint does not even allege that the named Plaintiffs deleted any Specific Media browser cookies or had such browser cookies "re-spawned" by Specific Media. Instead, the Complaint alleges merely that Specific Media installed Flash cookies on Plaintiffs' computers and then speculates that "*Plaintiffs believe that, **if** they were* to re-visit the websites on which Specific Media [Flash cookies] were set, or *were to* visit other websites on which Specific Media served online advertisements, the tracking devices *would be used* as substitutes for HTTP cookies and to re-spawn previously deleted cookies." Compl. ¶ 25 (emphasis added).

B. Specific Media, Inc.

Defendant Specific Media, Inc. is a California corporation based in Irvine, California. *Id.* ¶ 4. Specific Media is "an online third-party ad network that earns its revenue by delivering targeted advertisements." *Id.* ¶ 8. "According to comScore Media Metrix's report for October 2010, Specific Media displayed ads to over 153 million users, a 'reach' of over 72 percent of the total Internet audience, placing Specific Media ninth among online ad networks." *Id.* ¶ 9. "Specific Media delivers its

[2] Since Plaintiffs' Complaint necessarily hinges on highly individualized issues such as notice and consent, even if the Complaint survived a motion to dismiss, individual issues would predominate, and thus certification of the proposed class would be inappropriate. *See Lozano v. AT&T Wireless Servs., Inc.*, 504 F.3d 718, 734 (9th Cir. 2007) (affirming finding that individual issues predominated in breach of contract claim where liability "required an individualized analysis of awareness and knowledge of [defendant's] billing practices"); *Gregurek v. United of Omaha Life Ins. Co.*, 2009 U.S. Dist. LEXIS 119521, at *17-23 (C.D. Cal. Nov. 10, 2009) (decertifying class where liability required an individualized inquiry into the notice provided to each policy holder during individual sales presentations and other conversations between the policy holder and his or her sales agent).

clients' advertisements on an ad network consisting of websites, or 'publishers,' which Specific Media pays for its inventory. 'Inventory' is advertising display space on web pages." *Id.* ¶ 11. "For delivering its ads on Specific Media's inventory, advertisers pay Specific Media performance-based fees." *Id.* ¶ 12.

C. Browser Cookies

Browser cookies, also known as HTTP cookies, "are computer programs commonly used by Web sites to store useful information such as usernames, passwords, and preferences, making it easier for users to access Web pages in an efficient manner." *In re DoubleClick Privacy Litig*., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001); *see also Blumofe v. Pharmatrak, Inc. (In re Pharmatrak, Inc. Privacy Litig.)*, 329 F.3d 9, 14 (1st Cir. 2003) ("A cookie is a piece of information sent by a web server to a web browser that the browser software is expected to save and to send back whenever the browser makes additional requests of the server (such as when the user visits additional webpages at the same or related sites)."). "Cookies are widely used on the Internet by reputable websites to promote convenience and customization. . . . Cookies may also contain unique identifiers that allow a website to differentiate among users." *Pharmatrak*, 329 F.3d at 14; *see also Netscape Communs. Corp. v. Valueclick, Inc*., 684 F. Supp. 2d 678, 682 (E.D. Va. 2009) ("[T]oday the 'cookies' technology is ubiquitous[.]").

Browser cookies are routinely placed on the computers of Internet users when they visit websites on the World Wide Web. The placement of such cookies by third-party advertising networks like Specific Media is widespread and allows those advertising networks to (1) count the number of unique visitors to a website (by recognizing the browser cookie associated with a particular computer), which in turn affects the pricing of the inventory on that website, and (2) build basic "behavioral profiles" for specific computers that are then used to target relevant advertisements to those computers. *See* Compl. ¶¶ 11-12. As further explained by Plaintiffs, "[l]ike many online, third-party services, Specific Media tracks [computers] by depositing and reading HTTP cookies containing unique identifiers and browsing history information that it uses to create behavioral profiles; when a profiled [computer] visits a web page on which Specific Media serves advertisements, Specific Media uses the profile to select particular categories of ads with which to target the [computer]."[3] *Id.* ¶ 13. Importantly, the Complaint does not and cannot challenge the legality of browser cookies, including for "tracking" unique computers, even in those instances when an Internet user does not know about or consent to the placement of a browser cookie on his computer.

D. Flash Cookies (Adobe Local Stored Objects)

Browser cookies are not the only type of "cookie" that may be deposited on a user's computer when the user visits a website. So-called "Flash cookies" also may be placed onto a user's computer for a variety of valid purposes, including by a third-party advertising network. Specific Media does not use Flash cookies.[4] Specific Media recognizes, however, that solely for purposes of determining the legal adequacy of the Complaint, the Court must credit the well-pled allegations in the Complaint.

Flash cookies, also known as Local Stored Objects ("LSOs"), support Adobe Flash, which is a multimedia platform used to add animation, video, and interactivity to Web pages. Flash is frequently used in Internet advertisements and video content on the Internet. "A Flash cookie can be set when a website 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 . . . . Thus, merely visiting some websites . . . can cause Flash data from a third-party advertiser to be stored on the user's computer . . . ." Ashkan Soltani, et al., *Flash*

[3] Plaintiffs do not (and could not consistent with their obligations under Fed. R. Civ. P. 11) allege that Specific Media is collecting any Personally Identifiable Information ("PII") (such as names, addresses, dates of birth, and so forth) from Internet users.

[4] Specific Media is an active board member of the Network Advertising Initiative (NAI), a body that has led the way toward industry best practices and self-regulation in areas such as the use of Flash cookies.

Cookies and Privacy, University of California, Berkeley (Aug. 10, 2009) (hereinafter, "Soltani"), at 2.[5]

As with browser cookies, there are different kinds of Flash cookies. For instance, some Flash cookies "provide[] the benefit of allowing a given application to 'save state' on the user[']s computer and provide better functionality to the user. Examples of such could be storing the volume level of a Flash video or caching a music file for better performance over an unreliable network connection." *Id.* at 1. Other types of Flash cookies contain unique identifiers that allow websites or advertising networks to recognize unique computers. *See id.* Importantly, the Complaint does not and cannot challenge the legality of Flash cookies *per se*.

E. Using Flash Cookies To "Respawn" Browser Cookies

Instead, Plaintiffs challenge the use of Flash cookies for a single, specific purpose – *i.e.*, to "respawn" or recreate the contents of browser cookies that have been deleted by users. By way of background, browser cookies are stored in one or more files on a computer and may, if the person using the computer so desires, be deleted by a user. *See* Compl. ¶ 21. Users also may configure their browsers to block browser cookies from being deposited on their computers in the first place. *See id.* Flash cookies, although less well-known, are also stored on a user's computer, albeit in a different location from the browser cookies. Soltani at 1. Like browser cookies, Flash cookies may be deleted by a user, and a user may also block Flash cookies. *See id*. at 4. Deleting and blocking browser cookies does not delete or block Flash cookies (and

[5] Footnote 1 of the Complaint indicates that the Soltani paper is attached to the Complaint as Exhibit B. The article does not in fact appear to be attached to the Complaint. Nonetheless, this Court may consider its contents when ruling on the instant motion. "Documents whose contents are alleged in a complaint and whose authenticity no party questions, but which are not physically attached to the pleading, may be considered in ruling on a Rule 12(b)(6) motion to dismiss." *Anderson v. Clow (In re Stac Elecs. Sec. Litig.)*, 89 F.3d 1399, 1405 n.4 (9th Cir. 1996). A copy of the Soltani article is attached hereto as Exhibit A.

vice versa); rather, a user who desires to clear a computer of Flash cookies must delete and/or block Flash cookies separately. *See id.* at 1, 4.

The gravamen of the Complaint is that Specific Media allegedly used Flash cookies to "respawn" browser cookies that unspecified users – not the named Plaintiffs – had blocked or deleted so it could continue to serve tailored advertisements to specific computers. *See* Compl. ¶¶ 17-18.

F. The Widespread Use Of Flash Cookies

According to Plaintiffs' counsel, Specific Media was not the only company engaged in the alleged conduct. Far from it, according to the 2009 Berkeley paper that prompted this lawsuit and the other carbon copy lawsuits against a host of other companies brought by the same group of plaintiffs' lawyers, "both HTTP and Flash cookies are a popular mechanism on the top 100 websites." Soltani at 3. Indeed, even federal government websites (including Whitehouse.gov) deposit Flash cookies onto computers visiting their websites. *Id.* at 4. Thus, despite the Complaint's efforts to paint Flash cookies in a sinister light, Flash cookies were – at least when the Berkeley paper was published in 2009 – widely used by reputable companies and federal government agencies. Indeed, the Berkeley paper quotes Emmy Huang of Adobe, a senior product manager for Flash Player, who puts the use of Flash cookies into context: "It is accurate to say that the privacy settings people make with regards to their browser activities are not immediately reflected in Flash player. Still, privacy choices people make for their browsers aren't more difficult to do in Flash player, and deleting cookies recorded by Flash player isn't a more difficult process than deleting browser cookies. However, it is a different process, and people may not know it's available." *Id.*

Because of the apparent widespread use of Flash cookies and the existence of a "different," less well-known process for deleting Flash cookies, Plaintiffs' counsel saw a potential cash cow. Multiple lawsuits filed by Plaintiffs' counsel – against a host of advertising networks and publishers – predictably followed. *See In re Clearspring*

Flash Cookie Litig., No. 2:10-cv-05948-GW-JCG; *In re Quantcast Advertising Cookie Litig.*, No. 2:10-cv-05484-GW-JCG; *Davis, et al. v. VideoEgg, Inc.*, No. 2:10-cv-07112-GW-JCG. Most of the companies sued in the other lawsuits have denied liability but have determined that it is easier to simply settle the cases (even if the claims are meritless) than put up a fight. But Specific Media refuses to go along – and for some simple reasons: the alleged actions are not unlawful and no one was harmed as a result of them (and moreover, Specific Media *does not engage* in the practices challenged in the Complaint). Plaintiffs therefore lack standing to sue Specific Media, and their claims fail as a matter of law.[6]

III. MOTION TO DISMISS STANDARDS

A. Motion To Dismiss For Lack Of Standing Under Rule 12(b)(1)

"A federal court's judicial power extends to cases arising under the laws of the United States." *Waste Mgmt. of N. Am., Inc. v. Weinberger*, 862 F.2d 1393, 1397 (9th Cir. 1988) (citing U.S. Const. art. III, § 2). "However, it is not enough that a litigant alleges that a violation of federal law has occurred; the litigant must have standing to invoke the federal court's power. Absent injury, a violation of a statute gives rise merely to a generalized grievance but not to standing." *Waste Mgmt.*, 862 F.2d at 1397-98 (internal citations omitted). A challenge to standing under Article III "pertain[s] to a federal court's subject-matter jurisdiction" and is therefore "properly raised in a motion under Federal Rule of Civil Procedure 12(b)(1)." *White v. Lee*, 227 F.3d 1214, 1242 (9th Cir. 2000). On a motion to dismiss for lack of standing, "no presumptive truthfulness attaches to plaintiff's allegations, and the existence of

[6] Plaintiffs' Complaint purports to assert the following seven claims: (1) Violation of Computer Fraud and Abuse Act (18 U.S.C. § 1030); (2) Violation of California's Computer Crime Law (Cal. Penal Code § 502); (3) Violation of California's Invasion of Privacy Act (Cal. Penal Code § 630); (4) Violation of California's Consumer Legal Remedies Act (Cal. Civ. Code § 1750) ("CLRA"); (5) Violation of California's Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) ("UCL"); (6) Trespass to Personal Property/Chattels; and (7) Unjust Enrichment.

disputed material facts will not preclude the court from evaluating for itself the merits of jurisdictional claims." *Augustine v. U.S.*, 704 F.2d 1074, 1077 (9th Cir. 1983).

B. Motion to Dismiss For Failure To State A Claim Under Rule 12(b)(6)

Under Federal Rule of Civil Procedure 12(b)(6), a defendant may move to dismiss a complaint for failure to state a claim upon which relief can be granted. Fed. R. Civ. P. 12(b)(6). To survive a motion to dismiss for failure to state a claim, a complaint must state "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007); *see also Ashcroft v. Iqbal*, 556 U.S. __, 129 S. Ct. 1937 (2009). The complaint need not contain detailed factual allegations, but the plaintiff must "provide the 'grounds' of his 'entitle[ment] to relief'"; this "requires more than labels and conclusions, and a formulaic recitation of the elements of a cause of action will not do." *Bell Atl. Corp.*, 550 U.S. at 555.

IV. ARGUMENT

A. Plaintiffs Lack Article III Standing To Pursue Their Claims

Plaintiffs have failed to plead facts sufficient to establish that they satisfy "the irreducible constitutional minimum of standing" under Article III, as required to pursue their claims in this Court. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992). Simply stated, because Plaintiffs have failed to make plausible allegations that they suffered a non-speculative injury in fact – or *any* injury – Plaintiffs lack standing, and their Complaint must be dismissed.

To meet the requirements of Article III standing, Plaintiffs must allege that they "have suffered an 'injury in fact'—an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual and imminent, not conjectural or hypothetical." *Lujan*, 504 U.S. at 560-561. A plaintiff does not satisfy the standing requirement "[w]hen 'speculative inferences' are necessary . . . to establish [the] injury . . . ." *Johnson v. Weinberger*, 851 F.2d 233, 235 (9th Cir. 1988).

In a putative class action suit, the named plaintiffs purporting to represent the class must establish that they personally have standing to bring the cause of action. If the named plaintiffs cannot maintain the action on their own behalf, they may not seek such relief on behalf of the class. *See Lewis v. Casey*, 518 U.S. 343, 357 (1996) ("[E]ven named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'") (dismissing a class action complaint for lack of standing) (internal citations omitted); *Leong v. Square Enix of Am. Holdings, Inc.*, 2010 U.S. Dist. LEXIS 47296, at *9 (C.D. Cal. Apr. 20, 2010) ("In a class action, at least one named plaintiff must have standing.") (dismissing a class action complaint for lack of standing).

Here, the 108-paragraph Complaint is completely devoid of a single allegation that a single named plaintiff lost money or was in any way harmed by Specific Media's alleged conduct. Simply stated, Plaintiffs have failed to allege that *any* of the named plaintiffs personally suffered any injury in fact due to the purported use of "Flash cookies" to "respawn" their browser cookies or otherwise. Indeed, the named Plaintiffs do not even allege that Specific Media tracked *their* online activity, that Plaintiffs deleted any Specific Media browser cookies, or that *their* browser cookies were "re-spawned" by Specific Media. Instead, the Complaint alleges merely that Specific Media installed Flash cookies on Plaintiffs' computers and then states that "*Plaintiffs believe that, **if** they were* to re-visit the websites on which Specific Media [Flash cookies] were set, or *were to* visit other websites on which Specific Media served online advertisements, the tracking devices *would be used* as substitutes for HTTP cookies and to re-spawn previously deleted cookies." Compl. ¶ 25 (emphasis added). These speculative allegations are the antithesis of an allegation of an invasion of a legally protected interest that is both "concrete and particularized" and "actual and imminent, not conjectural or hypothetical." *See Johnson*, 851 F.2d at 235 (affirming dismissal of complaint for lack of Article III standing where injury was hypothetical); *Space Exploration Techs. Corp. v. Boeing Co.*, 2006 U.S. Dist. LEXIS 96389, at *20 (C.D. Cal. May 11, 2006) (dismissing plaintiff's antitrust claims where plaintiff failed to establish injury in fact); *Two Jinn, Inc. v. Gov't Payment Serv., Inc.*, 2010 U.S. Dist. LEXIS 31825, at *8 (S.D. Cal. Apr. 1, 2010) (dismissing plaintiff's claims for lack of Article III standing where plaintiff's claims of injury were speculative and non-concrete); *Lee v. Capital One Bank*, 2008 U.S. Dist. LEXIS 17113, at *8-9, 13 (N.D. Cal. Mar. 5, 2008) (dismissing complaint for lack of Article III standing where injury was "hypothetical" and not "actual or imminent'). Accordingly, Plaintiffs lack standing to maintain suit.

The result would be the same even if the Court were to overlook the absence of any allegation of injury by the named plaintiffs (which it should not) and consider the vague and generic allegations of "injury" made on behalf of the putative class members. Those allegations are devoid of even the most general particulars and cannot establish an actual and non-speculative injury in fact. *See id.* For example, Plaintiffs allege that Specific Media's alleged conduct somehow has caused unspecified "economic loss" to putative class members "in that their personal information has discernable value . . . of which Defendant has deprived Plaintiffs and Class Members, and, in addition, retained and used for its own economic benefit." Compl. ¶ 31. But the Complaint does not specify the nature of any alleged "economic loss" or the nature of the alleged "personal information," much less explain how Specific Media's purported use of Flash cookies operated to "deprive" unspecified class members of their personal information.

And to the extent that Plaintiffs are alleging – as they appear to be – that the "injury" they suffered was that Specific Media was able to use unspecified personal information about them to target specific advertisements (Advertisement A instead of Advertisement B or C) to them as a result of the installation of Flash cookies on their computers, this does not constitute an injury in fact *as a matter of law*. Indeed, this theory was specifically rejected ten years ago in *In re DoubleClick Privacy Litigation*, which held that the use of browser cookies to track information about computer users for the purpose of delivering targeted advertisements did not result in any economic loss or other cognizable injury:

> We do not commonly believe that the economic value of our attention is unjustly taken from us when we choose to watch a television show or read a newspaper with advertisements and we are unaware of any statute or caselaw that holds it is. We see no reason why Web site advertising should be treated any differently. *A person who chooses to visit a Web page and is confronted by a targeted advertisement is no more deprived of his attention's economic value than are his off-line peers. Similarly, although demographic information is valued highly . . . the value of its collection has never been considered an economic loss to the subject. Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers. However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.* Therefore, it appears to us that plaintiffs have failed to state any facts that could support a finding of economic loss . . . .

154 F. Supp. 2d at 525 (emphasis added). Thus, even if the Court were to consider these general (*i.e.*, non-named-plaintiff) allegations, which it should not, the Complaint still fails to allege a cognizable injury in fact.

B. Plaintiffs Also Lack Standing Under California's UCL And CLRA

Under California's UCL, a private person has standing to bring a UCL action only if he or she "has suffered injury in fact *and* has lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204 (emphasis added). *See also Peterson v. Cellco Partnership*, 164 Cal. App. 4th 1583, 1590 (2008). Plaintiffs here have not shown that they suffered any injury in fact, and they certainly have not pointed to any loss of money or property. Accordingly, they lack standing to pursue their UCL claim. *See, e.g., In re Tobacco II Cases*, 46 Cal. 4th 298, 319-20 (2009) (holding that representative plaintiffs must meet Proposition 64 standing requirements); *Clayworth v. Pfizer*, 49 Cal. 4th 758, 789 (2010). For the same reason – namely, the absence of any actual injury – Plaintiffs also lack standing to pursue a claim under California's Consumer Legal Remedies Act. *See, e.g., Meyer v. Sprint Spectrum L.P.*, 45 Cal. 4th 634, 638, 646 (2009) (holding that "a plaintiff has no standing to sue under the CLRA without some allegation that he or she has been damaged by an alleged unlawful practice"; further stating that "the Legislature . . . set a low but nonetheless palpable threshold of damage, and did not want the costs of a [CLRA] lawsuit to be incurred when no damage could yet be demonstrated").

C. To The Extent Plaintiffs' Complaint Or Any Of The Claims Therein Sound In Fraud, Plaintiffs Have Failed To Plead Fraud With Particularity

Even if Plaintiffs could establish standing to prosecute this action – and they cannot – their Complaint (or at a minimum their CFAA, UCL, CLRA, and trespass claims, all of which allege deception) still fails as a matter of law because Plaintiffs have made allegations of fraud (*see, e.g.*, Compl. ¶¶ 33, 82, 87, 91, 98, 99) but have failed to plead that fraud with the specificity required by Rule 9(b).

"In alleging fraud . . . , a party must state with particularity the circumstances constituting fraud." Fed. R. Civ. P. 9(b). The Ninth Circuit repeatedly has held that the heightened pleading requirements of Rule 9(b) are applicable to *all* averments of fraud, regardless of whether fraud is an essential element of the underlying cause of action. *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103-05 (9th Cir. 2003); *FTC v. Lights of Am., Inc.*, 2010 U.S. Dist. LEXIS 137088, at *9 (C.D. Cal. Dec. 17, 2010); *see also Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009) (Rule 9(b) applies to CLRA and UCL claims where those claims are grounded in fraud); *Yumul v. Smart Balance, Inc.*, 2010 U.S. Dist. LEXIS 86394, at *9-10 (C.D. Cal. May 24, 2010).

Under Rule 9(b), allegations of fraud must be "specific enough to give defendants notice of the particular misconduct which is alleged to constitute the fraud charged so that they can defend against the charge and not just deny that they have done anything wrong." *Neubronner v. Milken*, 6 F.3d 666, 671 (9th Cir. 1993) (internal citation omitted). At a minimum, "the pleader must state the time, place, and specific content of the false representations as well as the identities of the parties to the misrepresentation." *Shreiber Distrib. Co. v. Serv-Well Furniture Co.*, 806 F.2d 1393, 1401 (9th Cir. 1986); *Vess*, 317 F.3d at 1106 ("Averments of fraud must be accompanied by the 'who, what, when, where, and how' of the misconduct charged."). Plaintiffs also must allege specifically "what is false or misleading about a statement, and why it is false." *Vess,* 317 F.3d at 1106 (quoting *In re GlenFed, Inc. Sec. Litig.*, 42 F.3d 1541, 1548 (9th Cir. 1994)).

In the present case, Plaintiffs' claims fall far short of satisfying these requirements. Plaintiffs' Complaint fails to provide even basic details about (1) which Flash cookies supposedly were installed on Plaintiffs' computers, (2) when they were installed, (3) which websites Plaintiffs were visiting when the Flash cookies allegedly were installed, (4) whether those websites' privacy policies (or the privacy policy of Specific Media) disclosed the existence or use of Flash cookies, (5) what specific misrepresentations by Specific Media (or third parties) Plaintiffs may have relied upon, and (6) why the unspecified representations were false or misleading. For this independent reason, Plaintiffs' claims against Specific Media must be dismissed. *See, e.g.*, *McKinniss v. General Mills, Inc.*, 2007 U.S. Dist. LEXIS 96107, at *5 (C.D. Cal. Sept. 18, 2007) (granting motion to dismiss under Rule 9(b)).

D. Plaintiffs' Claim For Violation Of The Computer Fraud And Abuse Act Fails As A Matter Of Law

Even if Plaintiffs' Complaint could pass Rule 12(b)(1) and 9(b) muster – and it cannot – the Complaint still fails to state a claim under Rule 12(b)(6) because Plaintiffs purport to assert claims under a series of inapplicable federal and state laws that prohibit intentional, destructive acts of computer hacking and interception and that cannot be construed to encompass the routine transmission of data between websites, computer browsers and web servers via cookies on the Internet.

Plaintiffs' first cause of action purports to state a claim for violation of a federal criminal statute, the Computer Fraud and Abuse Act ("CFAA") (18 U.S.C. § 1030). Initially enacted in 1984, the CFAA is an anti-hacking statute that criminalizes different kinds of computer hacking, such as "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing]— . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Plaintiffs' CFAA claim here fails as a matter of law for three reasons.

First, the CFAA was never intended to criminalize standard Internet protocols, such as cookies, or to provide a vehicle for creative plaintiffs' lawyers to challenge the use of such widespread technical protocols in court. Rather, the CFAA was intended to combat destructive computer hacking, something Plaintiffs do not and could not allege here. Plaintiffs are not the first persons to attempt to misuse the CFAA to challenge the use of cookies by advertising networks. Indeed, ten years ago, another group of plaintiffs attempted to use the CFAA to challenge the use of browser cookies in *In re DoubleClick Privacy Litigation*. But the *DoubleClick* court rejected their claims as a matter of law, noting, among other things, "[t]he absence of evidence in the legislative or judicial history of . . . [the CFAA] to suggest that Congress intended to prohibit conduct like DoubleClick's . . . ." *Id.* at 526. "To the contrary," the *DoubleClick* court observed, "the histor[y] of [this] statute[] reveal[s] [a] specific Congressional goal[] – punishing destructive hacking . . . – that [is] carefully embodied in [this] criminal statute[] and [its] corresponding civil right[] of action." *Id.; see also LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1130 (9th Cir. 2009) ("The [CFAA] was originally designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality[.]"); *Shamrock Foods Co. v. Gast*, 535 F. Supp. 2d 962, 965-66 (D. Ariz. 2008) ("[T]he legislative history supports a narrow view of the CFAA. . . . The general purpose of the CFAA 'was to create a cause of action against computer hackers (e.g., electronic trespassers).' . . . Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense. . . . Simply stated, the CFAA is a criminal statute focused on criminal conduct. The civil component is an afterthought.") (internal citations omitted); *U.S. v. Aleynikov*, 2010 U.S. Dist. LEXIS 92101, at *56 (S.D.N.Y. Sept. 3, 2010); *Orbit One Communs. v. Numerex Corp.*, 692 F. Supp. 2d 373, 385-86 (S.D.N.Y. 2010); *Jet One Group, Inc. v. Halcyon Jet Holdings, Inc.*, 2009 U.S. Dist. LEXIS 72579, at *19-21 (E.D.N.Y. Aug. 14, 2009).

Second, even if Congress had intended to cast a wide enough net in the CFAA to criminalize the use of browser or Flash cookies – and it did not – Plaintiffs' Complaint fails to plausibly allege that Plaintiffs suffered "damage or loss by reason of a violation of this section" *and* that they suffered at least $5,000 in economic damages in a one-year period as a result of Specific Media's actions – threshold requirements to state a claim under the CFAA. *See* 18 U.S.C. §§ 1030(g) & (c)(4)(A)(i)(I). Specifically, Plaintiffs here do not plausibly allege (or allege at all) that the installation of Flash cookies on their computers caused any "impairment to the integrity or availability of data, a program, a system, or information," nor do they plausibly allege that the installation of Flash cookies resulted in any "cost to any victim." 18 U.S.C. §§ 1030(e)(8) & (11) (defining "damage" and "loss"). Additionally, even if the Court were to conclude that Plaintiffs had suffered some *de minimis* "damage" or "loss," Plaintiffs have failed to plausibly allege that they suffered $5,000 in economic damages in a one-year period.

As discussed above, it is well settled that Plaintiffs' allegations that Specific Media used Flash cookies to enable it to continue targeting relevant advertisements to Plaintiffs on websites that Plaintiffs voluntarily visited simply do not constitute an allegation of economic damages. *See* Section IV.A, *supra*; *DoubleClick*, 154 F. Supp. 2d at 525-26 (holding that even assuming "some value could be placed on [plaintiffs' alleged] losses . . . plaintiffs have failed to allege facts that could support the inference that the damages and losses plaintiffs incurred from DoubleClick's access to any particular computer, over one year's time, could meet [the $5,000] damage threshold); *Creative Computing v. Getloaded.com*, 386 F.3d 930, 935 (9th Cir. 2004) (holding that "economic damages" refer to instances in which "an individual or firm's money or property are impaired in value, or money or property lost, or money must be spent to restore or maintain some aspect of a business affected by a violation"); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1281 (C.D. Cal. 2001) (granting defendant's motion to dismiss CFAA claim based on installation of cookies because the Complaint did "not include sufficient facts constituting an allegation or reasonable inference therefrom that Plaintiffs suffered at least $ 5,000 in economic damages"); *Czech v. Wall Street On Demand*, 674 F. Supp. 2d 1102, 1113-18 (D. Minn. 2009).

Finally, Plaintiffs' CFAA claim fails as a matter of law because Plaintiffs have failed to plausibly allege, as they must, that Specific Media accessed their computers "without authorization." 18 U.S.C. §§ 1030(a)(2) & (5). First, Plaintiffs acknowledge that the placement of browser cookies on their computers is authorized, but they cannot articulate any legitimate basis for why the placement of this type of cookie (which Internet users may or may not know about) is authorized, while the placement of another type of cookie (the Flash cookie) is not authorized – and no such basis exists. Second, Plaintiffs concede that the placement of Flash cookies related to the functionality of Flash content is authorized. Plaintiffs thus apparently would have this Court draw a distinction between the placement of certain types of Flash cookies (such as those controlling volume) and the placement of other types of Flash cookies (such as those identifying unique users). But this is an argument about the use of the Flash cookies *after* they were installed on users' computers. To state a claim for a CFAA violation, however, Plaintiffs must show that Specific Media accessed their computers "without authorization" – an allegation they simply cannot plausibly make. *See Shamrock Foods*, 535 F. Supp. 2d at 966 ("[T]he legislative history confirms that the

CFAA was intended to prohibit electronic trespassing, not the subsequent use or misuse of information."); *Aleynikov*, 2010 U.S. Dist. LEXIS 92101, at *54-55 (same).[7]

E. Plaintiffs Fail To State A Claim Under California's Computer Crime Law

Plaintiffs also attempt to state a claim against Specific Media for violating another *criminal* statute, specifically Section 502 of the California Penal Code. Like the CFAA, Section 502 was enacted to prevent the knowing unauthorized access of computer systems and theft or alteration of computer data. *See People v. Gentry*, 234 Cal. App. 3d 131, 141 n.8. (1991). It permits *civil* suit if, and only if, a computer system is accessed "without permission" (*i.e.*, broken into) by an outsider who thereby causes the victim some "damage or loss." Cal. Penal. Code § 502(e); *see also* Cal. Penal Code §§ 502(c) and (b)(10).

Plaintiffs' § 502 claim fails for the same reasons as Plaintiffs' CFAA claim. First, the statute was designed to target computer hackers. *See, e.g., Chrisman v. City of Los Angeles*, 155 Cal. App. 4th 29, 34 (2007) ("Section 502 defines 'access' in terms redolent of 'hacking' or breaking into a computer."). Second, Plaintiffs have not plausibly alleged that they suffered any "damage or loss" as a result of Specific Media's alleged actions. *See* Section IV.D, *supra*. Third, the applicable provisions of the statute all require that the alleged violator act "without permission," which Specific Media did not do. *See* Cal. Penal Code § 502(c)(1)-(8) & (b)(10). Accordingly, the claim fails as a matter of law. *See, e.g.*, *Swearingen v. Haas Automation, Inc.*, 2009 U.S. Dist. LEXIS 106754, at *11 (S.D. Cal. Nov. 12, 2009).

[7] To the extent that Plaintiffs contend that Specific Media "exceeded authorized access," Plaintiffs again have no basis for drawing a distinction between the various kinds of Flash cookies, since according to their own allegations, they may not have known about any varieties of Flash cookies – such that they could have "authorized" certain of them but not others. Additionally, to the extent that Plaintiffs attempt to rely on subsection (a)(5)(A), Plaintiffs have failed to allege that Specific Media "intentionally caus[ed] damage" to their computers.

F. Plaintiffs Fail To State A Claim Under California's Invasion Of Privacy Act

If there were any further need to show that Plaintiffs' Complaint is grasping at legal straws, Plaintiffs' third claim for relief is styled "Violation of the Invasion of Privacy Act, California Penal Code § 630, *et seq*." As explained below, that criminal statute has *nothing* to do with the type of conduct alleged in the Complaint.

Section 630 of the California Penal Code, which was enacted in **1967**, declares only a "legislative finding and intent" – it provides in pertinent part that "[t]he Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of *eavesdropping upon private communications*" – it does not proscribe any specific acts. Cal. Penal Code § 630 (emphasis added). The proscription of specific acts is enumerated in the sections following Section 630. Except for a throwaway reference to Section 631, Plaintiffs' Complaint does not call out any of *those* sections, however, and with good reason: none of them comes close to covering the type of conduct alleged in Plaintiffs' Complaint.

Indeed, while each of the specific provisions following Section 630 differs in its precise scope, each relates generally to eavesdropping upon or intercepting private communications. Section 631, for example, concerns "wiretapping" – conduct that plainly is not implicated here[8] – and Section 632 creates criminal liability for "[e]very person who, intentionally and without the consent of all parties to a confidential communication, by means of any electronic amplifying or recording device, eavesdrops upon or records the confidential communication . . . ." Cal. Penal Code § 632(a).

[8] Section 631 prohibits "three ways of obtaining information being sent over a telephone or telegraph line: (1) tapping the line, (2) making an unauthorized connection with the line, and (3) reading, attempting to read, or learning the contents or meaning of a message while the message is in transit." *Membrila v. Receivables Performance Mgmt., LLC*, 2010 U.S. Dist. LEXIS 33565, at * 4 (S.D. Cal. Apr. 6, 2010) (quoting *Rogers v. Ulrich*, 52 Cal. App. 3d 894, 899 (1975)).

Section 632 on its face does not apply here. First, Section 632 requires the use of an "electronic amplifying or recording device," which Plaintiffs have not alleged (and could not allege). Second, Section 632(c) defines the term "confidential communication" to "include[] any communication carried on in circumstances as may reasonably indicate that any party to the communication desires it to be confined to the parties thereto, but excludes a communication made in a public gathering . . . or in any other circumstance in which the parties to the communication may reasonably expect that the communication may be overheard or recorded." Cal. Penal Code § 632(c). In the present case, there is no "communication" (confidential or otherwise) that Specific Media is alleged to have "eavesdrop[ped] upon or record[ed]." *See, e.g., Bradley v. Google*, 2006 U.S. Dist. LEXIS 94455, at *15 (N.D. Cal. Dec. 22, 2006) (dismissing plaintiffs' Invasion of Privacy Act claim where plaintiff claimed Google had accessed her e-mail account and deleted certain of her e-mails; "[Plaintiff] has not alleged that Google intercepted her communications, only that her stored emails were deleted from her account."). And to the extent that Plaintiffs are suggesting that their anonymous visits to websites constitute "communications," such "communications" are not "confidential" because Plaintiffs acknowledge that they know the websites themselves and third parties like Specific Media routinely place browser cookies on their computers (Compl. ¶¶ 10, 13). *See* Cal. Penal Code § 632(c); *Deteresa v. American Broadcasting Companies, Inc.*, 121 F.3d 460, 464 (9th Cir. 1997) ("where someone reasonably expects that the communication may be overheard, the communication is not confidential" for the purposes of § 632(c)); *cf. Steele v. County of San Bernardino*, 2009 U.S. Dist. LEXIS 125000, at *43-44 (C.D. Cal. Oct. 28, 2009).

G. Plaintiffs Fail To State A Claim Under California's Consumer Legal Remedies Act

Plaintiffs' purported CLRA claim is meritless for three reasons. First, as explained above, Plaintiffs lack standing to pursue a claim under the CLRA because they have not alleged that they have "been *damaged* by an alleged unlawful practice." *Meyer*, 45 Cal. App. 4th at 638 (emphasis added).

Second, CLRA claims only apply to a "consumer," which is defined as "an individual who seeks or acquires, by purchase or lease, any goods or services for personal, family, or household purposes." Cal. Civ. Code § 1761(d). Plaintiffs here do not allege – nor could they – that they sought or acquired goods or services from Specific Media, and this fact alone is fatal to their CLRA claim. *See, e.g.*, *Kleffman v. Vonage Holdings Corp.*, 2007 U.S. Dist. LEXIS 40487, at *11 (C. D. Cal. May 22, 2007) ("Kleffman is not a 'consumer' because he specifically alleges that he and the class members have not acquired or sought any products or services offered by [defendant] Vonage."), *aff'd*, 387 Fed. Appx. 696, 698 (9th Cir. 2010); s*ee also Schauer v. Mandarin Gems of Cal., Inc.*, 125 Cal. App. 4th 949, 960 (2005).

Finally, even if Plaintiffs could plead that they were "consumers" as to Specific Media, the claim still would fail because Specific Media does not provide "goods" or "services" as those terms are defined in the statute (*see* Cal. Civ. Code § 1761(a)-(b)), but rather is, according to Plaintiffs' own allegations, "an online third-party ad network that earns its revenue by delivering targeted advertisements." Compl. ¶ 8; *see Kleffman*, at *12 (distinguishing between "services" and "advertisements for which the recipient pays no fee," and holding that the latter is not covered by the CLRA).

H. Plaintiffs Fail To State A Claim Under California's Unfair Competition Law

Plaintiffs do not have standing to maintain a UCL claim, but even if they did, the claim still fails as a matter of law because Plaintiffs' allegations fail to plausibly allege that the alleged conduct is unlawful, unfair, or fraudulent.

1. Plaintiffs Do Not And Cannot Plausibly Allege That Specific Media Engaged In Any Unlawful Business Practice

Plaintiffs allege that Specific Media's conduct is "unlawful" because it allegedly runs afoul of the CFAA, California's Computer Crime Law, and the CLRA. *See*

Compl. ¶ 88. As explained above, however, Plaintiffs' allegations fail to state a claim for violation of any of those statutory provisions. Accordingly, alleged violations of these statutes cannot satisfy the "unlawful" prong of the UCL. *See*, *e.g*., *Sybersound Records*, *Inc*. *v*. *UAV Corp*., 517 F.3d 1137, 1152-53 (9th Cir. 2008) (affirming dismissal of UCL claim because alleged conduct was not independently unlawful); William L. Stern, *Bus. & Prof. Code § 17200 Practice*, ¶ 5:141 (The Rutter Group 2010) (where a plaintiff cannot "state a violation of an underlying law, the § 17200 [unlawfulness] claim on which it is premised fails too").[9]

2. Plaintiffs Do Not And Cannot Plausibly Allege That Specific Media Engaged In Any Fraudulent Business Practice

Plaintiffs similarly cannot state a claim under the UCL's "fraud" prong because they have failed to plead any alleged fraud with particularity. *See* Section IV.C; *Tobacco II*, 46 Cal. 4th at 326 (holding that the UCL's "as a result of" language "imposes an actual reliance requirement on plaintiffs prosecuting a private enforcement action under the UCL's fraud prong"); *Sateriale v. R.J. Reynolds Tobacco Co.*, 2010 U.S. Dist. LEXIS 138739, at *25-26 (C.D. Cal. Dec. 7, 2010).

3. Plaintiffs Do Not And Cannot Plausibly Allege That Specific Media Engaged In Any Unfair Business Practice

Plaintiffs' allegation that Specific Media has violated the "unfair" prong of the UCL also fails. First, Plaintiffs have pled no facts that plausibly suggest that Specific Media's actions "offend[ed] an established public policy or [that they are] immoral, unethical, oppressive, unscrupulous or substantially injurious to consumers." *McDonald v. Coldwell Baker*, 543 F.3d 498, 506 (9th Cir. 2008); *Leong*, 2010 U.S.

[9] In addition to the foregoing alleged statutory violations, Plaintiffs also allege that Specific Media's conduct is unlawful because it violates California's False Advertising Law (Business and Professions Code § 17500, *et seq*.), but such allegations are grounded in fraud, and, as explained above, Plaintiffs have failed to satisfy the heightened pleading requirements of Rule 9(b) (and even the lesser pleading requirements of Rule 8). *See* cases cited in Section IV.C, *supra*.

Dist. LEXIS 47296, at *22 (same). In fact, Plaintiffs identify no conduct at all beyond that alleged to be "deceptive" and "unlawful" under the FAL and UCL, which does not support a UCL claim. *See Mathison v. Bumbo*, 2008 U.S. Dist. LEXIS 108511, at *32-33 (C.D. Cal. Aug. 18, 2008). Second, Plaintiffs' allegations of unfairness are not "tethered to some legislatively declared policy or proof of some actual or threatened impact on competition" in Specific Media's industry, as would be required to establish "unfairness" under the definition established in *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.,* 20 Cal. 4th 163, 185-87 (1999). *See, e.g., Spiegler v. Home Depot U.S.A., Inc.*, 552 F. Supp. 2d 1036, 1045 (C.D. Cal. 2008) (rejecting "unfair" business practices claim because plaintiffs failed to allege "a legislatively declared policy" that the conduct violated); *Belton v. Comcast Cable Holdings*, *LLC*, 151 Cal. App. 4th 1224, 1239-40 (2007). Because Plaintiffs have provided no details or facts indicating how Specific Media's conduct is unfair – other than the conclusory allegations contained in paragraphs 89 and 90 of the Complaint – their claim under the UCL "unfairness" prong should be dismissed. *See, e.g.*, *Mertan v. Am. Home Mortg. Servicing, Inc.*, 2009 U.S. Dist. LEXIS 99024, at *21 (C.D. Cal. Oct. 13, 2009).[10]

I. Plaintiffs Fail To State A Claim For Trespass to Personal Property/Chattels

"[T]he tort of trespass to chattels allows recovery for interferences with possession of personal property 'not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing with which he has interfered.'" *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1350 (2003). "In order to

[10] Even if Plaintiffs had standing to bring a UCL claim and could state such a claim (and they do not and cannot), their UCL claim would still fail because Plaintiffs are seeking a remedy under the statute that is unavailable – namely, damages. *Compare* Compl. ¶ 92 (alleging that "Plaintiffs and the Class have suffered and will continue to suffer damages" due to alleged UCL violation) *with Cel-Tech*, 20 Cal. 4th at 179 ("Prevailing [UCL] plaintiffs are generally limited to injunctive relief and restitution."). *See also Korea Supply Co. v. Lockheed Martin Corp*., 29 Cal. 4th 1134, 1148-49 (2003) ("The object of restitution is to restore the status quo by returning to the plaintiff funds in which he or she has an ownership interest.").

prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish: (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and (2) defendant's unauthorized use proximately resulted in damage to plaintiff." *Ebay, Inc. v. Bidder's Edge*, 100 F. Supp. 2d 1058, 1069-70 (N.D. Cal. 2000) (citations omitted). Plaintiffs here cannot plausibly make either allegation.

First, as explained above, Specific Media's actions were not "without authorization." *See* Section IV.D, *supra*. Moreover, Specific Media did not interfere with Plaintiffs' "possessory interest" in their computers, as Plaintiffs do not and could not plausibly allege that they lost possession of their computers or any significant portion of their computers. *See Intel*, 30 Cal. 4th at 1357 ("Short of dispossession, personal injury, or physical damage . . . intermeddling is actionable only if the chattel is impaired as to its condition, quality, or value, or . . . the possessor is deprived of the use of the chattel for a substantial time. In particular, an actionable deprivation of use must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession . . . .") (citations and internal quotation marks omitted).

Second, Plaintiffs have failed to plausibly allege that they were damaged in any way by the alleged placement of Flash cookies on their computers. As explained by the *Intel* court:

> [U]nder California law the [trespass to chattels doctrine] does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning. Such an electronic communication does not constitute an actionable trespass to personal property, i.e., the computer system, because it does not interfere with the possessor's use or possession of, or any other legally protected interest in, the personal property itself.

30 Cal. 4th at 1347. Indeed, as another court in this District has noted, "scholars and practitioners alike have criticized the extension of the trespass to chattels doctrine to the internet context, noting that this doctrinal expansion threatens basic internet functions (i.e., search engines) and exposes the flaws inherent in applying doctrines based in real and tangible property to cyberspace . . . ." *Ticketmaster Corp. v. Tickets.com, Inc.*, 2003 U.S. Dist. LEXIS 6483, at *12 (C.D. Cal. Mar. 6, 2003) (holding that unless there is some "tangible interference with the use or operation of the computer" or "actual dispossession of the chattel for a substantial time (not present here), the elements of the tort have not been made out").

J. California Does Not Recognize A Claim for Unjust Enrichment

Finally, Plaintiffs' purported "claim" for unjust enrichment should be dismissed *with prejudice* because California does not recognize a cause of action for unjust enrichment. *See*, *e.g.*, *Jogani v. Superior Court*, 165 Cal. App. 4th 901, 911 (2008) ("[U]njust enrichment is not a cause of action. . . . Rather, it is a general principal underlying various doctrines and remedies, including quasi-contract."); *In re DirectTV Early Cancellation Litig.*, 2010 U.S. Dist. LEXIS 98204, at *76 (C.D. Cal. Sept. 7, 2010) (dismissing unjust enrichment claim on grounds that "California does not recognize a claim for unjust enrichment").

V. CONCLUSION

Plaintiffs lack standing to prosecute the present action, and their purported claims fail as a matter of law in any event. Moreover, because the Complaint is subject to dismissal not because of minor pleading defects but because it lacks a cognizable legal theory, any attempted amendment would be futile, and Plaintiffs should not be granted leave to amend. *See Sisseton-Wahpeton Sioux Tribe v. United States*, 90 F.3d 351, 356 (9th Cir. 1996) (affirming denial of leave to amend when further amendment "would be redundant and futile").

Dated: February 17, 2011

Respectfully submitted,

JEFFREY H. REEVES
S. ASHLIE BERINGER
JOSHUA A. JESSEN
GIBSON, DUNN & CRUTCHER LLP

By: /s/ Jeffrey H. Reeves
Jeffrey H. Reeves

Attorneys for Defendant SPECIFIC MEDIA, INC.

EXHIBIT A

Flash Cookies and Privacy

Ashkan Soltani[A], Shannon Canty[B][1], Quentin Mayo[B][2], Lauren Thomas[B][3] & Chris Jay Hoofnagle[C]
School of Information[A]
Summer Undergraduate Program in Engineering Research at Berkeley (SUPERB) 2009[B]
UC Berkeley School of Law[C]
University of California, Berkeley
Berkeley, USA
correspondence to: choofnagle@law.berkeley.edu

***Abstract*—This is a pilot study of the use of "Flash cookies" by popular websites. We find that more than 50% 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.**

Privacy, tracking, flash, cookies, local stored objects, usability, online advertising, behavioral targeting, self-help

I. Introduction

Advertisers are increasingly concerned about unique tracking of users online.[4] Several studies have found that over 30% of users delete first party HTTP cookies once a month, thus leading to overestimation of the number of true unique visitors to websites, and attendant overpayment for advertising impressions.[4]

Mindful of this problem, online advertising companies have attempted to increase the reliability of tracking methods. 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."[5] 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 anti-spyware, mal-ware, or adware removal program. They will even function at the default security setting for Internet Explorer."[5] (Since 2005, a Firefox plugin called "BetterPrivacy", and more recently, a shareware program called "Glary Utilities Pro" can assist users in deleting Flash cookies.)

United Virtualities' PIE leveraged a feature in Adobe's Flash MX: the "local shared object,"[6] also known as the "flash cookie." Flash cookies offer several advantages that lead to more persistence than standard HTTP cookies. Flash cookies can contain up to 100KB of information by default (HTTP cookies only store 4KB).[7] Flash cookies do not have expiration dates by default, whereas HTTP cookies expire at the end of a session unless programmed to live longer by the domain setting the cookie. Flash cookies are stored in a different location than HTTP cookies,[7] thus users may not know what files to delete in order to eliminate them. Additionally, they are stored so that different browsers and stand-alone Flash widgets installed on a given computer access the same persistent Flash cookies. Flash cookies are not controlled by the browser. Thus 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. These differences make Flash cookies a more resilient technology for tracking than HTTP cookies, and creates an area for uncertainty for user privacy control.

It is important to differentiate between the varying uses of Flash cookies. These files (and any local storage in general) provides the benefit of allowing a given application to 'save state' on the users computer and provide better functionality to the user. Examples of such could be storing the volume level of a Flash video or caching a music file for better performance over an unreliable network connection. These uses are different than using Flash cookies as secondary, redundant unique identifiers that enable advertisers to circumvent user preferences and self-help.

With rising concern over "behavioral advertising," the US Congress and federal regulators are considering new rules to address online consumer privacy. A key focus surrounds users' ability to avoid tracking, but the privacy implications of Flash cookies has not entered the discourse.

Additionally, any consumer protection debate will include discourse on self-help. Thus, consumers' ability to be aware of and control unwanted tracking will be a key part of the legislative debate.

To inform this debate, 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.

We also studied the privacy settings provided by Adobe for Flash cookies, in an effort to better understand the practical effects of using self-help to control Flash cookies. Because some sites rely so heavily on the use of Flash content, users may encounter functionality difficulties as a result of enabling these privacy settings.

We found that Flash cookies are a popular mechanism for storing data on the top 100 sites. 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, and many companies using Flash are privacy certified by TRUSTe.

II. Flash Cookies

Some exposition on Adobe's system for managing Flash cookies is necessary here.

Flash data is stored in a different folder on different computing platforms. For instance, on an Apple, Flash local shared objects (labeled .sol) are stored at:

```
/users/[username]/Library/Preferences/Macromedia/Flash Player/
```

On a Windows computer, they are stored at:

```
\Documents and Settings\[username]\Application Data\Macromedia
\Flash Player
```

Several subdirectories may reside at that location: "#SharedObjects" contains the actual Flash cookies and subdirectories under "Macromedia.com" contains persistent global and domain-specific settings for how the Flash player operates. As such, there will be a subdirectory for each Flash-enabled domain a user visits under the "Macromedia.com" settings folder. This has privacy implications that will be visited in section IV(F) below.

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.

III. Methods

We analyzed HTTP and Flash cookies from the top 100 domains ranked by QuantCast results of July 1, 2009. The data for this survey were captured on July 27, 2009.

We also analyzed six additional government websites: CDC.gov, DATA.gov, DHS.gov, IRS.gov, NASA.gov, and Whitehouse.gov. We took care not to leave the top-level domain when analyzing these sites. That is, the URL always displayed the domain to be analyzed during our browsing session.

A. Potential for Tracking

We used Mozilla Firefox 3.5 (release June 30, 2009) and Windows XP Professional Version 2002 Service Pack 3 for capturing data from the top 100 websites. To avoid contamination from different domains visited, we created a small program to handle the process of deleting all data stored between sessions since Firefox's "Clear Private Data" tool does not remove stored Flash objects.

Each session consisted of starting on a Firefox about:blank page with clean data directories. We then navigated directly to the site in question (by entering the domain name into the browser's navigation bar) and mimicked a 'typical' users session on that site for approximately 10 pages. For example, on a video site, we would search for content and browse videos. On a shopping site, we would add items to our shopping cart. We did not create accounts or login for any of the sites tested. As a result, we had to 'deep link' directly into specific user pages for sites such as Facebook.com or Myspace.com since typically these sites do not easily allow unauthenticated browsing.

We used SoThink SWF Catcher, a Firefox plugin which identifies all SWF files present on a webpage, to capture the Flash content encountered throughout the user session. We also quit the browser after each session and ran a program to capture the resulting persistent data such as HTTP cookies, Flash objects, and the Firefox cache.

Because of the dynamic nature of websites and online advertising, any given survey may produce different advertisements and correspondingly different Flash data from varied advertising networks. Thus, our snapshot of HTTP and Flash cookies may differ from another user's experience. However we feel that this provides reasonable sample for an initial study.

1) Respawning Deleted HTTP cookies

To manually test for HTTP cookie respawning, we used Safari 4.0.1 in a clean state (no HTTP or Flash cookies as well as no items in the browser cache) to visit a top 100 site. After browsing on the site and HTTP and Flash cookies are acquired, we deleted all HTTP cookies, cleared the cache, and restarted the browser, but did not modify the Flash cookies. We then visited the same site and noted the values of HTTP cookies set and whether they matched the Flash cookies set in the previous session.

B. Implications of Manipulating User Controls

We tested usability to explore how a hypothetical privacy-sensitive user's experience would differ if his/her settings were changed to restrict Flash cookies. The test was performed using Mozilla Firefox with the BetterPrivacy 1.29 add-on installed. BetterPrivacy provides an easy-to-use interface to review, protect or delete Flash cookies. Flash player settings are controlled via a webpage on Adobe.com's website called the Adobe Flash Player: Settings Manager[8].

The user navigated to each of the top 100 websites and took notes of any pop-ups, broken content, or any other abnormalities experienced while browsing the site. Each session began with clearing all non-Adobe Flash Player shared object files (i.e. those not under the Macromedia.com folder), navigating to the site in question, and then mimicking a 'typical' user's session. Caution was taken not to navigate away from the domain of the site being tested. After each session, BetterPrivacy was checked for the appearance of any Flash cookies that may have been accumulated while browsing the site.

[1] We use the popular gamer word "respawn" to describe the recreation of a HTTP cookie after its affirmative removal by the user.

We attempted to identify changes in user-experience after restricting the ability for third party Flash objects from being stored on a user's computer (first party objects were still allowed). This option is enabled by: navigating to the Adobe Flash Player Settings Manager, locating the 'Global Storage Settings' option panel, then deselecting the option that reads, "Allow third party flash content to store data on your computer."

IV. Results and Discussion

A. *Presence of Flash and HTTP Cookies*

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.

Thus, both HTTP and Flash cookies are a popular mechanism on top 100 websites.

B. *Common Flash Cookie Variable Names*

We attempted to infer the potential use of Flash cookies via examining the actual variable names for each cookie. Often, developers will use the term 'uid' or 'userid' to refer to a unique identifier whereas 'volume' could suggest volume settings for a music or video player. Below is a table of the most frequently occurring names in our sample.

Cookie Name	Frequency
volume	21
userid	20
user	14
id	8
lts	6
_tpf	6
_fpf	6
uid	5
perf	5
computerguid	5

The most frequently occurring Flash cookie outside of those used in the Flash Player system directory was 'volume'. Given the dominance of Flash video on the web, it is reasonable to expect that volume settings would be a commonly occurring use of Flash cookies. However, it is surprising with which the prominence of Flash cookies such as 'userid, user, and id', which were found to store unique identifiers which could be used to track the user, were found. 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'.

C. *Shared Values Between HTTP and Flash Cookies*

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. Our tests revealed 37 matching HTTP and Flash values from the following advertisers: ClearSpring (8), Iesnare (1), InterClick (4), ScanScout (2), SpecificClick (14), QuantCast (6), VideoEgg (1), and Vizu (1).

In 4 cases, the following first-party domains HTTP cookies matched Flash cookie values: Sears, Lowe's, AOL, and Hulu.

D. *Flash Cookie Respawning*

Shared values between HTTP and Flash cookies raises the issue of whether websites and tracking networks are using Flash cookies to accomplish redundant unique user tracking. That is, storing the same values in both the Flash and HTTP cookie would give a site the opportunity to backup HTTP cookies if the user deleted them.

We found that taking the privacy-conscious step of deleting HTTP cookies to prevent unique tracking could be circumvented through "respawning" (See Figures 1-3). The Flash cookie value would be rewritten in the standard HTTP cookie value, thus subverting the user's attempt to prevent tracking.

We found HTTP cookie respawning on several sites.

On About.com, a SpecificClick Flash cookie respawned a deleted SpecificClick HTTP cookie. Similarly, on Hulu.com, a QuantCast Flash cookie respawned a deleted QuantCast HTTP cookie.

We also found HTTP cookie respawning across domains. For instance, a third-party ClearSpring Flash cookie respawned a matching Answers.com HTTP cookie. ClearSpring also respawned HTTP cookies served directly by Aol.com and Mapquest.com. InterClick respawned a HTTP cookie served by Reference.com

E. *Interaction with NAI Opt-Out*

"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."[9] 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.

F. Presence of Flash Settings Files

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.

G. Privacy Policies

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.

H. Government Sites

The Obama Administration is considering whether to change policy concerning the use of HTTP cookies on government websites. Currently, government officials require a "compelling need" to use persistent HTTP cookies, and must disclose their use in a privacy policy.

In light of this we arbitrarily chose six government websites to determine whether Flash was being used to assign unique values to visitors. Of the 6 government sites we tested, 3 had Flash cookies. Three were set by whitehouse.gov, one of which was labeled, "userId." Five of these sites used persistent HTTP cookies.

Whitehouse.gov disclosed the presence of a tracking technology in its privacy policy, but the policy does not specify that Flash cookies are present, nor does it provide any information on how to disable Flash cookies.[10]

I. User Experience

Since users generally do not know about Flash cookies, it stands to reason that users lack knowledge to properly manage them. In comments to the New York Times, Emmy Huang of Adobe said, "It is accurate to say that the privacy settings people make with regards to their browser activities are not immediately reflected in Flash Player. Still, privacy choices people make for their browsers aren't more difficult to do in Flash Player, and deleting cookies recorded by Flash Player isn't a more difficult process than deleting browser cookies. However, it is a different process and people may not know it is available."[11]

A separate issue arises with user controls: if a privacy sensitive individual knows about them and employs them, will they still be able to use the internet normally?

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.

Ten sites did not function optimally with third party context storage disabled. Nine of these 10 sites would not display Flash content. One site displayed an advertisement intermittently that never stabilized.

V. Conclusion

Flash cookies are a popular mechanism for storing data on top 100 websites. Some top 100 websites are circumventing user deletion of HTTP cookies by respawning them using Flash cookies with identical values. Even when a user obtains a NAI opt-out cookie, Flash cookies are employed for unique user tracking. These experiences are not consonant with user expectations of private browsing and deleting cookies. Users are limited in self-help, because anti-tracking tools effective against this technique are not widespread, and presence of Flash cookies is rarely disclosed in privacy policies.

A tighter integration between browser tools and Flash cookies could empower users to engage in privacy self-help, by blocking Flash cookies. But, to make browser tools effective, users need some warning that Flash cookies are present. Disclosures about their presence, the types of uses employed, and information about controls, are necessary first steps to addressing the privacy implications of Flash cookies.

Acknowledgments

This work was supported in by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, Telecom Italia, and United Technologies. We are grateful for the opportunities offered by the Summer Undergraduate Program in Engineering Research at Berkeley (SUPERB), and to its program leaders, Dr. Kristen Gates, Dr. Sheila M. Humphreys, and Beatriz Lopez-Flores.

References

[1] Shannon Canty is a senior at Clemson University majoring in bioengineering.

[2] Quentin Mayo is a senior at Jacksonville State University majoring in computer science.

[3] Lauren Thomas is a senior at Louisiana State University majoring in industrial engineering.

[4] M. Abraham, C. Meierhoefer, and & A. Lipsman, "The Impact of Cookie Deletion on the Accuracy of Site-Server and Ad-Server Metrics: An Empirical Comscore Study," 2007, available at http://www.comscore.com/Press_Events/Presentations_Whitepapers/2007/Cookie_Deletion_Whitepaper.

[5] United Virtualities, "United Virtualities develops ID backup to cookies, Browser-Based 'Persistent Identification Element' will also restore erased cookie, Mar. 31, 2005, available at http://www.unitedvirtualities.com/UV-Pressrelease03-31-05.htm.

[6] Antone Gonslaves, "Company bypasses cookie-deleting consumers, March 31, 2005, available at http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=160400801.

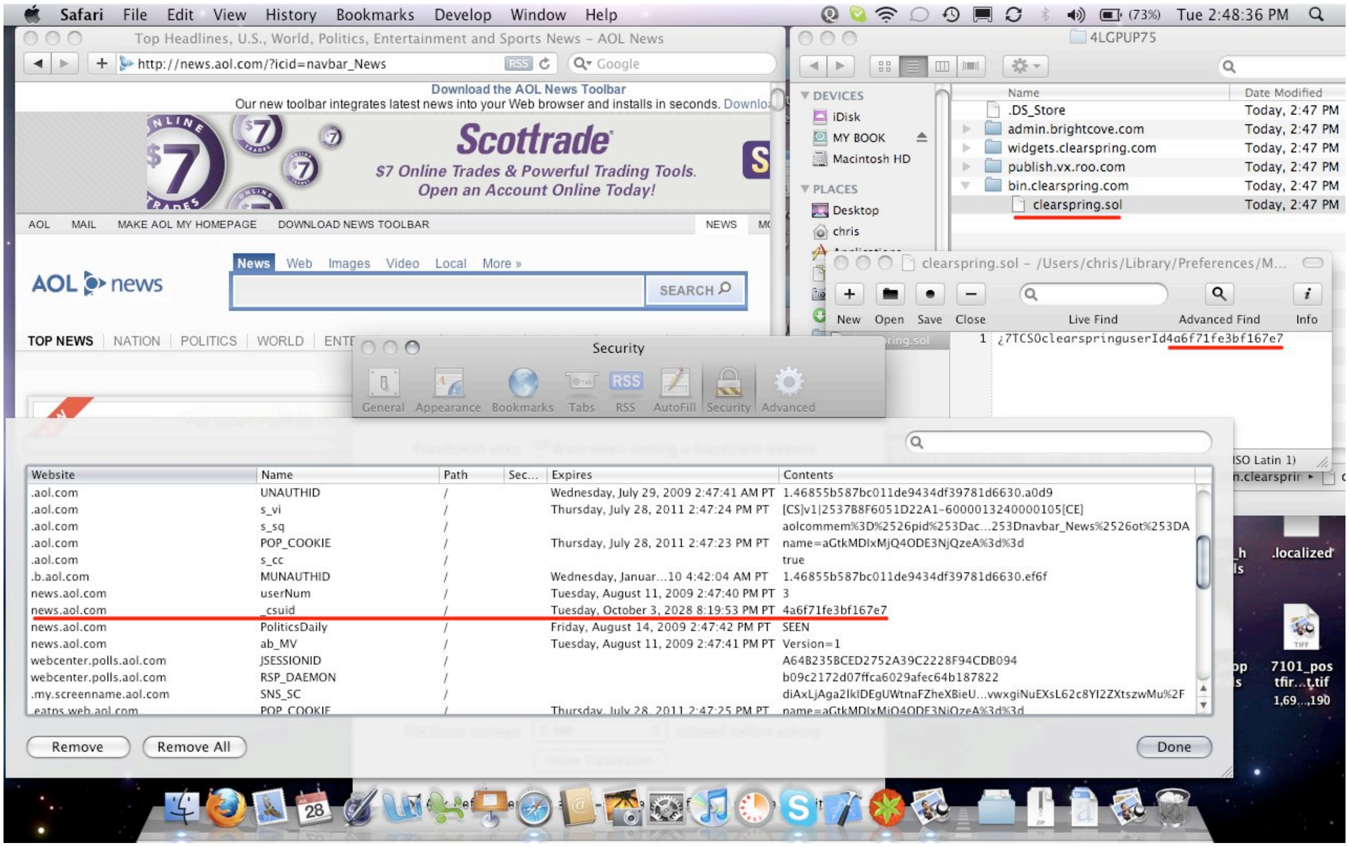
[7] J. Lott, D. Schall, and K. Peters, Actionscript 3.0 Cookbook, O'Reilly, 2006, p. 410.

[8] Adobe, Flash Settings Manager, available at http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager.html

[9] NAI, About the NAI, available at http://www.networkadvertising.org/about/.

[10] The White House, Our Online Privacy Policy, n.d., available at http://www.whitehouse.gov/privacy/

[11] Stone, Brad. "Adobe's Flash and Apple's Safari Fail a Privacy Test." Technology - Bits Blog – NYTimes.com. 30 Dec. 2008. 23 June 2009 http://bits.blogs.nytimes.com/2008/12/30/adobes-flash-and-apples-safari-fail-a-privacy-test


Safari File Edit View History Bookmarks Develop Window Help
(73%) Tue 2:48:36 PM
Top Headlines, U.S., World, Politics, Entertainment and Sports News – AOL News
http://news.aol.com/?icid=navbar_News
Google
Download the AOL News Toolbar
Our new toolbar integrates latest news into your Web browser and installs in seconds. Downlo
Scottrade
$7 Online Trades & Powerful Trading Tools.
Open an Account Online Today!
AOL MAIL MAKE AOL MY HOMEPAGE DOWNLOAD NEWS TOOLBAR NEWS
AOL news
News Web Images Video Local More »
SEARCH
TOP NEWS NATION POLITICS WORLD ENT
Security
General Appearance Bookmarks Tabs RSS AutoFill Security Advanced
4LGPUP75
DEVICES
iDisk
MY BOOK
Macintosh HD
PLACES
Desktop
chris
New Open Save Close Live Find Advanced Find Info
ISO Latin 1)
.localized
7101_pos tfir...t.tif
1,69...,190

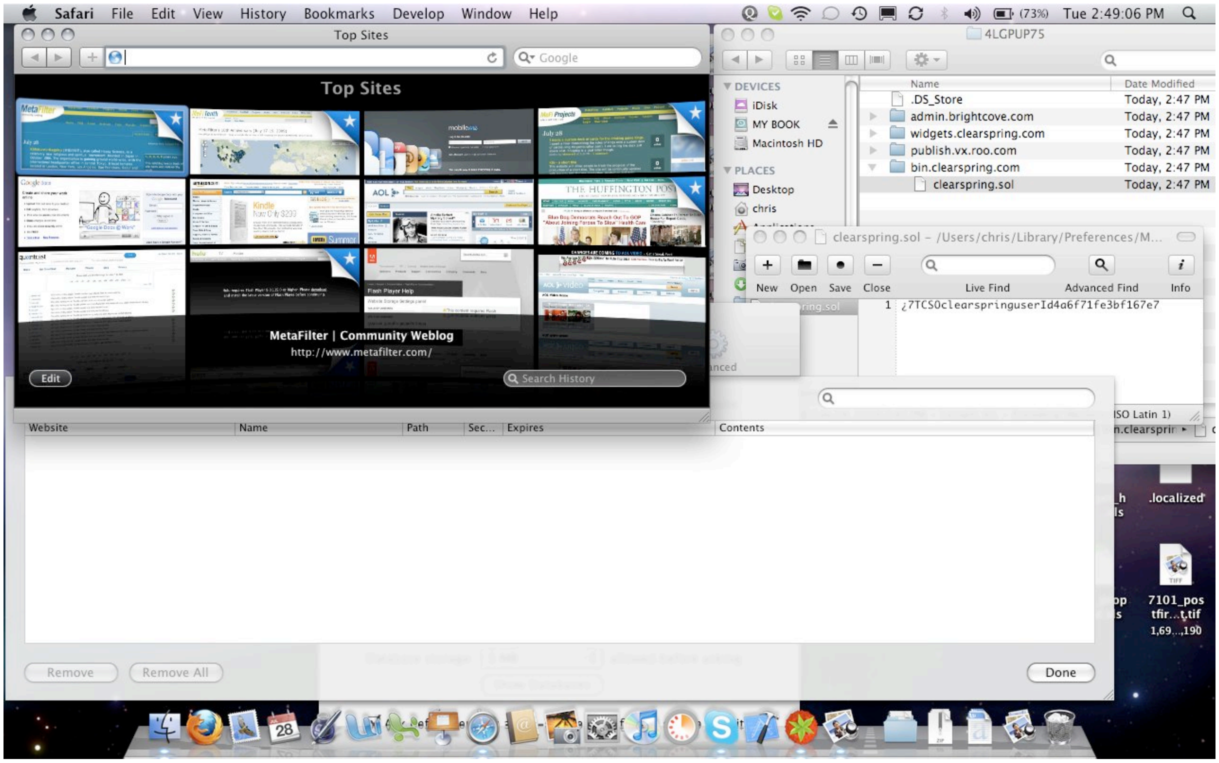
Name	Date Modified
.DS_Store	Today, 2:47 PM
admin.brightcove.com	Today, 2:47 PM
widgets.clearspring.com	Today, 2:47 PM
publish.vx.roo.com	Today, 2:47 PM
bin.clearspring.com	Today, 2:47 PM
clearspring.sol	Today, 2:47 PM

clearspring.sol – /Users/chris/Library/Preferences/M...

```
1 ¿7TCSOclearspringuserId4a6f71fe3bf167e7
```

Website	Name	Path	Sec...	Expires	Contents
.aol.com	UNAUTHID	/		Wednesday, July 29, 2009 2:47:41 AM PT	1.46855b587bc011de9434df39781d6630.a0d9
.aol.com	s_vi	/		Thursday, July 28, 2011 2:47:24 PM PT	[CS]v1|2537B8F6051D22A1-6000013240000105[CE]
.aol.com	s_sq	/			aolcommem%3D%2526pid%253Dac...253Dnavbar_News%2526ot%253DA
.aol.com	POP_COOKIE	/		Thursday, July 28, 2011 2:47:23 PM PT	name=aGtkMDIxMjQ4ODE3NjQzeA%3d%3d
.aol.com	s_cc	/			true
.b.aol.com	MUNAUTHID	/		Wednesday, Januar...10 4:42:04 AM PT	1.46855b587bc011de9434df39781d6630.ef6f
news.aol.com	userNum	/		Tuesday, August 11, 2009 2:47:40 PM PT	3
news.aol.com	_csuid	/		Tuesday, October 3, 2028 8:19:53 PM PT	4a6f71fe3bf167e7
news.aol.com	PoliticsDaily	/		Friday, August 14, 2009 2:47:42 PM PT	SEEN
news.aol.com	ab_MV	/		Tuesday, August 11, 2009 2:47:41 PM PT	Version=1
webcenter.polls.aol.com	JSESSIONID	/			A64B235BCED2752A39C2228F94CDB094
webcenter.polls.aol.com	RSP_DAEMON	/			b09c2172d07ffca6029afec64b187822
.my.screenname.aol.com	SNS_SC	/			diAxLjAga2lkIDEgUWtnaFZheXBieU...vwxgiNuEXsL62c8YI2ZXtszwMu%2F
.eatps.web.aol.com	POP_COOKIE	/		Thursday, July 28, 2011 2:47:25 PM PT	name=aGtkMDIxMjQ4ODE3NjQzeA%3d%3d

Figure 1: A matching Flash and HTTP cookie is set by AOL.com and ClearSpring.


Safari File Edit View History Bookmarks Develop Window Help
(73%) Tue 2:49:06 PM
Top Sites
Google
Top Sites
MetaFilter | Community Weblog
http://www.metafilter.com/
Edit
Search History
4LGPUP75
DEVICES
iDisk
MY BOOK
Macintosh HD
PLACES
Desktop
chris
New Open Save Close Live Find Advanced Find Info
Remove Remove All Done

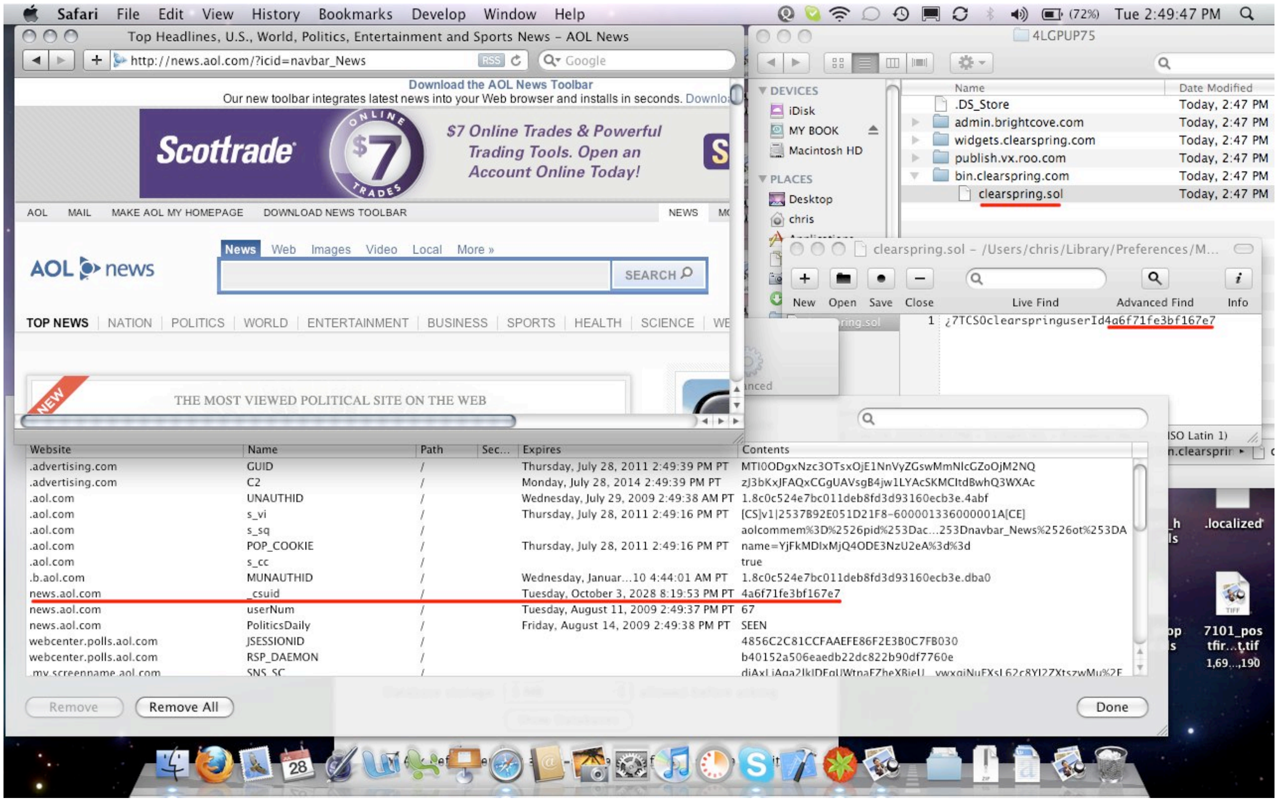
Name	Date Modified
.DS_Store	Today, 2:47 PM
admin.brightcove.com	Today, 2:47 PM
widgets.clearspring.com	Today, 2:47 PM
publish.vx.roo.com	Today, 2:47 PM
bin.clearspring.com	Today, 2:47 PM
clearspring.sol	Today, 2:47 PM

clearspring.sol – /Users/chris/Library/Preferences/M...

```
1  ¿7TCSOclearspringuserId4a6f71fe3bf167e7
```

Website	Name	Path	Sec...	Expires	Contents

Figure 2: The researcher deleted HTTP cookies and cleared the cache, leaving the Flash cookies unaltered


Safari File Edit View History Bookmarks Develop Window Help
(72%) Tue 2:49:47 PM
Top Headlines, U.S., World, Politics, Entertainment and Sports News – AOL News
http://news.aol.com/?icid=navbar_News
Google
Download the AOL News Toolbar
Our new toolbar integrates latest news into your Web browser and installs in seconds. Downlo
Scottrade
ONLINE $7 TRADES
$7 Online Trades & Powerful Trading Tools. Open an Account Online Today!
AOL MAIL MAKE AOL MY HOMEPAGE DOWNLOAD NEWS TOOLBAR NEWS
AOL news
News Web Images Video Local More »
SEARCH
TOP NEWS NATION POLITICS WORLD ENTERTAINMENT BUSINESS SPORTS HEALTH SCIENCE
NEW
THE MOST VIEWED POLITICAL SITE ON THE WEB
4LGPUP75
DEVICES
iDisk
MY BOOK
Macintosh HD
PLACES
Desktop
chris
New Open Save Close Live Find Advanced Find Info
Remove Remove All Done

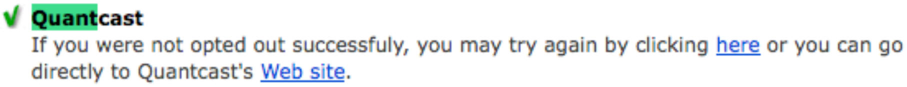
Name	Date Modified
.DS_Store	Today, 2:47 PM
admin.brightcove.com	Today, 2:47 PM
widgets.clearspring.com	Today, 2:47 PM
publish.vx.roo.com	Today, 2:47 PM
bin.clearspring.com	Today, 2:47 PM
clearspring.sol	Today, 2:47 PM

clearspring.sol – /Users/chris/Library/Preferences/M...

```
1  ¿7TCSOclearspringuserId4a6f71fe3bf167e7
```

Website	Name	Path	Sec...	Expires	Contents
.advertising.com	GUID	/		Thursday, July 28, 2011 2:49:39 PM PT	MTI0ODgxNzc3OTsxOjE1NnVyZGswMmNlcGZoOjM2NQ
.advertising.com	C2	/		Monday, July 28, 2014 2:49:39 PM PT	zJ3bKxJFAQxCGgUAVsgB4jw1LYAcSKMCItdBwhQ3WXAc
.aol.com	UNAUTHID	/		Wednesday, July 29, 2009 2:49:38 AM PT	1.8c0c524e7bc011deb8fd3d93160ecb3e.4abf
.aol.com	s_vi	/		Thursday, July 28, 2011 2:49:16 PM PT	[CS]v1|2537B92E051D21F8-600001336000001A[CE]
.aol.com	s_sq	/			aolcommem%3D%2526pid%253Dac...253Dnavbar_News%2526ot%253DA
.aol.com	POP_COOKIE	/		Thursday, July 28, 2011 2:49:16 PM PT	name=YjFkMDIxMjQ4ODE3NzU2eA%3d%3d
.aol.com	s_cc	/			true
.b.aol.com	MUNAUTHID	/		Wednesday, Januar...10 4:44:01 AM PT	1.8c0c524e7bc011deb8fd3d93160ecb3e.dba0
news.aol.com	_csuid	/		Tuesday, October 3, 2028 8:19:53 PM PT	4a6f71fe3bf167e7
news.aol.com	userNum	/		Tuesday, August 11, 2009 2:49:37 PM PT	67
news.aol.com	PoliticsDaily	/		Friday, August 14, 2009 2:49:38 PM PT	SEEN
webcenter.polls.aol.com	JSESSIONID	/			4856C2C81CCFAAEFE86F2E3B0C7FB030
webcenter.polls.aol.com	RSP_DAEMON	/			b40152a506eaedb22dc822b90df7760e
.my.screenname.aol.com	SNS_SC	/			diAxLiAqa2lkIDFqUWtnaFZheXBieU...vwxqiNuFXsL62c8YI2ZXtszwMu%2F

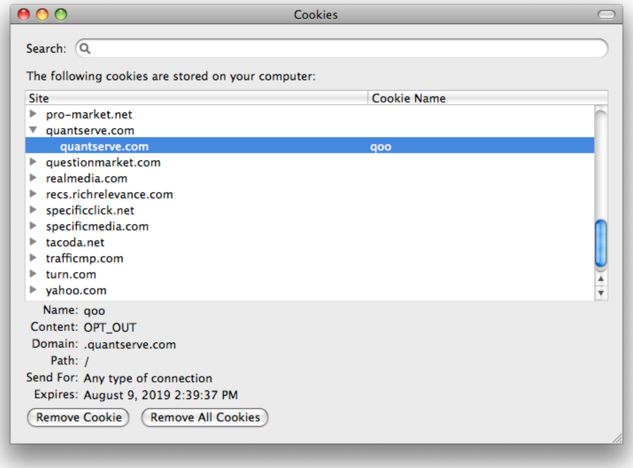
Figure 3: Upon revisiting AOL.com, a new HTTP cookie is set with the same value before HTTP cookies were deleted



✓ **Quantcast**

If you were not opted out successfuly, you may try again by clicking here or you can go directly to Quantcast's Web site.

Figure 4: Researcher obtains opt-out cookie from QuantCast

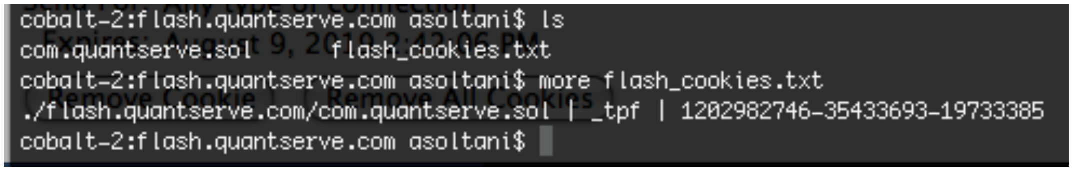


The following cookies are stored on your computer:

Site	Cookie Name
▸ pro-market.net	
▾ quantserve.com	
quantserve.com	qoo
▸ questionmarket.com	
▸ realmedia.com	
▸ recs.richrelevance.com	
▸ specificclick.net	
▸ specificmedia.com	
▸ tacoda.net	
▸ trafficmp.com	
▸ turn.com	
▸ yahoo.com	

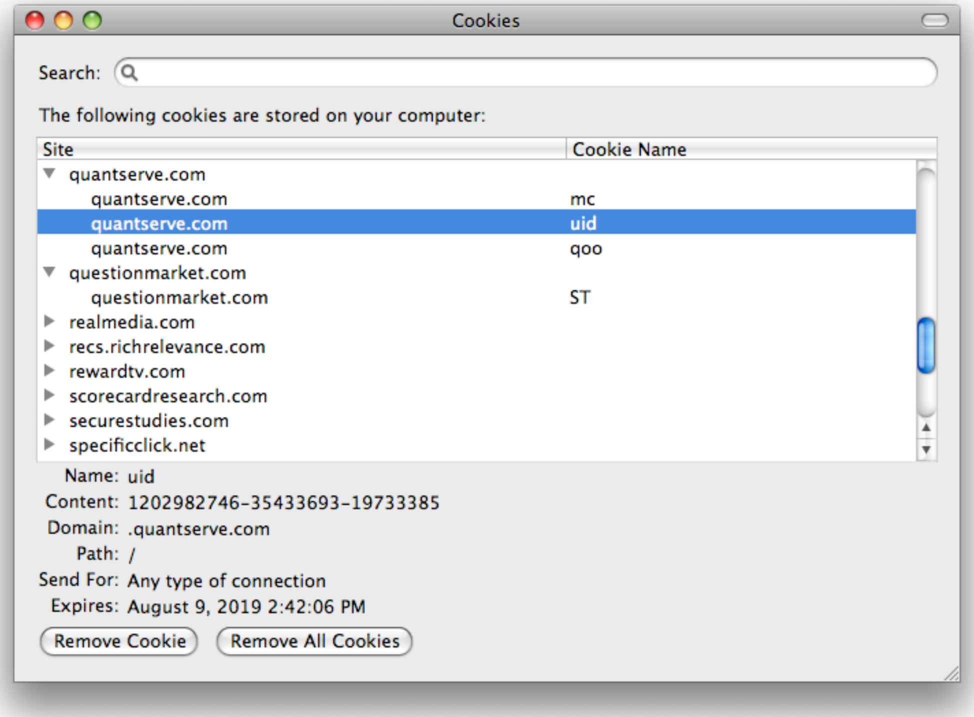
Name: qoo
Content: OPT_OUT
Domain: .quantserve.com
Path: /
Send For: Any type of connection
Expires: August 9, 2019 2:39:37 PM

Figure 5: QuantCast opt-out cookie is retained



```
cobalt-2:flash.quantserve.com asoltani$ ls
com.quantserve.sol      flash_cookies.txt
cobalt-2:flash.quantserve.com asoltani$ more flash_cookies.txt
./flash.quantserve.com/com.quantserve.sol | _tpf | 1202982746-35433693-19733385
cobalt-2:flash.quantserve.com asoltani$
```

Figure 6: Even after opting out, a Flash tracking cookie is present



The following cookies are stored on your computer:

Site	Cookie Name
▼ quantserve.com	
quantserve.com	mc
quantserve.com	uid
quantserve.com	qoo
▼ questionmarket.com	
questionmarket.com	ST
▶ realmedia.com	
▶ recs.richrelevance.com	
▶ rewardtv.com	
▶ scorecardresearch.com	
▶ securestudies.com	
▶ specificclick.net	

Name: uid
Content: 1202982746-35433693-19733385
Domain: .quantserve.com
Path: /
Send For: Any type of connection
Expires: August 9, 2019 2:42:06 PM

Figure 7: Flash tracking cookie matches Quantserve uid cookie

CERTIFICATE OF SERVICE

The undersigned certifies that, on February 17, 2011, he caused this document to be electronically filed with the Clerk of Court using the CM/ECF system, which will send notification of filing to counsel of record for each party.

Dated: February 17, 2011

GIBSON, DUNN & CRUTCHER LLP

By: _*/s/ Jeffrey H. Reeves*_________________
Jeffrey H. Reeves

Attorneys for Defendant SPECIFIC MEDIA, INC.