UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

SANDRA PERSON BURNS, an Individual, on Behalf of Herself and All Others Similarly Situated,	)	
Plaintiff,	)	Civil Action No.: _____
v.	)	
	)	COMPLAINT
AOL INC.; BRIGHTCOVE INC.; and SCANSCOUT, INC.,	)	JURY DEMAND
Defendants.	)	

I. CLASS ACTION COMPLAINT

Plaintiff, on her own behalf and on behalf of all others similarly situated (each, a "Class Member" and, collectively, the "Classes") allege as follows based on personal knowledge and on information and belief based on investigations of counsel.

II. NATURE OF THE ACTION

1. Plaintiff and Class Members—like the substantial majority of U.S. consumers across all age groups value their privacy while browsing the World Wide Web (the "Web"). They believe their Web-browsing is private and not the business of anyone except the parties with whom they have chosen to communicate. Like most U.S. consumers, they particularly do not want to be tracked for the sake of seeing tracking-based, "behaviorally targeted" online ads—whether for mortgage assistance, weight loss products, or political candidates.

2. Behaviorally targeted advertising and trafficking in consumer data has exploded since cookies were first added to Web-browsing capability. Online tracking used to be associated with online ad networks. It now involves companies that perform a wide range of tracking-

related functions (collectively, "Tracking Companies"), and which often have no direct relationship with the consumer at all.[1]

3. The moment a consumer connects to the Internet, Tracking Companies bid against each other in automated, real-time auctions for the chance to track and target the consumer. Tracking Companies track individual consumers across their networks of "affiliate" Websites—which, nowadays, may simply mean the many millions of Websites affiliated only by the fact that they display ads served by a particular Tracking Company. Tracking Companies observe where consumers click, whether on a Website or in a commercial e-mail message. They track consumers from the moment of seeing but not clicking on a product ad to the consumers' purchase of the product many days later. Many Tracking Companies claim their tracking and profiling is anonymous when, in fact, they merge consumer profiles with purchased profile data about the individual consumers' online Web activities and offline shopping, as well as details about income, education, family status and number of children, type of vehicle driven, and location of residence and work.

4. The tracking explosion has been invisible, or "non-transparent," to consumers browsing the Web. It is even invisible to many of the Websites where tracking takes place. These Websites often do not know what information the advertisers are taking or how they are taking it. The Websites just post the ads and take the money.

5. The online ad industry's machinery for monetizing consumers' information has spawned a market in consumer information. Consumer profiles are up for sale, affecting not only

[1] *E.g.*, ad exchange, analytics provider, analytics panel, content delivery network, demand-side optimizer, profile aggregator, supply-side optimizer, Web-enabled application provider, and others; *see Data Usage & Control Primer: Best Practices & Definitions*, Interactive Advertising Bureau (IAB), May 2010, available at http://www.iab.net/media/file/data-primer-final.pdf.

what product advertisement a consumer sees but also her credit card line for buying it, all based on inferences from where she browses on the Web or who her social network friends are.

6. Tracking Companies have designed their technology and business processes in ways that deter consumers from participating in the marketing of the consumers' information.

7. Likewise, Tracking Companies technologies and business processes deter consumers from seeing or controlling the Tracking Companies' marketing of consumers' information; for consumers to control at least some tracking and information marketing, they must use the same browser tools as ten years ago, when cookies first appeared on the scene.

8. In this matter, those are the tools Plaintiff used to turn off tracking, which is why Plaintiff was surprised when she starting noticing online advertisements for products and services, shortly after she had bought those same products or used those same services offline. Plaintiff discovered that, though she thought she had turned off tracking, she not only had numerous tracking cookies on her computer, but also tracking devices she had never heard of before, put there by Defendants.

9. Defendants wanted to ensure they could track Plaintiff, regardless of her browser controls, so they simply worked around them. Defendants commandeered Plaintiff's computer, repurposing its software and using her computer storage and her Internet connection to bypass her browser controls. Defendants created a shadow tracking system on her computer, effectively decommissioning the browser cookie controls she had explicitly set. Defendants did so repeatedly, for years, for a significant part of Plaintiff's Web-browsing, and did likewise to millions of consumers, for years.

10. Specifically, Plaintiff here alleges that Defendants AOL, Brightcove, and ScanScout each knowingly and intentionally circumvented her browser privacy controls and re-

purposed the Adobe Flash software on her computer. They used her Flash software for an unintended purpose—to create back-ups and substitutes for browser cookies, so they could track her in ways she could neither see or control.

11. Plaintiff, based on the allegations of this complaint and on behalf of herself and a class of similarly situated individuals, now seeks compensatory, injunctive, and declaratory relief under the federal the Electronic Communications Privacy Act (Wiretapping Act); the Computer Fraud and Abuse Act; the federal Video Privacy Protection Act; the Massachusetts Privacy Act; the Massachusetts Consumer Protection Act; and based on tort claims of Trespass to Chattel; and equitable claims of Unjust Enrichment.

III. PARTIES

A. Plaintiff

12. PLAINTIFF Sandra Person Burns is a resident of Hinds County, Mississippi.

13. Plaintiff is a consumer who, during the Class Period (as defined herein), browsed online using Microsoft Internet Explorer and/or AOL Explorer, and a customized, AOL version of Microsoft Internet Explorer (collectively, "IE"). Plaintiff set her browser privacy controls at a maximum level, to delete all cookies at the end of each browsing session.

14. Plaintiff was a paying AOL subscriber from the late 1990s until the spring of 2011, paying a monthly fee to AOL to use its proprietary online portal, through which she browsed the Web and exchanged e-mail messages. From 1997 until 2005, Plaintiff paid AOL $19.95 per month for the use of its services; from 2005 until early 2011, she paid AOL $9.95 per month for the use of its services.

B. ScanScout

15. Defendant SCANSCOUT, INC. ("ScanScout") is and throughout the Class Period was a Delaware corporation headquartered at 129 South Street, Boston, Massachusetts 02111, a

registered agent of Corporation Service Company, 84 State Street, Boston, Massachusetts 02109, and doing business through the United States.

16. ScanScout claims to operate the largest network of streaming video advertisements on the Web and that, while delivering those ads to consumers across numerous Websites, it analyzes their characteristics and compiles profiles consisting of billions of data points.

17. The ScanScout Video Ad Network has been integrated into the Brightcove Platform, so that ScanScout video ads can be delivered using Brightcove Inc.'s technology.

C. Brightcove

18. Defendant BRIGHTCOVE INC. ("Brightcove") is and throughout the Class Period was a Delaware corporation headquartered at One Cambridge Center, Cambridge, Massachusetts 02142, C T Corporation System, 155 Federal Street, Suite 700, Boston, Massachusetts 02110, and doing business throughout the United States.

19. Brightcove provides a technology platform to other companies that want to monetize videos they display to consumers online by tracking and profiling consumers' viewing of video content and targeting particular video content to particular consumers.

20. Brightcove asserts that it provides services to more than 3,000 customers in 50 countries, delivering video content on consumers' computers, mobile devices, and Internet-connection televisions.

21. Brightcove's services are heavily utilized by AOL Inc. in displaying online video content and advertisements.

D. AOL

22. Defendant AOL INC. ("AOL") is a Delaware corporation with headquarters at 770 Broadway, New York, New York 10003, a registered agent of Corporation Service Com-

pany, 84 State Street, Boston, Massachusetts 02109, and doing business through the United States.

23. AOL provides online consumer services that include AOL Mail, Lifestream (for consumers to manage social networks through one interface); AIM (instant message), about.me (web content-building), mobile applications, and subscription-based access to AOL content.

24. AOL offers online content in over 70 other AOL-branded Websites.[2]

[2] AOL's 70-plus AOL-branded Web properties include the following (specific descriptions are quoted from http://advertising.aol.com/brands, June 21, 2011):

Finance: AOL Autos–AOL Autos helps consumers make automotive decisions with the confidence of an expert; ***AOL Jobs***–AOL Jobs is an online destination for job-seekers, providing job search, tools and resources to help manage career transitions; ***AOL Real Estate***–Finding a new home is a big job! AOL Real Estate connects users with all the info they need to make smart, confident decisions about buying, selling and renting: whether they're moving across town or across the country; ***AOL Small Business***–AOL Small Business is the premier source of news, advice and success stories for small business owners, start-ups and entrepreneurs; ***Daily Finance***–DailyFinance is the destination for timely business and investment news, analysis and commentary; ***WalletPop***–WalletPop helps ordinary people reach their financial potential with bargain alerts, service features and columns produced by leading consumer finance experts.

Shopping: AOL Shopping–Whether you're looking for a jacket, sofa or engagement ring, AOL Shopping connects you with the merchants offering the products and services you want; ***Shortcuts***–Shortcuts makes saving easy, with coupons for every aisle of the grocery store, and beyond; ***Wow***–Wow provides you and your family with savings at your favorite local and national locations.

News, society, and culture: The Huffington Post–The Huffington Post is one of the fastest-growing, most influential properties on the internet. ***AOL Latino***–AOL Latino is an award-winning bilingual portal providing original programming and exclusive coverage of events and issues that matter to the U.S. Hispanic community; ***AOL News***–Read watch react: and interact. AOL News delivers the day's top stories to the most engaged news audience on the web; ***Black Voices***–Black Voices offers a fresh African-American perspective on news, entertainment, lifestyle, finance and more; ***Lifestyle***–The busy woman's destination for must-reads on food, health, style, family and home; ***Mydaily***–MyDaily helps today's women stay informed by providing the content they love in a smart, lively format; ***Patch***–Patch is dedicated to providing comprehensive and trusted local news coverage for individual towns and communities; ***Tuvoz***–A site for Latinas, by Latinas, Tu Voz empowers Hispanic women everywhere to get the most out of life.

Video: AOL Television–Packed with exclusive content and up-to-the-minute TV listings, AOL Television is the web's deepest resource for what's on, what's hot and what's happening in the world of television; ***Cinematical***–Cinematical is the in-depth movie blog for the fan, by the fan; ***Moviefone***–Moviefone is the web's premier destination for film news, celebrity interviews, movie trailers, showtimes and more; ***SlashControl***–Watch thousands of TV shows and hundreds of movies free, anytime, on Slash-Control; ***Truveo***–With hundreds of millions of videos in its index, Truveo is one of the web's most popular video search engines; ***Video***–The only complete online video solution, with premium content, brand-safe distribution, effective targeting and contextual relevance; ***Winamp***–The ultimate media player for consumers and advertisers alike, Winamp lets users manage and play audio/video files, rip and burn CDs, listen to free music, share music with friends, and much more.

25. Through AOL Video (including AOL Television), AOL offers consumers "millions of free, high quality videos including music videos, news clips, movie trailers, viral videos, and full-length TV shows."[3] AOL's video content includes original offerings, such as its 2005 Emmy-winning online broadcast of "Live 8 on AOL" following the Live 8 world poverty awareness concert.

26. Since 2006, advertising has been AOL's primary revenue generation focus.

27. AOL delivers advertisements and advertising-related services through Website content, video content, brand advertisements, online ad-serving, and sponsored listings through: the consumer-facing content and services described in paragraphs 23 and 24, above; 5min Media; ADTECH (international ad-serving); Advertising.com network of third-party Websites; buy.at (affiliate marketing); goowy (developer tool for widgets and customized desktops); goviral (distribution of branded video content); Pictela (high-resolution branded video content); Quigo (site and content-targeting); TACODA ("audience insights" and behavioral targeting); Third Screen Media (mobile advertising); and Video (including the consumer-facing AOL Video).

28. AOL sells advertising services to enable advertisers to target particular audiences, such as moms, men 18-34 years of age, teens, African Americans, Hispanics, affluents, boomers, and "influencers."

29. AOL sells advertising services designed to meet the needs of particular types of promotions, such as political campaigns, with online advertising for fundraising, awareness,

---

AOL-branded Websites also include sites with content focused on games, entertainment, music, travel, and child and youth-oriented content.

[3] http://www.insideaolvideo.com/.

campaign organization and field management, persuasion, rapid response, "get out the vote," and issue advocacy.

30. AOL was a minority investor in Brightcove until earlier this year.

IV. JURISDICTION AND VENUE

31. This Court has diversity jurisdiction in this case under the Class Action Fairness Act, 28 U.S.C. §1332(d)(2). This complaint states claims on behalf of a national classes of consumers who are minimally diverse from Defendants. The amount in controversy exceeds $5 million, exclusive of interest and costs. The Classes (as defined herein) consist of more than one hundred members.

32. This Court also has federal question jurisdiction under 28 U.S.C. §1331 as this action arises in part under a federals statute, including the Computer Fraud and Abuse Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.

33. This Court has supplemental jurisdiction with respect to the pendent state law claims under 28 U.S.C. §1367.

34. This Court has personal jurisdiction over Defendants because some of the acts alleged herein were committed in the state of Massachusetts and because AOL is registered to do business in this state and systematically and continuously conducts business here.

35. Venue is proper in this District under 28 U.S.C. §1391(b) because ScanScout is a corporation headquartered in Boston, Massachusetts. Defendant Brightcove is headquartered in Cambridge, Massachusetts. In addition, AOL maintains an office in this district.

V. GENERAL ALLEGATIONS

A. Background

36. Plaintiff includes these background allegations to provide context for her allegations that the browser privacy controls circumvented by Defendants are material to Plaintiff and

Class Members' ability to protect their online privacy interests and ownership interests in their information and computer assets.

i. Widespread online tracking originated with the release of browsers configured to accept unverified, third-party cookies by default.

37. Browsing the Web consists of a series of stateless communication exchanges, that is, no active state of connection exists between a Website and a consumer visiting that Website. Instead, a Web communication consists of a request-and-respond exchange over the Internet between the consumer and a Website.[4] Each consumer's "click" is a standalone request from the consumer's Web-browsing software,[5] asking for a Web page to be downloaded: via the Internet, the consumer's browser transmits a request for a Website to download a particular Web page; the Website responds by downloading a file containing the requested Web page to the consumer's computer.

38. Because of statelessness on the early Web, there was no generally accepted way for a Website to tell if the visitor requesting a Web page was the same one who, moments before, had asked for another page. Unless the Website required its visitors to register and log in, a visitor could not be recognized from one session to another. Within a visitor's "session" browsing an e-commerce Website, reliable, online shopping cart functions were not practical.

39. In 1994, Netscape addressed statelessness by adding a feature to its Netscape Navigator browser, enabling the browser to accept cookies[6] from Websites and store them on consumers' computers.

---

[4] Allegations of this complaint use the term "Website" to refer to "Website's servers" or "Website's owner/operator."

[5] Web-browsing software, or a "browser," is software installed on a user's computer with which the user, by communicating through an electronic network such as the Internet, can access Websites.

[6] A cookie is a small string of text transmitted by a server to the user's browser. For purposes of this complaint, a cookie is described as being linked to an individual. Technically, a cookie is associated with a particular browser installed on a particular computer, although this distinction has been made less relevant

40. Cookies allow a Website to use a consumer's Internet connection, browser software, and computer processing and storage to create and read data of its own choosing on her computer whenever the consumer downloads a Web page.

41. Often, the Website a consumer visits—a "first-party" Website—may choose to incorporate other Websites' content into its Web pages. For example, a news Web page from a news site may also display related news images from a photo service Website and advertisements from an ad display service. In relation to the first-party Website, the Websites providing the added content are "third-party" Websites.

42. When a first-party Web page incorporates third-party content, the first-party Web page essentially instructs the consumer's browser to fetch the third-party content from the third party's Website. This action gives the third party the ability to set and read cookies on the consumer's computer.

43. When cookies were in their infancy and the standards body for Internet communications, the Internet Engineering Task Force (IETF), assessed the ability of third parties to set cookies, it labeled them "unverified transactions." Third-party cookies were considered unverified because, before a consumer views a Web page, she has no way of knowing in advance what third parties might be setting cookies and for what reason.[7] Once the consumer views the Web

---

by advanced tracking capabilities enabling Tracking Companies to distinguish among users of the same computer. A cookie contains whatever information the Website decides to store in it. A Website may use a cookie to remember user information, such as a zip code provided by the user for viewing the local weather each time the user visits the Website. The Website can store a unique identifier in a cookie, so it can recognize a click as coming from a particular user.

[7] "HTTP Cookies: Standards, Privacy, and Politics," David M. Kristol, 2001, p. 11, available at http://arxiv.org/abs/cs/0105018.

page, the third party's cookies have already been set. The IETF's position was that third-party cookies posed risks to consumers' privacy and security.[8]

44. The IETF standards for browsers' handling of cookies specified that browsers should be configured to reject third-party cookies by default.[9]

45. In 1997, Netscape committed to abide by the IETF's standard.[10]

46. However, by the end of the 1990s, the leading browser makers of the time, Netscape and Microsoft, were distributing browsers that accepted third-party cookies by default.

47. With the dominant browsers in the market defaulting to acceptance of third-party cookies, online advertising companies were able to engage in widespread "network advertising" and tracking by delivering ads to many Websites.

ii. The scale and methods of tracking have grown.

48. The numbers and types of companies that participate in tracking consumers online have grown over the past ten years (*see* n.1, p. 2, above). In 1999, the Network Advertising Initiative (NAI), an online ad industry organization, was formed with ten members. In 2001, one of the NAI members, DoubleClick served ads on a network of fewer than 12,000 Websites.

49. In 2009, Google, which acquired DoubleClick, served ads on a network of millions of Websites and, today, the NAI has 74 members. Other sources indicate far greater num-

[8] In addition to the privacy risks of online tracking, the downloading of any Web content from an unknown source increases the consumer's risk of privacy and security threats such as screen-scraping, browser history sniffing, and malicious code installation and execution.

[9] "RFC 2965, HTTP State Management Mechanism," Kristol and Montulli, Internet Engineering Task Force, Oct. 7, 2000, available at http://www.ietf.org/rfc/rfc2695.txt.pdf; "RFC 2964, BCP (Best Current Practice) 44, Use of HTTP State Management," Moore and Freed, Internet Engineering Task Force, Oct. 12, 2000, available at http://www.ietf.org/rfc/rfc2964.txt.pdf.

[10] Testimony of Peter Harter (Global Public Policy Counsel, Netscape Comm. Corp.), *In the Matter of: Public Workshop On Consumer Information Privacy; Session 2, Consumer Online Privacy*, Federal Trade Commission at 139, June 11, 1997, available at http://www.ftc.gov/bcp/privacy/wkshp97/volume2.pdf.

bers of companies that participate in tracking consumers online ("Tracking Companies")—as many as 281.[11]

50. Tracking Companies track consumers visiting Web pages, opening e-mails, and through toolbars installed as browser plug-ins. New tracking technologies include "widgets"—portable, mini-Web pages, such as a video clip a radio tuning button tool the consumer can snag, drop into an email, paste into a blog, or post on a social network page. Other consumers can then snag the widget and share it further, along with its tracking capabilities.

51. Metrics/analytics Tracking Companies track consumers across huge networks of Websites and through the pieces of third-party content incorporated into those Websites. Metrics/analytics companies invite Websites to "measure your audience" and, then, "sell your audience" to advertisers looking for consumers likely to be interested in their ads. A consumer may be tracked from the moment she is shown a Web ad for a product to her purchase of the product many days later on a different website.

52. Within a given Web page, specialty technologies track whether and where a consumer clicks on a Web page and even where the consumer moves her mouse on a page, even if she does not click on anything.

53. Companies that have access to online consumers, space in which to place an ad, and ads looking to be served now meet in online exchanges. The moment a consumer connects to the Internet and appears on a Website, Tracking Companies make offers and bid against each other in automated, real-time auctions for the chance to track, profile, and target the consumer.

iii. Web-browsing has become less anonymous.

54. Many Tracking Companies claim their profiles are anonymous.

[11] *Evidon Open Data Partnership*, available at http://www.evidon.com/consumers/profile_manager#tab3.

55. It is contrary to industry standards to "de-anonymize" a consumer's profile data by inferring identity from multiple data points or linking anonymous data with personally identifiable information (PII).[12]

56. However, many Tracking Companies profiles are detailed enough to enable them to purchase other profile data about a specific consumer—including non-public data about an individual consumer's online and offline shopping history, interests, and demographic details such as income, education, family status, type of vehicle driven, and location of residence and work. The Tracking Companies that buy this data use it to "enhance" their consumer profiles.

57. As noted by the NAI:

> While advertising networks do collect data on consumers who view their advertising, this data is often anonymous. However, profiles derived from tracking consumers' activities on the Web can be linked or merged with "personally identifiable information" (PII). It can also be combined with offline purchase data or information collected via a survey, census, or registration form.

FAQs, NAI, available at http://www.networkadvertising.org/managing.

58. One information broker, Rapleaf, reportedly maintains profiles that include age, gender, and location for over 70 percent of active U.S. e-mail users. Rapleaf responds to over a billion monthly requests from business seeking profile details. The profiles Rapleaf maintains incorporate information culled from voter-registration files, shopping histories, and social-networking Website activities.

[12] In 2009, Defendant AOL unintentionally demonstrated how easily data that is supposedly anonymous can be de-anonymized. AOL's research department publicly released a compressed text file containing twenty million search keywords for over 650,000 users over a three-month period. AOL had supposedly anonymized the data by scrubbing identification information and Internet Protocol (IP) addresses. Reporters were able to identify specific individuals whose searches were included in the AOL database. *See*, Michael Barbaro, Tom Zeller, Jr., "A Face Exposed for AOL Searcher No. 4417749," *New York Times,* Aug. 9, 2009.

59. Consumers' profiles are used and marketed for more than ad-targeting. For example, Websites use profile information to decide what content to present to a consumer. That means two consumers making the same search request about a breaking news event may see not just different ads, but different search results.

60. Another example, discriminatory pricing, was illustrated in 2000, when Amazon.com came under fire for charging returning customers more then new customers for the same CD.[13]

61. Recently, Media6Degree's CEO reportedly stated that banks would find Media6Degrees' conclusions of interest in assessing consumers' creditworthiness; Media6Degrees derives inferences about particular consumers' characteristics by comparing their browsing patterns with those of other consumers whom it has already profiled.

iv. Tracking and trafficking in consumer data are invisible to consumers.

62. While a Tracking Company can watch a consumer across the consumer's visits to many Websites, the converse is not true. Tracking Companies are invisible and their actions are "nontransparent"; consumers cannot see what is being collected from them and how it is being used or, often, by whom.

63. As the NAI stated in its FAQs (*id.*):

> All that consumers see are the Websites they visit and the advertising that is shown on those Websites. Unless the Websites visited by consumers provide notice of the ad network's presence and data collection, consumers may be unaware that their activities online are being monitored.

64. Consumers who want to learn anything about how they are being tracked face an impossible task. It is not uncommon for a Web page to include content, ads, and other tracking devices from Tracking Companies numbering in the double digits.

[13] *Web sites change prices based on customers' habits,* Anita Ramasastry, Findlaw Law Center on CNN.com (June 24, 2005), http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.

65. The specific identifies of these Tracking Companies are not likely to be specifically identified in the Website's privacy policy.

66. In fact, given the nature of real-time exchanges, the Website may not know which Tracking Companies of the many types of Tracking Companies (*see* n.1, p. 2, above) are present on or receiving consumer data from their Web pages.

67. The consumer can try to locate industry associations to which Tracking Companies belong, but that does not tell the consumer who is tracking her, where, or how.

68. On an industry association's website, such as the NAI, the consumer can, however, opt out of tracking by the association's members, but: with the NAI's 74 members, hundreds of tracking companies do not participate in the NAI's opt-out program and some do not participate in any opt-out program. Therefore, the consumer is left with no assurance of having exercised an opt out that covers the field.

69. In addition, the NAI website promises only that, by opting out, its member Tracking Company "will no longer deliver ads tailored to your Web preferences and usage patterns." This is a promise to refrain from displaying targeted ads, but it is not a promise to refrain from tracking.

70. Further, enrolling in an opt-out program requires that the consumer have her browser controls set to accept third-party cookies, which exposes the consumer to tracking by any third-party Tracking Company for which she cannot fully opt out of tracking.

v. Consumers have limited resources for controlling tracking and no resources for controlling trafficking.

71. As alleged above in paragraph 46, early browser makers configured their browser defaults to allow Websites to use consumers' computers and Internet connection to set cookies

and track consumers. This shifted the burden to consumers who, if they did not want to be tracked, had to manually override the default browser controls.[14]

72. Since persistent, third-party browser cookies remain the primary vehicle for online tracking of consumers, the most effective means available to a consumer to say "no" is by changing her default browser controls to a setting that blocks or deletes persistent browser cookies, particularly third-party cookies. (This does not prevent all tracking, which can also be conducted by first-party Websites, but rejecting first-party cookies may cause the Websites the consumer visits not to function properly.)

73. In the context of the online tracking and trafficking ecosystem, a consumer's ability to use or rely on her browser controls to to block and delete browser cookies is critical, particularly because, as discussed above: (a) online tracking is invisible, pervasive, and not adequately disclosed; (b) trafficking in data collected from consumers, including personally identifiable information, is invisible, pervasive, and not disclosed at all; (c) online tracking and trafficking depends on the invisible use of consumers' computers, software, and connectivity; and (d) consumers' ability to block or delete browser cookies is the most effective option available to consumers for controlling tracking across their Web-browsing activities.

74. By some estimates, as many as 30 percent of consumers delete cookies on a monthly basis and approximately 12 percent block cookies completely.[15]

---

[14] Since the release of the first cookie-enabled browsers, Apple has released its Safari browser configured to block third-party cookies by default (expressed as "accept cookies only from sites I visit.)"

Conversely, in early 2008, Microsoft reportedly decided not to implement design changes for Internet Explorer 8.0 that would have automatically prevented tracking by default. The Internet Explorer product team strongly advocated for the changes but were unsuccessful due to internal opposition because of Microsoft's online advertising business and external pressure from online advertising industry members. *What They Know: Microsoft Quashed Effort to Boost Online Privacy*, N. Wingfield, Wall Street Journal, Aug. 2, 2010, available at http://online.wsj.com/article/SB10001424052748703467304575383530439838568.html.

[15] *The Impact of Cookie Deletion on the Accuracy of Site-Server and Ad-Server Metrics: An Empirical ComScore Study*, M. Abraham, C. Meierhoefer, A. Lipsman, ComScore, Inc., June 2007, available at

75. Thus, consumers' ability to use and rely on their browser controls to block and delete browser cookies is material to them in protecting their privacy interests online and keeping their computers, software, and connectivity from being used to diminish and invade those interests.

B. Plaintiff and Class Members' used their browser privacy controls to prevent tracking.

76. Plaintiff and Class Members value their privacy while Web-browsing.

77. Plaintiff and Class Members have a reasonable expectation of privacy while Web-browsing.

78. Plaintiff and Class Members do not want to be tracked online.

79. Plaintiff and Class Members do not want to be tracked for the sake of seeing tracking-based, "behaviorally targeted" online ads.

80. Plaintiff and Class Members believe their Web-browsing is private and not the business of anyone except the Website with which they choose to communicate.

81. Plaintiff and Class Members consider many of their online communications to involve their personal information—information of a private, confidential, sensitive, and intimate nature involving personal and professional matters such as finance, health, politics, religion, family and relationship matters and events, and other matters regarding which they protect their communications from disclosure to others.

82. Plaintiff's online communications included such information, both her own and of persons with whom she corresponded.

---

http://blog.comscore.com/2007/06/comscores_cookie_deletion_whit_1.html (site registration required).

83. Plaintiff and Class Members believe their decisions to disclose or not disclose information when they view a particular Web page, select content or options on the page, or enter information on the page, is their decision to make.

84. Plaintiff and Class Members believe the information they disclose online is an asset they possess and to which online third parties have no presumptive right of access.

85. Plaintiff and Class Members believe their computers, Internet connectivity through their ISPs, and software installed on their computers ("Computer Assets")—are theirs to use and control, to preserve their privacy and for other reasons, such as preventing unwanted communications from diminishing the speed of their Internet connections.

86. Plaintiff and Class Members believe their Computer Assets are assets they pay for, possess, and/or to which they enjoy a right of possession and use.

87. Plaintiff and Class Members believe online parties with whom they have not chosen to communicate have no presumptive right to access or use Plaintiff and Class Members' Computer Assets.

88. Plaintiff and Class Members' ability to block and delete browser cookies is material to them in protecting their privacy interests and keeping their Computer Assets from being used in ways Plaintiff and Class Members' do not want their Computer Assets used, including to diminish and invade their privacy interests.

89. To avoid being tracked online, Plaintiff and Class Members used and relied on their browser controls to block and/or delete browser cookies from Tracking Companies, including Defendants.

90. Since approximately 1997, typically approximately five times a week, Plaintiff used her browser controls to delete browser cookies on her computer (which AOL described as

"small files kept on your computer that websites use to track your visits") and clear her browsing history, browser cache; blocked pop-ups list, saved thumbnail images, and search history.

91. Plaintiff did so to protect her privacy interests and to improve the performance of her computer while she browsed the Web.

92. Plaintiff continued to pay AOL a subscription fee and continued to use the AOL Explorer browser available through AOL's online portal because of her familiarity with and the ease of use of the AOL Explorer browser controls ("Clear AOL Explorer Footprints") and her trust that the controls would operate as AOL represented.

93. Plaintiff and Class Members reasonably expected their browser controls to block or delete cookies, preventing them from being tracked online, profiled, and served behaviorally targeted advertisements.

94. Last summer, Plaintiff bought chair pads for her kitchen chairs while shopping at a large chain grocery store. At a self-service checkout kiosk, she swiped her store loyalty card and paid for the chair pads with a credit card and also swiped her store loyalty card. Shortly after Plaintiff returned home with her purchase, she checked her e-mail. She was very surprised to receive a Web-enabled e-mail message containing an advertisement from an online merchant for the same chair pads she had just bought.

95. Plaintiff subsequently discovered that, despite her use of browser controls, Defendants had been tracking her online activities and had stored a number of files on her computer.

96. The files Defendants stored on her computer were not browser cookies. They were Adobe Flash Local Stored Objects (LSOs).

C. Defendants' Employed Flash Exploits to Circumvent Plaintiff and Class Members' Browser Privacy Controls.

97. Adobe Flash Player software is installed on the majority of U.S. consumers' computers, including those of Plaintiff and Class Members.

98. When a consumer downloads a Web page that contains video content designed to be displayed using Flash software, the Adobe Flash Player software installed on the consumer's computer can be used to display the video content on the Web page. Adobe has stated that, worldwide, over 75 percent of online videos and over 70 percent of Web-based games utilize Flash technology.[16]

99. When a Website incorporates content displayed using Flash technology, the site can store files called local shared objects ("LSOs") on the computer of a consumer using Flash Player; Adobe Corporation has stated that LSOs were designed to support consumers' ability to experience "rich Internet application" content using the Adobe Flash Player.[17]

100. An LSO stored on a consumer's computer can retain the consumer's score for an online video game, so the consumer can resume playing at another time. An LSO can be used to store a consumer's audio volume preferences for playing news clips on the Web pages a consumer downloads from a news Website.

101. Defendants stored LSOs on Plaintiff and Class Members' computer for a different purpose; they used LSOs as substitutes and back-ups for browser cookies.

102. Defendants used LSOs as substitutes and back-ups for browser cookies to circumvent the browser controls Plaintiff and Class Members had set to block or delete browser cookies, so Defendants could track and profile Plaintiff and Class Members.

---

[16] Letter to FTC, Adobe Systems Inc., Jan. 27, 2010, available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf.

[17] *Id*.

103. When LSOs are used the way Defendants used them—as backups and/or substitutes for browser cookies—they are sometimes rhetorically referred to as "Flash cookies," but they are not cookies.

104. On Plaintiff's computer, she discovered LSOs set by AOL dating back to 2006, including LSOs for AOL's ad network and other, third-party Tracking Companies.

105. On Plaintiff's computer, she discovered LSOs set by Brightcove dating back to 2009, including one in which Brightcove set an LSO for another third party tracking and including several in which Brightcove set LSOs for AOL, including for its advertising network.

106. Defendants used the LSOs they stored on her computer as an alternative to browser cookies for tracking Plaintiff and Class Members."[18]

i. ScanScout

107. Defendant ScanScout circumvented Plaintiff and Class Members' browser controls, stored Flash LSOs on their computers, and used the Flash LSOs and Plaintiff and Class Members' Computer Assets to track Plaintiff and Class Members against their express prohibition.

108. ScanScout stored approximately four to seven LSOs on each of the computers of Plaintiff and Class Members whose computers it accessed, using these LSOs in place of and as backups for browser cookies.

109. On Plaintiff's computer, she discovered tracking LSOs set by ScanScout dating back to 2008.

110. The names of some LSOs stored by ScanScout indicate ScanScout used them in place of cookies to track its display of advertising to Plaintiff and Class Members, track Plaintiff

[18] Defendants' use of LSOs as an alternative or back-up for cookies was independently confirmed. *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.

and Class Members' activities, and override their browser controls over the creation and use of cookies, *e.g.*, "SS_ARE_BrandAdHistory.sol," "SS_ARE_CampaignHistory.sol," "SS_ARE_CatFreqHist.sol," "SS_ARE_UserData.sol," and "SS_ARE_CookieJar.sol."

111. In addition, the names of other LSOs stored by ScanScout on Plaintiff and Class Members' computers show that ScanScout stored cross-domain LSOs, that is, it stored LSOs on Plaintiff and Class Members' computer not for its own use, but for use by yet other third-party Tracking Companies. Those Tracking Companies then used the LSOs for their own tracking purposes, outside of ScanScout's control, *e.g.*, "com.quantserve.sol" (which is the name of an LSO used by third-party advertising and metrics Tracking Company, Quantcast, Inc.).

ii. Brightcove

112. On Plaintiff's computer, she discovered numerous Brightcove tracking LSOs.

113. Like ScanScout, these included cross-domain LSOs that Brightcove set for other companies, including Quantcast.

114. Scores of other Tracking Companies are partners in Brightcove's "alliance," through which Brightcove facilitates these Tracking Companies' ability to use its technology and domain name to display the Tracking Companies' videos online.

115. In essence, Plaintiff and Class Members visited Websites that included video content; the Websites, themselves, that may or may not have known that advertisements were being delivered to their visitors using Brightcove technology; neither Plaintiff, Class Members, nor the Websites were aware Brightcove was repurposing Plaintiff and Class Members' Flash software and using their Computer Assets to set tracking LSOs; and neither Plaintiff, Class Members, nor the Websites were aware that LSOs deposited by Brightcove sometimes resulted in tracking of Plaintiff and Class Members by yet another Tracking Company.

iii. AOL

116. One of the Tracking Companies for which Brightcove set LSOs on Plaintiff and Class Members' computers was Defendant AOL.

117. In addition, AOL set its own LSOs on Plaintiff and Class Members' computers. The names of some of these LSOs indicated that AOL used them to override Plaintiff and Class Members' browser controls, using the LSOs in place of cookies for its advertising and tracking purposes, *e.g.*, "UID.sol" ("UID" is a common abbreviation for "user ID") and "lightningcast.sol" (Lightningcast was an online video/audio ad technology company acquired by AOL in 2006).[19]

118. Some LSOs set by AOL on Plaintiff and Class Members' computers were named "AOL_ComScore.sol," indicating that AOL was using the LSOs to track Plaintiff and Class Members and reporting their activities to ComScore for analysis of visitor traffic on AOL Websites and viewership of ads served by AOL.

iv. AOL's disclosure records of audiovisual goods and services

119. AOL used LSOs to collect information about Plaintiff and Class Members' online activities and combined that information with clickstream data from Plaintiff and Class Members' activities while on AOL Websites or viewing AOL-supplied online content on other Websites (the combination being "Enhanced Clickstream Data").

120. AOL transmitted Enhanced Clickstream Data of Plaintiff and Class Members' online activities to other Tracking Companies and/or analytics/metrics Tracking Companies.

[19] In contrast, AOL set LSOs that appear, based on their file names, to comport with consumers' reasonable expectations regarding the use of LSOs and their Flash software, Examples include "volume.sol," which would support expected Flash uses if it is indeed used to retain a consumers' desired volume control setting; and R20PLAYER.sol, which appears to be used to support a consumer's ability to listen to AOL's online broadcasts of CBS Radio.

121. The Enhanced Clickstream Data also included Plaintiff and Class Members' personally identifying information.

122. In addition, the Enhanced Clickstream Data included information about Plaintiff and individual Class Members' gender; income; which Websites they were visiting before they clicked on AOL-owned websites or AOL-provided content or ads; which Websites they visited after leaving AOL-owned websites; and other personal details.

123. AOL offers a great deal of video content to consumers and, through its advertising, has access to further information about consumers' video choices. *See* ¶¶24-29, above.

124. AOL's video services include providing the ability for a consumers to customize AOL Website pages with content, including video content, relating to topics of interest to the consumer.

125. Plaintiff frequently selected video content offered on AOL's portal Web page, including news-related videos and videos of highlights from SEC football games.

126. Plaintiff and Class Members' requests for specific video materials and/or services and/or obtaining of specifically requested video materials and/or services were included in the Enhanced Clickstream Data that AOL transmitted to other Tracking Companies and/or analytics/metrics Tracking Companies.

127. The analytics/metrics Tracking Companies and/or other Tracking Companies to which AOL disclosed Plaintiff and Class Members' Enhanced Clickstream Data used the Enhanced Clickstream Data, including Plaintiff and Class Members' video and/or video services requests, for purposes other than AOL's fulfillment of Plaintiff and Class Members' requests for video materials and/or services.

128. Plaintiff and Class Members did not consent to such disclosure and reasonably expected that AOL would not disclose their video and/or video services requests to analytics/metrics Tracking Companies and/or any other Tracking Companies.

129. Plaintiff and Class Members did not authorize AOL to disclose their video and/or video services requests to analytics/metrics Tracking Companies and/or any other Tracking Companies.

D. Scope and characteristics of Defendants' use of LSOs

130. Because of the expansive "reach" of Defendants, that is, their presence on a significant number of frequently visited, U.S. websites, their circumvention of browser controls affected Plaintiff and Class Members across a significant amount of their web-browsing so that, when they thought they had foreclosed being tracking, they were being tracked far and wide.

131. Defendants' setting of LSOs and tracking were invisible to Plaintiff and Class Members as well as to the Websites with which Plaintiff and Class Members communicated.

132. In addition, Defendants' conduct was designed specifically to circumvent Plaintiff and Class Members' browser privacy controls.

133. Defendants circumvented Plaintiff and Class Members' browser privacy controls because those controls were Plaintiff and Class Members' primary means of preventing online tracking and because Defendants wanted to override Plaintiff and Class Members' controls and track Plaintiff and Class Members.

134. Defendants intentionally circumvented Plaintiff and Class Members' browser privacy controls, knowing that Plaintiff and Class Members used and reasonably expected those controls to protect their privacy interests.

135. Defendants disclosed these processes neither to Plaintiff and Class Members nor to the Websites with which Plaintiff and Class Members communicated.

136. Defendants' actions were surreptitious and without notice and so were conducted without authorization and/or exceeding authorization.

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

138. Only Plaintiff and Class Members possessed the authority to consent to the bypassing of their browser privacy controls.

139. Because Defendants' actions were invisible, undisclosed, and unexpected, Defendants did not receive any valid consent for their actions.

140. Defendants' tracking was therefore conducted without the consent of any party to the communications between Plaintiff and Class Members, and the Websites they visited.

141. In addition to the Enhanced Clickstream Data collected by AOL, all Defendants collected details of Plaintiff and Class Members' Web-browsing across the many Websites on which Defendants encountered Plaintiff and Class Members; those details included which Web pages Plaintiff and Class Members had visited inside and outside of Defendants' tracking networks; information Plaintiff and Class Members provided on the Web pages; search requests; uniquely identifying information permitting identification of Plaintiff and Class Members on their visits to other Websites; their browser fingerprints; and, potentially, details of which ads they clicked on and purchases they made, including personal information they provided in making purchases.

142. The information acquired by Defendants and that Defendants caused to be acquired by other Tracking Companies consisted of and included Plaintiff and Class Members' personal information as alleged in paragraph 81, above.

Figure 1. *Comparison of cookies and LSOs*

	Cookies	*Adobe Flash LSOs*
	Characteristics and Operation	
[a]	subject to global standards	subject to Adobe specifications
[b]	set/used only by originating Website	set/used by multiple Websites*
[c]	encrypted if Web page is encrypted	unencrypted; warning messages from user's browser can be suppressed
[d]	4 kilobytes	up to 100 KB by default; may be larger
[e]	expires when user exits browser by default	persistent by default
	User Controls	
[f]	can control through browser	cannot control through browser**
[g]	can identify originating Website	cannot reasonably identify originating Website*
[h]	can view cookie contents	cannot reasonably view LSO contents
[i]	relatively apparent and usable (compared to other options)	not reasonably apparent and usable; constitutes added burden

* Adobe Flash permits cross-domain LSO creation and use, *i.e.*, a Website can set an LSO for another Website, or read another Website's LSO. *See, e.g.*, ¶¶111, 113, *et seq.*, above.

** User must be aware of and use proprietary Adobe tools available on Adobe Website.

143. Adobe Systems Incorporated has stated[20]:

> Adobe does not support the use of our products in ways that intentionally ignore the user's expressed intentions.
>
> . . .
>
> In every case where rich Internet applications are possible, Local Storage is available (and necessary). The Local Storage capability in Adobe Flash Player is equivalent in concept to the emerging Local Storage capabilities in i.e. HTML5 and Silverlight. The fact that Local Storage in these technologies is distinct from the existing browser cookie system and treated as such by the browsers today underscores the need for responsible use of Local Storage in modern Web applications.

[20] *3 Responses to Adobe's small step forward on Flash-cookie control*, posted by Wiebke Lips, Adobe Systems Inc., Jan. 29, 2010, available at http://blog.privacychoice.org/2010/01/29/adobes-small-step-forward-on-flash-cookie-control; *see also Letter to FTC*, Adobe Systems Inc., Jan. 27, 2010, p. 9, available at http://www.ftc.gov/os/comments/privacyroundtable/544506-00085.pdf.

144. On Plaintiff and Class Members' computers, Defendants' LSOs remain stored and available to Defendants for their use.

145. Unlike cookies, for which commercial browsers provide consumers some measure of control, consumers have no reasonable means to block, detect, or delete LSOs and are burdened by other, material differences between cookies and LSO. *See* Figure 1 on page 27, above.

146. Plaintiff and Class Members sought to maintain the secrecy and confidentiality of their personal information assets acquired by Defendants, including by setting and/or relying on their browser controls to block or delete cookies.

E. Harm

147. Defendants acquired personal information to which they were not entitled and which Plaintiff and Class Members had affirmatively sought and reasonably expected to prevent Defendants from acquiring.

148. Defendants' conduct in acquiring such information without authorization or consent has caused and causes economic loss to Plaintiff and Class Members in that the personal information acquired by Defendants has economic value to Plaintiff and Class Members.

149. In addition, Defendants' conduct in acquiring such information without authorization or consent has caused economic loss to Plaintiff and Class Members in that such information has economic value to Plaintiff and Class Members as an asset they exchange for valuable content and services provided by Websites; Plaintiff and Class Members would have blocked Defendants' LSOs, would not have patronized Defendants' Websites, and would have avoided Websites utilizing Defendants' repurposed LSOs; Defendants' conduct has thus imposed opportunity costs on Plaintiff and Class Members, depriving them of the opportunity to exchange their valuable information for the content and services of Websites engaging in practices that comported with Plaintiff and Class Members' reasonable privacy expectations.

150. Defendant's conduct in using Plaintiff and Class Members' Computer Assets to set and use LSOs for tracking Plaintiff and Class Members constituted the unconsented use of Plaintiff and Class Members' Computer Assets, including Internet connectivity, for which Plaintiff and Class Members paid, and so Defendants acquired the use of such assets without payment and thus subjected Plaintiff and Class Members to economic loss.

151. Defendant's unconsented use of Plaintiff and Class Members' Computer Assets, for which Plaintiff and Class Members paid, diminished the performance of Plaintiff and Class Members' computers and Internet connectivity, in that LSO-based methods of information collection require the transfer of larger files using more resource-intensive computer processes that must be completed in sequence during the download of Web pages, causing Web pages to load more slowly than Web pages involving the transfer of cookie values; such diminution in performance of Computer Assets constituted an economic loss to Plaintiff and Class Members.

152. The consequences of the aforementioned conduct also constitute an interruption in service in that they were recurrent, through the Class Period, affecting Plaintiff and Class Members' experiences on numerous Websites.

153. Defendants' conduct has caused economic loss to Plaintiff and Class Members who were AOL subscribers during the Class Period in that they have paid subscription fees to AOL for services that included a browser with functionality that AOL purported would clear cookies, browsing history, and other Web-browsing artifacts from their computers but which, because of Defendants' conduct did not do so, thereby diminishing the value of services for which Plaintiffs and Class Members paid AOL and constituting loss to them.

154. Defendants' use of Plaintiff and Class Members' Computer Assets and collection and use of their personal information in a nontransparent manner, which cannot reasonably be

detected at the time or later discovered, has deprived Plaintiff and Class Members of the ability to protect their privacy and Computer Assets, assess the effects of Defendants' actions on their privacy and Computer Assets, and reasonably undertake self-help measures.

155. Defendants' use of LSOs subjects and/or has subjected Plaintiff and Class Members to additional harm in that, in further circumvention of their browser settings, Defendants have re-spawned cookies that Plaintiff and Class Members deleted, and/or Plaintiff and Class Members face the imminent harm of such re-spawning which, in the case of AOL and ScanScout, was confirmed in reported academic research.[21]

156. The value of Plaintiff and Class Members' losses are discernable through the discovery of information from Defendants and expert evaluation.

VI. CLASS ALLEGATIONS

157. Pursuant to Rules 23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this action pursuant to on behalf of themselves and the following Classes:

a. "LSO Tracking Class"

> All individuals and entities in the United States whose Web browser privacy controls prevented or limited Defendants' persistent storage and use of cookies and on whose computers Defendants stored Adobe Flash Local Stored Objects for Defendants' or others' use in place of or as backups for cookies.

b. "Video Disclosure Class"

> All individuals and entities in the United States who, during the Class Period, whose requests for specific video materials and/or services and/or whose obtaining of specifically requested video materials and/or services, and whose personally identifiable information were disclosed to other persons.

[21] *Flash Cookies and Privacy*, at 3.

158. Excluded from the Classes are Defendants, and their assigns, successors, and legal representatives, and any entities in which Defendants have controlling interests.

159. Also excluded from the Classes are the judge to whom this case is assigned and members of the judge's immediate family.

160. The "Class Period" for the Classes is December 12, 2006 through the present.

161. Plaintiff reserves the right to revise the definitions of the Classes based on facts she learns in the course of litigation.

162. The Classes consists of millions of individuals, making joinder impractical. During the Class Period, on a monthly basis, as many as 50 million individuals viewed AOL content and received AOL LSOs; approximately 1.2 million individuals received Brightcove LSOs; and approximately 2.3 million individuals received ScanScout LSOs.

163. Plaintiff's claims are typical of the claims of all other members of the Classes.

164. Plaintiff will fairly and adequately represent the interests of the Classes. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions, including privacy cases.

165. Plaintiff and her counsel are committed to prosecuting this action vigorously on behalf of the Classes and have the financial resources to do so.

166. Plaintiff and her counsel do not have any interests adverse to those of the Classes.

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

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

169. Defendants have acted and failed to act on grounds generally applicable to Plaintiff and the Classes, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Classes.

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

171. There are many questions of law and fact common to Plaintiff and the Classes and which predominate over any questions that may affect only individual Class Members. Common and predominant questions for the Classes include but are not limited to the following:

a. whether Defendants' circumvented Plaintiff and Class Members' browser controls in placing and using LSOs on Plaintiff and Class Members' computers;

b. whether Defendants' placement and use of LSOs was without consent, without authorization, and/or exceeding authorization;

c. whether Defendants obtained and shared or caused to be obtained and shared Plaintiff and Class Members' personal information through tracking using LSOs Defendants placed on their computers;

d. what personal information of Plaintiff and Class Members was obtained and continues to be retained and used by Defendants;

e. what are the identities of third parties that obtained Plaintiff and Class Members' personal information as a result of Defendants' conduct;

f. whether Defendants' conduct described herein violates the Electronic Communications Privacy Act, 18 U.S.C. 2510, *et seq.*, the Computer Fraud and Abuse Act, 18 U.S.C. §1030 *et seq*., and M.G.L. Ch. 214 §1B, M.G.L. Ch. 93A;

g. whether Defendant AOL's conduct described herein violates the Video Privacy Protection Act, 18 U.S.C. §2710, *et seq.*;

h. whether Defendants' acquisition of Plaintiff and Class Members' personal information and use of Plaintiff and Class Members' Computer Assets harmed Plaintiff and Class Members;

i. whether Defendants' use of Plaintiff and Class Members' Computer Assets damaged and/or diminished the utility and/or value of those Computer Assets;

j. whether, as a result of Defendants' conduct, Plaintiff and Class Members are entitled to equitable relief and/or other relief, and if so the nature of such relief; and

k. whether, as a result of Defendants' conduct, Plaintiff and Class Members are entitled to damages, punitive damages, and/or treble damages.

172. The questions of law and fact common to the Classes 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.

173. Plaintiff's claims for relief include those set forth below.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT TITLE 18, UNITED STATES CODE, SECTION 2510, *et seq.* (Wiretap Act) ON BEHALF OF THE LSO TRACKING CLASS AS TO ALL DEFENDANTS

174. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

175. Each Defendant intercepted Plaintiff and Class Members' electronic communications in that each Defendant executed Flash applications and placed LSO files on Plaintiff and Class Members' computers, which the Defendant used as a device to acquire the contents of communications between Websites and respectively, Plaintiff and Class Members, thereby di-

verting and transferring information containing and constituting the substance, purport, and meaning of Plaintiff and Class Members' communications.

176. Defendants' conduct was in violation of Title 18, United States Code, Section 2511(1)(a) because Defendant intentionally intercepted and endeavored to intercept Plaintiff and Class Members' electronic communications.

177. Defendants' conduct was in violation of Title 18, United States Code, Section 2511(1)(d) in that Defendant used and endeavored to use the contents of Plaintiff and Class Members' electronic communications, knowing and having reason to know that the information was obtain through interception in violation of Title 18, United States Code Section 2511(1).

178. Defendant AOL's conduct was in violation of Title 18, United States Code, Section 2511(3)(a) in that AOL, as an entity providing an electronic communication service to the public and while Plaintiff and Class Members' communication were in transmission on the electronic communications service provided by AOL, intentionally divulged the contents of Plaintiff and Class Members' communications to persons and entities other than the addressees, intended recipients, or agents of addressees or intended recipients.

179. Defendants' conduct was knowing and intentional in that Defendants' designed their processes for setting LSOs and using Plaintiff and Class Members Flash software, and Defendants executed those processes, specifically for the purpose of engaging in the interceptions that Defendants did, in fact, carry out.

180. Defendants were not parties to the respective communications between Plaintiff and Class Members and Websites.

181. Defendants' interception processes were invisible to Plaintiff and Class Members as well as to the Websites with which Plaintiff and Class Members communicated.

182. In addition, Defendants' interception processes were designed specifically to circumvent Plaintiff and Class Members' browser privacy controls that prevented Defendants from collecting Plaintiff and Class Members information through standard and more accepted means, *i.e.*, through the use of browser cookies.

183. Defendants disclosed their interception processes neither to Plaintiff and Class Members nor to the Websites with which Plaintiff and Class Members communicated.

184. Because Defendants' interception processes were invisible and undisclosed, any consent Defendants received to participate in or provide content for communications did not constitute consent to Defendants' interception.

185. Only Plaintiff and Class Members possessed the authority to consent to another party's overriding of their browser privacy controls.

186. Defendants' interception was therefore undertaken without the consent of any party to the communications Defendants intercepted.

187. Further, Defendants' interception was accomplished through their surreptitious and unexpected repurposing of Flash software installed on Plaintiff and Class Members computers, which was not in Defendants' ordinary course of business.

188. Defendants' repurposing of Plaintiff and Class Members Flash software and interception of Plaintiff and Class Members' electronic communications were not necessarily incident to Defendants' rendition of services or protection of rights or property.

189. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members' electronic communications were intercepted and intentionally used in violation of Title 18, United States Code, Chapter 119.

190. Accordingly, Plaintiff and Class Members are entitled to such preliminary and other equitable or declaratory relief as may be just and proper.

191. Plaintiff and Class Members are also entitled to damages computed as the greater of: (i) the sum of actual damages suffered by Plaintiff and Class Members plus Defendants' profits made through the violative conduct herein; (ii) statutory damages for each Class Member of $100 a day for each day of violation; or (iii) statutory damages of $10,000 per individual.

192. Plaintiff and Class Members are also entitled to and request Defendants' payment of punitive damages.

193. Plaintiff and Class Members are also entitled to and hereby request Defendants' payment of reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CLAIM FOR RELIEF
VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT
TITLE 18 UNITED STATES CODE, SECTION 1030, *et seq*.
ON BEHALF OF THE LSO TRACKING CLASS AS TO ALL DEFENDANTS

194. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

195. Defendants created and manipulated its Flash LSOs in storage areas of Plaintiff 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).

196. Defendants knowingly caused transmission of commands to be downloaded to protected computers in that Defendants caused commands to be inserted in Web pages visited by Plaintiff and Class Members, which commands Defendants intended to be transmitted to the computers of Plaintiff and Class Members' when they downloaded Web pages, and which were in fact downloaded to Plaintiff and Class Members' computers.

197. Defendants obtained information from Plaintiff and Class Members' computers, including the information described above in paragraph 141, above.

198. Defendants caused damage to Plaintiff and Class Members in that Defendants circumvented their browser privacy controls, effectively rendering those controls non-operational for all of Plaintiff and Class Members' Web-browsing on the many Websites on which Defendants conducted tracking.

199. Defendants intended to caused such damage in that their tracking technology was designed to disable Plaintiff and Class Members' browser privacy controls.

200. Defendants' access to Plaintiff and Class Members' computers, disabling of browser privacy controls, and taking of information, was without authorization and exceeding authorization in that they circumvented Plaintiff and Class Members' express prohibition against tracking.

201. Defendants' unlawful access to Plaintiff and Class Members' computers, use of their Computer Assets, interruption of their services, and taking of their information was carried out through the same automated process, caused loss as alleged in section V(E), page 28, above, and resulted in an aggregated loss to Plaintiff and Class Members of at least $5,000 within a one-year period.

202. Therefore, Plaintiff and Class Members are entitled to compensatory damages.

203. In addition, Defendants' conduct has caused Plaintiff and Class Members' irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff and Class Members' remedy at law is not adequate to compensate them for these inflicted, imminent, threatened, and continuing injuries, entitling Plaintiff and Class Members to remedies including injunctive relief as provided by 18 U.S.C. §1030(g).

THIRD CLAIM FOR RELIEF
VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
TITLE 18 UNITED STATES CODE, SECTION 2710, *et seq*. (Video Privacy Protection Act)
ON BEHALF OF THE VIDEO DISCLOSURE CLASS AS TO DEFENDANT AOL

204. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

205. Defendant AOL is and was throughout the Class Period engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials in that AOL offered to online consumers prerecorded video programs, including previously released and posted, and originally developed news, entertainment, educational, and general interest video programs, and so was, throughout the Class Period, a video tape service provider as defined in the Video Privacy Protection Act.

206. Plaintiff and Class Members were renters, purchasers, and/or subscribers of goods and/or services from AOL and so were consumers as defined in the Video Privacy Protection Act.

207. As set forth in section V(C)(iv), above, AOL knowingly and without Plaintiff and Class Members' consent disclosed to other Tracking Companies, including analytics/metrics Tracking Companies, Enhanced Clickstream Data, knowing that such disclosure included the disclosure of personally identifying information of Plaintiff and Class Members and their requests for and/or obtaining of specific video materials and/or services from AOL.

208. AOL's actions were therefore in violation of the Video Privacy Protection Act, 18 U.S.C. §2710(b)(1).

209. Plaintiff and Class Members, as to each of them, are entitled to $2,500 in liquidated damages.

210. Plaintiff and Class Members are entitled to equitable relief that includes Defendant AOL's cessation of the conduct alleged herein.

211. Plaintiff and Class Members are entitled to equitable relief that includes an accounting of what records regarding their video materials requests and services were disclosed and to whom.

212. Plaintiff and Class Members are entitled to equitable relief that includes an accounting of AOL's compliance 18 U.S.C. §2710(e), regarding its destruction of personally identifiable information as soon as practicable, but no later than one year from the date the information is no longer necessary for the purpose for which it was collected.

213. Plaintiff and Class Members seek punitive damages.

214. Plaintiff and Class Members are entitled reasonable attorneys' fees and other litigation costs reasonably incurred.

215. Plaintiff and Class Members request such other preliminary and equitable relief as the Court deems appropriate.

FOURTH CLAIM FOR RELIEF
VIOLATION OF THE PRIVACY ACT
MASSACHUSETTS GENERAL LAWS, CHAPTER 214, SECTION 1B
ON BEHALF OF THE LSO TRACKING CLASS AS TO ALL DEFENDANTS

216. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

217. Defendants, each a Tracking Company, circumvented Plaintiff and Class Members browser privacy controls and used Plaintiff and Class Members' Computer Assets to store LSOs on behalf of other Tracking Companies.

218. Through the use of the LSOs, Defendants disclosed to the other Tracking Companies and/or caused to be disclosed to the other Tracking Companies on Plaintiff and Class Members' Web-browsing information, which included facts of a highly private and sensitive information of a personal or intimate nature, as alleged in paragraphs 80 through 84, above.

219. Defendants did so despite the Plaintiff and Class Members' specific prohibitions in their browser privacy controls.

220. Defendants did so repeatedly throughout the Class Period.

221. Defendants did so knowing and intending to engage in conduct that Plaintiff and Class Members did not reasonably expect.

222. Defendants did so knowing Plaintiff and Class Members' had taken reasonable measures to protect their privacy and that Plaintiff and Class Members reasonably believed was protected.

223. Defendants did so intending to circumvent the measures Plaintiff and Class Members' had taken to protect their privacy.

224. Defendants did so knowing their actions would seriously diminish, intrude upon, and invade Plaintiff and Class Members' privacy.

225. Defendants did so intending to seriously diminish, intrude upon, and invade Plaintiff and Class Members' privacy.

226. Defendants did so in a manner designed to evade detection by Plaintiff and Class Members.

227. Defendants had no legitimate, countervailing business interest in engaging in such conduct.

228. Defendants' actions did unreasonably, substantially, and seriously interfered with Plaintiff and Class Members' privacy.

229. In addition, Defendants' conduct has caused and causes Plaintiff and Class Members' irreparable injury. Unless restrained and enjoined, Defendants will continue to commit such acts. Plaintiff and Class Members' remedy at law is not adequate to compensate them for these

inflicted, imminent, threatened, and continuing injuries, entitling Plaintiff and Class Members to remedies including injunctive relief

230. Plaintiff and Class Members are entitled to equitable relief that includes Defendants' cessation of the conduct alleged herein.

231. Plaintiff and Class Members are entitled to equitable relief that includes an accounting of what personal information of theirs was collected, used, merge, and further disclosed to whom, under what circumstances, and for what purposes.

232. As a proximate and direct result of Defendant's invasion of privacy, Plaintiff and Class Members were harmed, including as alleged in section V(E), page 28, above.

233. Plaintiff and Class Members are therefore entitled to damages in an amount to be determined at trial.

234. Plaintiff and Class Members request such other preliminary and equitable relief as the Court deems appropriate.

FIFTH CLAIM FOR RELIEF
VIOLATION OF THE CONSUMER PROTECTION ACT MASSACHUSETTS GENERAL LAWS, CHAPTER 93A ON BEHALF OF THE LSO TRACKING CLASS AS TO ALL DEFENDANTS

235. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

236. During the Class Period, Defendants were engaged in trade or commerce within the meaning of M.G.L. ch. 93A §1.

237. Defendants ScanScout and Brightcove maintain places of business within the Commonwealth of Massachusetts.

238. On October 4, 2010, pursuant to M.G.L. Ch. 93A, Plaintiff, through her counsel, sent a demand letter to Brightcove outlining Plaintiff's allegations and subsequently received a response from Brightcove that did not include a written offer of settlement.

239. On June 27, 2011, pursuant to M.G.L. Ch. 93A, Plaintiff, through her counsel, sent a demand letter to ScanScout outlining Plaintiff's allegations.

240. Defendant AOL does not maintain a place of business or keep assets within the Commonwealth of Massachusetts.

241. Defendants' actions alleged herein constitute unfair and/or deceptive acts or practices in the conduct of trade or commerce within the meaning of, and in violation of, M.G.L. ch. 93A §§2 and 9 as described herein.

242. Defendants' actions described above occurred within the Commonwealth of Massachusetts, including AOL's use of Brightcove's technology and services to store LSOs on Plaintiff and Class Members' computers.

243. Defendants' actions described above have at all times relevant to this action been willing and/or knowing.

244. Pursuant to M.G.L. ch. 93A §9, as a direct and proximate result of Defendants' actions alleged above, Plaintiff and Class Members have no adequate legal remedy, has been irreparably injured, and has suffered monetary damages in an as yet undetermined amount.

245. Plaintiff and Class Members request such other preliminary and equitable relief as the Court deems appropriate.

SIXTH CLAIM FOR RELIEF
TRESPASS TO CHATTEL
ON BEHALF OF THE LSO TRACKING CLASS AS TO ALL DEFENDANTS

246. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

247. Plaintiff and Class Members were, during the Class Period, the owners and/or possessors of computers on which Defendants, surreptitiously and without consent, stored LSOs, whose Computer Assets were used by Defendants to do so, and whose personal information was

collected by Defendants through its use of the LSOs they had stored on Plaintiff and Class Members' computers.

248. Defendants dispossessed Plaintiff and Class Members of the use of their computers, software, and Internet connectivity by commandeering those resources for Defendants' own purposes.

249. Defendants impaired the condition, quality, and value of Plaintiff and Class Members' computers by their circumvention of Plaintiff and Class Members' browser controls, their storage and use of LSOs, and their use of those LSOs to collect and/or cause the collection of Plaintiff and Class Members' personal information.

250. Defendants' conduct constituted an ongoing and effectively permanent impairment of Plaintiff and Class Members' computers in that Defendants' conduct affected Plaintiff and Class Members in a substantial amount of their Web-browsing, throughout the Class Period, through the use of LSOs that continue to reside on Plaintiff and Class Members' computers, and through which Defendants obtained information the use of which they continue to enjoy.

251. Plaintiff and Class Members each had and have legally protected, privacy and economic interests in the their Computer Assets and their personal information.

252. Plaintiff and Class Members sustained harm as a result of Defendants' actions, in that the expected operation and use of their Computer Assets were altered and diminished on an ongoing basis.

253. As a direct and proximate result of Defendants' trespass to chattels, interference, unauthorized access of and intermeddling with Plaintiff and Class Members' Computer Assets, Plaintiff and Class Members have been injured, as described above.

254. Plaintiff, individually and on behalf of the Class, seeks injunctive relief restraining Defendants from further such trespass to chattels and requiring Defendants to account for their use of Plaintiff and Class Members' computer assets, account the personal information they have acquired, purge such data, and pay damages in an amount to be determined.

SEVENTH CLAIM FOR RELIEF
UNJUST ENRICHMENT
ON BEHALF OF THE LSO TRACKING CLASS AS TO ALL DEFENDANTS

255. Plaintiff incorporates the above allegations by reference as if fully set forth herein.

256. Plaintiff and Class Members have conferred upon Defendants a benefit, including the money derived from the use of Plaintiff and Class Members Computer Assets, personal information, patronage of Defendants' Websites and advertiser clients, subscription fees (as to AOL), and which benefit Defendants would not have acquired but for their wrongful acts and practices, which benefit belongs to Plaintiff and Class Members and which money has been retained by Defendants through their wrongful acts and practices.

257. Defendants unjustly gained money and other benefits from Plaintiff and Class Members as a direct result of their conduct.

258. Defendants appreciate and has knowledge of said benefit.

259. Under principles of equity and good conscience, Defendants should not be permitted to retain the money and other benefits it acquired through its unlawful conduct. All funds, revenues, and benefits received by them rightfully belong to Plaintiff and Class Members, which Defendants have unjustly received as a result of their actions.

VII. PRAYER FOR RELIEF

Plaintiff, individually and on behalf of all others similarly situated, prays for the following relief:

A. Certify this matter as a class action.

B. Enter judgment in favor of Plaintiff and Class Members.

C. Enter injunctive and/or declaratory relief as is necessary to protect the interests of Plaintiff and Class Members, including reformation of practices and an accounting and purging of wrongfully obtained personal information;

D. Award statutory damages to Plaintiff and Class Members.

E. Award compensatory damages to Plaintiff and Class Members in amounts to be proved at trial.

F. Award restitution against Defendants in amounts to be proved at trial.

G. Award increased and/or treble damages in amounts to be proved at trial.

H. Award liquidated damages in amounts to be proved at trial.

I. Award punitive damages in the interest of justice.

J. Award disgorgement of monies obtained through and as a result of unfair and/or deceptive acts and/or practices and/or unjust enrichment, in amounts to be proved at trial.

K. Award Plaintiff and Class Members pre- and post-judgment interest to the extent allowable.

L. Make such orders or judgments as may be necessary to restore to Plaintiff and Class Members any money and property acquired by Defendants through wrongful conduct.

M. Award Plaintiff and Class Members reasonable litigation expenses and attorneys' fees.

N. Award such other and further relief as equity and justice may require or allow.

VIII. JURY REQUEST

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

Dated: June 28, 2011

Respectfully submitted,

By: /s/ Konstantine Kyros

Konstantine Kyros
konstantine@kyrospressly.com
Kyros & Pressly LLP
60 State Street, Suite 700
Boston, Massachusetts 02109
Telephone: 1-800-934-2921
Facsimile: 1-800-711-7030

Scott A. Kamber
skamber@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3071
Facsimile: (212) 920-3081

David A. Stampley
dstampley@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3071
Facsimile: (212) 920-3081

Grace E. Parasmo
gparasmo@kamberlaw.com
KamberLaw, LLC
100 Wall Street, 23rd Floor
New York, New York 10005
Telephone: (212) 920-3071
Facsimile: (212) 920-3081

Joseph H. Malley
malleylaw@gmail.com
Law Office of Joseph H. Malley
1045 North Zang Blvd
Dallas, Texas 75208
Telephone: (214) 943-6100

Attorneys for Plaintiff