

**FILED**  
**IN THE UNITED STATES DISTRICT COURT**  
**FOR THE NORTHERN DISTRICT OF ALABAMA**  
**2010 FEB -3 PLEASANTON EASTERN DIVISION**

**U.S. DISTRICT COURT**  
**N.D. OF ALABAMA**  
SAMUEL GREEN, et al., and )  
on behalf of himself and all others )  
similarly situated, )

*Plaintiffs,* )

v. )

CABLE ONE, INC., a Delaware )  
Corporation, )  
*Defendant.* )

N

CV-10-HS-0259-F

**Jury Trial Demanded**

**CLASS ACTION COMPLAINT**

Plaintiff Samuel Green (“Plaintiff”), on behalf of himself and all others similarly situated (the “Class” and each a “Class Member”), by and through his attorneys, Kenneth S. Nugent, P.C., KamberLaw LLC, Panish, Shea & Boyle, LLP, the Law Office of Joseph H. Malley, P.C., and Parisi & Havens LLP, as and for Plaintiff’s complaint and demanding trial by jury, allege as follows upon personal knowledge as to himself and his own acts and observations and, otherwise, upon information and belief based on the investigation of counsel and which Plaintiff believes further investigation and discovery will support with substantial evidence.

**NATURE OF THE CASE**

1. In late 2007, Cable One, Inc. (“Cable One” or “Defendant”) began installing spyware devices on its broadband networks. Cable One continued using

the spyware devices through early 2008. The devices funneled all affected users' Internet communications—inbound and outbound, in their entirety—to a third-party Internet advertisement-serving company, NebuAd.

2. NebuAd and Cable One used the intercepted communications to monitor and profile individual users, inject advertisements into the web pages users visited, transmit code that caused undeletable tracking cookies to be installed on users' computers, and forge the "return addresses" of user communications so their tampering would escape the detection of Users' privacy and security controls.

3. Historically, "spyware" is term that has been applied to software installed on users' personal computers. The ISP-based spyware provided by NebuAd and deployed by Cable One represented a radical innovation. In the context of Defendant's role as the trusted conduit for all its users' Internet communications, this ISP-based spyware created an unprecedented, extraordinarily pervasive ability to monitor users, identify particular individuals, and tamper with their communications and personal computers—even when those users were interacting with websites with which neither Defendant nor NebuAd had any relationship.

4. Cable One gave its users no notice of the impending infiltration and provided no opt-out opportunity. Rather, Cable One provided misleading statements in response to Congressional inquiries about its relationship with NebuAd.

5. Cable One did it for the money. For a price per customer per month, Cable One exploited its trusted position as a carrier for users' private communications, selling its unique ability to access users' Internet traffic and transmit communications to their personal computers. As to the effects of Defendant's conduct on users' privacy, their personal computers, and Defendant's quality of service, Defendant left users to fend for themselves. Accordingly, Plaintiff, on behalf of himself and all other similarly situated users, now seeks the relief requested in this complaint.

### **PARTIES**

6. At all times relevant to this complaint, Plaintiff Samuel Green ("Plaintiff") was a citizen and resident of Calhoun County, Alabama, was a subscriber to Cable One's broadband Internet services, and therefore a User, as defined herein.

7. At all times relevant to this complaint, Cable One was a commercial provider of high-speed, broadband Internet services to customers in approximately 19 states, including Alabama. Cable One is a wholly owned subsidiary of the Washington Post Company. At all times relevant to this complaint, Defendant was headquartered in Arizona.

a. Defendant provided Internet services to approximately 720,000 customer accounts, including Plaintiff, who accessed the Internet using Cable One-supplied cable modems connected to their personal computers. According to its

statement to Congress, the NebuAd test was only conducted in Anniston, Alabama, with 14,000 high-speed Internet subscribers, but overall Cable One had approx 720,000 customers in 19 states. Since a given customer account was often utilized for Internet access by multiple consumers, such as members of the account-holder's household, the actual number of consumers in the affected area using Defendant's ISP services ("Users") was much higher than 14,000.

b. As an Internet Services Provider ("ISP") providing broadband Internet services to the consuming public, Cable One was a "provider of an electronic communications service" as defined in the Electronic Communications Privacy Act, Title 18, United States Code, Section 2510(15) (the "Wiretap Act").

c. Users' Internet communications transmitted by Cable One consisted of the transfer of data transmitted in whole or in part by wire, radio, electromagnetic, photoelectronic, or photooptical systems that affected interstate and/or foreign commerce and were therefore "electronic communications" as defined in the Wiretap Act, Title 18, United States Code, Section 2510(12).

d. Cable One's Users were persons or entities who used Defendant's electronic communications services, were duly authorized by Defendant to engage in such use, and were therefore "users" as defined in the Wiretap Act, Title 18, United States Code, Section 2510(13).

e. The personal computers of Cable One's Users 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).

### **JURISDICTION AND VENUE**

8. This Court has original jurisdiction over this action pursuant to Title 28, United States Code, Section 1331, arising from the federal causes of action set forth in this complaint.

9. This Court has subject-matter jurisdiction over this action pursuant to Title 28, United States Code, Section 1332 in that the aggregate claims of Plaintiff and the proposed Class Members exceed the sum or value of \$5,000,000.

10. There is minimal diversity of citizenship between proposed Class Members and Defendant in that Cable One is a Delaware corporation headquartered in Arizona with customers in nineteen states, and Plaintiff is a citizen and resident of the State of Alabama asserting claims on behalf of a proposed class whose members reside in Alabama.

11. This Court has personal jurisdiction over Defendant because: (a) Defendant maintains offices and/or facilities in the State of Alabama; (b) a substantial portion of the wrongdoing alleged in this complaint took place in this State; and (c) Defendant is authorized to do business in and has sufficient minimum con-

tacts with this State and/or has otherwise intentionally availed itself of the markets in this State through the promotion, marketing, and sale of its products and/or services in this State, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

12. Venue is proper in this District under Title 28, United States Code, Sections 1391(b) and (c), in that Defendant conducts business with consumers in this District, and a substantial portion of the events and conduct giving rise to the violations of law set forth in this complaint took place in this District.

## **CONDUCT COMPLAINED OF**

### **A. Defendant's Deployment of Appliances**

13. An ISP is a conduit. Its job is to provide users with a connection to the Internet so users can communicate with other Internet-connected parties. Through the ISP's services, users browse websites, engage in e-commerce, hold voice-over-Internet-Protocol (VoIP) conversations, exchange e-mail correspondence, instant messages, and "tweets," and otherwise use the ISP's services to conduct all their Internet activities.

14. In or about late 2007 and continuing through early 2008, Cable One entered into an agreement with NebuAd, Inc. ("NebuAd"), a "third party provider of tailored advertising services." Cable One has acknowledged that it engaged NebuAd and participated in serving advertisements to its Users. (*See* Letter from

Philip P. Jimenez to the Hon. John D. Dingell, Chairman, Committee on Energy and Commerce, United States House of Representatives, August 8, 2008, p.2,[http://energycommerce.house.gov/Press\\_110/Responses%20to%20080108%20TI%20Letter/110-ltr.080108responseCABLE001.pdf](http://energycommerce.house.gov/Press_110/Responses%20to%20080108%20TI%20Letter/110-ltr.080108responseCABLE001.pdf)); (hereinafter, the “Cable One Resp. to Congress”.)

15. NebuAd agreed to share with Cable One the revenue from serving advertisements to Cable One Users, paying Cable One based on the number of subscriber accounts, per month, whose communications Cable One diverted to the Appliance.

16. Defendant’s and NebuAd’s actions set forth in this complaint were undertaken by Defendant and NebuAd in the performance of their respective obligations under their agreement.

17. On NebuAd’s website at <http://www.nebuad.com>, it provided the following overview of its business model:

Through its unique technology and methodology, industry expertise, and ISP partnerships, NebuAd is leading the industry to a new level of advertising effectiveness. NebuAd combines web-wide consumer activity data with reach into any site on the Internet. The result is vastly more data and relevance than existing solutions that are limited to one network or site.

18. NebuAd's ad-serving model relied on its gaining direct access to Users' Internet communications en route to and from Users' personal computers. To accomplish this, Defendant licensed and installed the NebuAd Ultra-Transparent Appliance (the "Appliance") from NebuAd and deployed Appliances in Defendant's Anniston broadband service network location.

19. Defendant began installing the Appliance in its broadband networks beginning in or about late 2007 and continuing through early 2008.

20. With NebuAd's cooperation, Defendant deployed the Appliance by physically situating it within Defendant's existing network infrastructure, reconfiguring its network to recognize the Appliance as a network device, and configuring its network connections to funnel all User Internet activity through the Appliance.

21. In the operation of the Cable One-NebuAd relationship, Cable One was responsible for installation of the Appliances; maintaining the flow of Users' Internet traffic to the Appliances; and, subsequently, resuming the handling of intercepted communications by delivering them to their destinations. Cable One supported the continued operation of the Appliances by providing ongoing network environment resources and services.

22. Owing to Cable One's unique position as an ISP for a large consumer population, it was able to divert Internet traffic on a massive scale. Assuming a single User from each of 14,000 customer accounts visited one website per day

during a six-month period, the number of diverted incoming and outgoing communications would be approximately 2.5 million.

23. Cable One claimed to have terminated its use of the Appliances in early 2008. (*See* Cable One Resp. to Congress, p. 3.)

## **B. Interception and Use of Personally Identifiable Information**

### ***Interception of Users' Electronic Communications***

24. The scope of Defendant's indiscriminate diversion of Internet traffic to the Appliance encompassed all of its Users' web navigation activity and other Internet transactions, such as file downloads and inbound and outbound messages—all unfiltered, in their entirety. The communicative components of User traffic diverted to the Appliance necessarily included:

a. all communications protocol types, including web communications (*http* traffic); encrypted web communications (*https* traffic); e-mail communications, including web-based email communications (*e.g.*, GMail, Hotmail, and Yahoo email account traffic); instant messages; file transfer protocol (*ftp*) and secure file transfer protocol (*ftps*) downloads; and voice-over-Internet-Protocol (VoIP) telephony communications;

b. all navigation information, including Users' search terms and the universal resource locators (URLs) identifying websites and Internet addresses accessed by Users;

c. Internet Protocol (IP) addresses, which uniquely and persistently identified Users' specific personal computers, in that, upon information and belief, Cable One's Users generally leave their cable modems in an always-on state, causing Users' personal computers to remain linked to unique, "sticky" IP addresses, much like static IP addresses;

d. personally identifying information<sup>1</sup> and substantive content in communications relating to personal and sensitive matters such as health events, insurance coverage, financial and e-commerce transactions, financial account status details, credit reports, political activities and interests, personal relationships and dating, job searches, and movie rental choices; privileged correspondence such as marital and attorney-client communications; and information contained in the financial records of financial institutions, of card issuers, as defined in Title 15, United States Code, Section 1602(n), and from the files of consumer reporting

---

<sup>1</sup> The Federal Trade Commission has defined "personally identifiable information" or "personal information" as:

individually identifiable information from or about an individual [consumer] including, but not limited to: (a) a first and last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name that reveals an individual's email address; (d) a telephone number; (e) a Social Security Number; (f) a persistent identifier, such as a customer number held in a "cookie" or processor serial number, that is combined with other available data that identifies an individual; or (g) any information that is combined with any of (a) through (f) above.

*In the Matter of Microsoft Corporation*, Federal Trade Commission, File No. 012 3240, Docket No. C-4069, Agreement Containing Consent Order, Aug. 8, 2002, pp. 2-3, <http://www.ftc.gov/os/caselist/0123240/microsoftagree.pdf>; accord *In the Matter of Eli Lilly and Company*, Assurance of Voluntary Compliance and Discontinuance, Attorneys General of the States of California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont, p. 7 n.3, [http://supplierportal.lilly.com/Home/Multi\\_State\\_Order.pdf](http://supplierportal.lilly.com/Home/Multi_State_Order.pdf) and <http://epic.org/privacy/medical/lillyagreement.pdf>.)

agencies on consumers, as defined in the Fair Credit Reporting Act, Title 15, United States Code, Section 1681, *et seq.*; and

e. information to, from, and about children under the age of 13.

25. Cable One implicitly admitted it diverted unfiltered Internet traffic to NebuAd—that is, Internet traffic containing personally identifiable information as well as *https* traffic, web mail, email, instant messages, and VoIP conversations—when Cable One told a United States Congressional committee that “no raw data linked to identifiable individuals was stored.” (*See* Cable One Resp. to Congress, p. 2.) Such an assurance would have been meaningful only if NebuAd was, in fact, receiving unfiltered data from Defendant.

26. NebuAd confirmed that it received unfiltered Internet traffic when it stated in Congressional testimony that “the NebuAd service constructs anonymous inferences about the user's level of qualification for a predefined set of market segment categories, *and then discards the raw data* that was used to create or update a user's anonymous profile.” (*See* Testimony of Bob Dykes, CEO, NebuAd, Inc., Senate Committee on Commerce, Science and Transportation, “Privacy Implications of Online Advertising,” July 9, 2008, p. 6, [http://commerce.senate.gov/public/\\_files/RobertDykesNebuAdOnlinePrivacyTestimony.pdf](http://commerce.senate.gov/public/_files/RobertDykesNebuAdOnlinePrivacyTestimony.pdf), emphasis added; hereinafter, “Dykes Senate Testimony.”) Thus, when NebuAd's CEO testified that “NebuAd's ad optimization and serving system does not collect PII or use informa-

tion deemed to be sensitive (e.g., information involving a user's financial, sensitive health, or medical matters),” he was not denying NebuAd’s acquisition of such information, merely claiming that NebuAd did not utilize such information to select and deliver advertisements. (*See id.*, p. 4.)

27. NebuAd confirmed that it assumed control of User information in testimony before Congress when it described “the NebuAd advertising service—part of which is co-located with, but operates separate and apart from, an ISP’s facilities.” (*See* Testimony of Bob Dykes, CEO, NebuAd, Inc., House Subcommittee on Telecommunications and the Internet, “What Your Broadband Provider Knows about Your Web Use: Deep Packet Inspection and Communications Law and Policies,” July 17, 2008, p. 4, <http://energycommerce.house.gov/images/stories/Documents/Hearings/PDF/Testimony/TI/110-ti-hrg.071708.Dykes-testimony.pdf>; hereinafter, “Dykes House Testimony.”)

28. In light of the foregoing admissions, Cable One misrepresented the content of User traffic it diverted to NebuAd when it represented to a Congressional committee that NebuAd collected no personally identifiable information. (*See* Cable One Resp. to Congress, p. 2.)

29. In light of the foregoing:

a. The Appliance was a device used to acquire the “contents” of communications, as that term is defined in the Wiretap Act, Title 18, United States

Code, Section 2510(8), in that Defendant used the Appliance to divert and transfer the substance, purport, and meaning of the communications to the Appliance. Therefore, the Appliance was used to “intercept” the contents of electronic communications, as that term is defined in the Wiretap Act, Title 18, United States Code, Section 2510(4);

b. Each of the Defendant’s networks or network segments incorporating the Appliance into its routine operations was a device and apparatus that could be and was used to intercept, retain, and transcribe in-transit electronic communications and was therefore an “electronic, mechanical, or other device” as defined in the Wiretap Act, Title 18, United States Code, Section 2510(5).

c. Likewise, each Appliance was itself a device and apparatus that could be and was used to intercept, retain, and transcribe in-transit electronic communications and was therefore an “electronic, mechanical, or other device” as defined in the Wiretap Act, Title 18, United States Code, Section 2510(6).

30. Neither Defendant nor NebuAd was the originator or recipient of the User communications traversing Defendant’s networks and, as further detailed in section E, “Defendant’s Deception and Lack of Authorization,” below, neither Defendant nor NebuAd were authorized to intercept and read the contents of Users’ communications. Therefore, neither Defendant nor NebuAd were a “party” to Us-

ers' electronic communications, as that term is used in the Wiretap Act, Title 18, United States Code, Section 2511(2)(d).

31. Defendant's interception and eavesdropping was intentional and knowing in that it was undertaken by Defendant in the performance of Cable One's agreement with NebuAd and accomplished with instrumentalities that included the Appliance and Defendant's networks installed and configured specifically to perform interception and eavesdropping.

***Tracking and Profiling of Individually Identified Users***

32. Regardless of whether NebuAd eventually discarded the personally identified content in Users' "raw data," it identified individual users and maintained behavioral profiles on them. NebuAd's profiles were linked not just to individual personal computers, but to the particular users, themselves.

33. To obtain information for NebuAd's behavioral profiles of Users, the Appliance included deep packet inspection ("DPI") functions that read and analyzed Users' communications. DPI software enables a party to read the contents OSI layers 6 and 7 of the data packets comprising an Internet communication—which is to say that DPI looks past the "envelope" and "handling instructions" layers of an Internet communication and drills down to transcribe the payload—the actual substance intended to be read by the recipient of the communications.

34. In addition, despite NebuAd's claim that "[t]here is no connection or link between the ISP's registration data systems and NebuAd" (*see* Dykes Senate Testimony, p. 7), NebuAd's user profiles included Users' five-digit zip codes, which it either deduced from Users' Internet communications or received from Defendant.

35. Through NebuAd's identification of individual Users and Defendant's interception of all of its Users' Internet communications, NebuAd could claim, "[W]e're able to get a 360-degree, multidimensional view over a long period of time of all the pages users visit." *Behavioral Insider*, Nov. 14, 2007, [http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art\\_aid=71020](http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=71020).

36. The relationship between Cable One and NebuAd represented an unprecedented and extraordinarily pervasive ability to locate and monitor Users and—as discussed below in section C, “Tampering with User Communications and Computers”—control Users' communications in all of their Internet activities. This ability to identify individuals and intervene in their communications extended to Users' interactions with websites with which neither Defendant nor NebuAd had any relationship.

37. The unique and persistent identifiers NebuAd used to track Users and link their online behavior to its profiles constituted personally identifying informa-

tion, just as a telephone number constitutes personally identifying information used to contact an individual, a street address constitutes personally identifying information used to find or correspond with persons residing at that address, or a global positioning system (GPS) signal constitutes personally identifying information used to locate the GPS device user while in transit. Therefore, Cable One's statement to a Congressional committee that NebuAd used no personally identifiable information was a misrepresentation. (*See Cable One Resp. to Congress, p. 2.*)

### **C. Tampering with User Communications and Computers**

38. NebuAd and the Appliance used DPI not only to read the contents of Users' communications, but to alter the contents, load the communications with atypically persistent tracking cookies, and forge components of the communications to evade Users' security and privacy controls when Defendant ultimately delivered the communications to Users, as follows:

a. For a communication en route to a User, if NebuAd identified the opportunity to serve a targeted advertisement, the Appliance inserted the advertisement into the web page being downloaded for display to the User.

b. The Appliance also inserted Javascript program code to be executed on the User's personal computer. Upon reaching Users' personal computers, the code forced Users' computers to download cookies from a NebuAd division. Causing Users' computers to contact a third-party website not authorized by the

original web page the User downloaded violates Internet Engineering Task Force (IETF) standards designed to maintain the security and integrity of Internet communications. Further, the cookies that the code caused to be deposited on Users' computers were no ordinary cookies that Users could manage with their privacy controls. They were super-persistent cookies that, if removed, simply reappeared. NebuAd's CEO alluded to this fact in testimony before Congress when he stated, "NebuAd has enhanced the industry-standard opt-out "cookie" based system with the use of proprietary techniques. This enables the opt-out to be more persistent." (Dykes Senate Testimony, p. 4 n.4.)

c. The Appliance forged the "envelope" of the altered communication to make the communication appear to the User's personal computer as if it were the authentic and unaltered web page the User had requested, thus escaping detection by Users' security controls designed to protect against unauthorized third-party content.

d. Cable One then delivered the altered, loaded, forged communications to the User's personal computer.

39. The Appliance's functions were consistent with NebuAd's March 30, 2007 patent application for "[a] network device for monitoring data traffic between a client device and a server device," which stated:

The data packets exchanged between a computer and a website being visited are altered or modified in such a way that the head of

the packets remains largely intact while the payloads of the packets are changed to suit the need.

(See U.S. Patent Application No. 11693719, “Network device for monitoring and modifying network traffic between an end user and a content provider,” filed Mar. 30, 2007, Abstract, Summary ¶¶ 9-10, Claims ¶¶ 4, 8, 12-14, 16; see also U.S. Patent Application No. 11759157, “Method and system for inserting targeted data in available spaces of a webpage,” filed June 6, 2007; U.S. Patent Application No. 11759179, “Network device for embedding data in a data packet sequence,” filed June 6, 2007; U.S. Patent Application No. 11759187, “Network devices for replacing an advertisement with another advertisement,” filed June 6, 2007.)

40. The content modification, forgery, and tracking code behavior of the Appliance implemented by Cable One was independently documented in “NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking” by Robert M. Topolski, co-published by Free Press and Public Knowledge, June 18, 2008, [http://www.freepress.net/files/NebuAd\\_Report.pdf](http://www.freepress.net/files/NebuAd_Report.pdf); <http://www.public-knowledge.org/pdf/nebuad-report-20080618.pdf>.

41. As further detailed in section E, “Defendant’s Deception and Lack of Authorization,” Cable One did not have authority to access Users’ personal computers and/or Cable One exceeded what authority they had to access Users’ personal computers in that Cable One was not authorized by its Users to transmit altered and forged communications that avoided detection and rejection by Users’

security controls and that caused the transmission and execution of code that defeated Users' privacy and security management tools.

42. Cable One's access of Users' personal computers was knowing and intentional and Cable One was aware of and intended the natural and probable consequences of such conduct, inasmuch as Cable One acted in concert with NebuAd and their actions were undertaken pursuant to an agreement between Cable One and NebuAd to engage in just such conduct.

43. Cable One knowingly caused the transmission of programs, information, codes, and commands in that Defendant transmitted forged communications designed to avoid detection by Users' security controls, and Defendant transmitted commands and code that created persistent tracking cookies on Users' personal computers, which were protected computers, defeating Users' privacy management tools.

**D. Defendant's Abnormal Course of Business and Unnecessary Conduct**

44. Defendant's acts alleged in this complaint far exceeded the scope of the "ordinary course of business" as that phrase is used in the Wiretap Act, Title 18, United States Code, Section 2510(5)(a) and the "normal course of [Defendant's] employment while engaged in any activity which is a necessary incident to the rendition of [its] service or to the protection of the rights or property of the pro-

vider of that service” as that phrase is used in the Wiretap Act, Title 18, United States Code, Section 2511(2)(a)(i).

45. It was not in Defendant’s normal course of business to engage in or facilitate User monitoring and behavioral profiling, advertisement selection, and advertisement delivery—whether by inserting ads into web content being downloaded by Users or by any other means.

a. Prior to Cable One’s relationship with NebuAd, it did not deliver targeted advertising to its users. As Cable One admitted, “Cable One does not generally tailor or facilitate the tailoring of Internet advertising based on consumers’ Internet search, surfing, or other online activities.” (Cable One Resp. to Congress, p. 2.)

b. Cable One has repeatedly characterized its foray into profiling and ad distribution with NebuAd as “small-scale” (Cable One Resp. to Congress.) Since Cable One’s termination of its NebuAd relationship, Cable One has been able to continue providing Internet services to their Users and have not found that it must engage in online ad-serving to be capable of providing such services.

c. Therefore, consumer profiling and ad selection and delivery were not activities Defendant conducted in the normal course of its business or as necessarily incident to its rendition of services or protection of rights or property.

46. The particular ad-serving activity in which Defendant participated with NebuAd was a novel ad-serving model, not one in which Defendant participated in the normal or necessary conduct of its business. As noted by NebuAd CEO Bob Dykes, NebuAd and its ISP partners adopted this novel model because “ISPs, who have up to now facilitated but barely participated in online advertising opportunities, can open new revenue streams that complement advertiser and publisher objectives to maximize revenue and generate higher revenue-per-subscriber.” *Behavioral Insider*, Nov. 14, 2007, [http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art\\_aid=71020](http://publications.mediapost.com/index.cfm?fuseaction=Articles.showArticle&art_aid=71020). Therefore, Cable One’s and NebuAd’s collaboration was motivated by the money-making potential of combining Defendant’s unique access to its Users’ communications combined with NebuAd’s technology and business relationships—not to provide Cable One’s Users the Internet services to which they had subscribed.

47. Defendant’s use of the Appliance and deep packet inspection technology was not in its normal course of business or a necessary incident to its rendition of services or protection of their rights or property. In the normal course of an ISP’s business and as a necessary incident to its need to protect its customers and network resources and to maintain the availability of its services, an ISP may indeed use tools that employ DPI. For example, an ISP may use DPI tools to scan Internet

communications for data content that matches recognized types of security threats, such as malicious viruses and worms.

48. In contrast, Cable One subjected Users' communications to deep packet inspection to identify users, monitor and track their Internet activity, alter the content of their communications, and forge communications characteristics that bypassed Users' security and privacy controls and bugged their personal computers. Contrary to Cable One's representations to Congress (*see* Cable One Resp. to Congress, p. 3), its activities were not for the operations support, policy enforcement, or security purposes disclosed in its Acceptable Use Policy. Cable One used DPI for its own commercial gain, independent of any normal and necessary activity in providing Internet services to Users, preserving its rights, or protecting its property.

49. The Appliance was spyware<sup>2</sup> in that it caused and enabled the surreptitious tracking of Users' Internet activity and transmittal of code that affected Users' control of their personal computers. However, unlike traditional spyware, which is

---

<sup>2</sup> "Spyware" has been defined as

any type of software that is surreptitiously installed on a computer and, without the consent of the user, could collect information from a computer, could allow third parties to control remotely the use of a computer, or could facilitate botnet communications.

*FTC v. Pricewert*, Case. No. C-09-2407 (RMW) (N.D. Cal.), Order Appointing Temporary Receiver, June 15, 2009 (Dkt. 38).

installed on a user's computers, the Appliance represented a new breed of ISP-hosted spyware.

50. The Appliance was adware<sup>3</sup> in that it caused the display of advertisements to computer users, and which advertisements were other than those authorized by the publishers of the web pages downloaded by users. Again, unlike traditional adware, the ISP-hosted location of the Appliance's represented an adware innovation.

51. Cable One was an adware marketing partner<sup>4</sup> in that its installation of the Appliance caused the display of advertisements through adware.

52. Spyware and adware hosting and execution and serving as NebuAd's adware marketing partner were not in Defendant's ordinary course of business, were not necessarily incident to Defendant's rendition of Internet connectivity services, and were not necessarily incident to Defendant's protection of rights and property.

---

<sup>3</sup> "Adware" has been defined as:

any downloadable software program that displays advertisements to a computer user, including, but not limited to, programs that display pop-up or pop-under advertisements, redirect website or search requests, install toolbars onto Internet browsers or electronic mail clients, or highlight particular keywords or phrases for Internet users as they surf the web.

*In the Matter of Priceline.com Incorporated*, Assurance of Discontinuance, Attorney General of the State of New York, Jan. 29, 2007, p. 1, [http://www.oag.state.ny.us/media\\_center/2007/jan/adware-scannedAODs.pdf](http://www.oag.state.ny.us/media_center/2007/jan/adware-scannedAODs.pdf).

<sup>4</sup> "Adware marketing partner" has been defined as "any adware company, ad buyer, affiliate, third party distribution partner or other entity that arranges for, purchases, places, or installs the adware program that displays advertising of the products or services . . . through adware." *Id.*

**E. Defendant's Deception and Lack of Authorization**

53. Cable One relied on its Acceptable Use Policy for authorization to engage in NebuAd-related conduct. It did not provide Users with any notice via letter and/or e-mail nor did it provide notice in its privacy policy on its website.

54. At no time did Cable One disclose that it was intercepting and funneling all User communications to NebuAd, including Users' personally identifiable information; enabling a third party to track and profile individually identified Users, anytime and anywhere, and forge communications being transmitted to them; delivering altered and forged communications that affected the integrity, performance, and operations of Users' personal computers. Therefore, Defendant failed to provide any notice and its existing "policy" was misleading, deceptive, and constituted material omissions.

55. In the case of the NebuAd Ultra-Transparent Appliance, "transparent" meant operating in a manner designed to be invisible to both of the authorized parties to an electronic communication. Users had no reasonable means by which they would have become aware that Cable One was diverting their communications to NebuAd.

56. Accordingly, Users received no notice of Defendant's conduct alleged in this complaint, and consequently, could not have obtained any User consent.

**F. User Consequences**

57. Cable One's interception and inspection of Users' electronic communications and monitoring of identified Users constituted invasions of Users' privacy by intruding upon the solitude and seclusion of Users' private affairs:

a. Cable One's job as an ISP was to provide a secure and confidential conduit for Users' Internet communications, through connectivity services in which in-transit communications are ordinarily transmitted in solitude and seclusion and not ordinarily displayed or available to the general public or third parties.

b. Users' Internet communications were confidential communications intended for receipt by particular recipients that did not include Cable One and NebuAd and, as such, were private affairs of Users.

c. Users' ability to engage in Internet communications in solitude and seclusion were private affairs of Users.

d. Users paid Cable One for its services and entrusted them with all their Internet communications—and the communications of Users who were their family members—with the material expectation that Cable One would provide a connectivity setting that would preserve the privacy of their communications, free from unauthorized and improper interception and inspection.

e. Cable One had a duty to Users to hold as confidential all information imparted by and linked to individual Users through their communications and Internet navigation.

f. Cable One invaded Users' privacy by intruding upon the solitude and seclusion of their communications when it caused Users' Internet communications to be intercepted, diverted to a third party, read and analyzed, and used for individual profiling.

g. Cable One perpetrated its intrusions surreptitiously, installing technology designed to escape user detection, and further hid its intrusions by issuing deceptive and misleading statements to Users and to a Congressional committee inquiring into the privacy consequences of Cable One's relationship with NebuAd.

h. Cable One used Users' communications for commercial purposes other than the purposes for which Users' had entrusted those communications to Cable One.

i. The degree of Cable One's intrusions encompassed the entire scope of Users' communications, including personal and confidential content and communications to and from minors; all communications types, including HTTPS, web mail, and VoIP traffic; the entire scope of Users' Internet navigation activity;

the entirety of Defendant's User base in Anniston, Alabama; a duration of at least several months; and many millions of User communications.

j. Cable One's motive was to make money by exploiting the trusted role through which it had access to Users' communications.

k. Cable One's intrusions continue to affect Users in that their personal information continues to be retained in identity-linked behavioral profiles stored on NebuAd servers.

l. Therefore—in light of Cable One's breach of trust in its role as a provider of confidential communications transmittal; Users' expectations in their ability to use Defendant's services to communicate privately; Users' expectations in the privacy and confidentiality of the particular communications they exchanged over connections provided by Cable One; Defendant's surreptitious and deceptive conduct and representations in carrying out its intrusions; Defendant's selfish motives and willingness to exploit its relationships with Users and betray their privacy interests for its own gain; and the scope and scale of Defendant's intrusions—Defendant's invasions of its Users' privacy by intruding upon the solitude and seclusion of their Internet communications would be highly offensive and objectionable to a reasonable person.

58. Further, Defendant's tampering with Users' electronic communications and personal computers constituted intrusions upon the solitude and seclusion

of Users' private affairs that would be highly offensive and objectionable to a reasonable person for reasons cited above, and in that:

a. Cable One had a duty to Users to hold as confidential all information imparted by and linked to individual Users through their communications and Internet navigation, and its duty of confidentiality include a duty to safeguard the integrity of those communications.

b. Cable One invaded Users' privacy by intruding upon the solitude and seclusion of their communications when it caused Users' Internet communications to be altered, loaded with computer-affecting code designed to facilitate tracking and defeat Users' privacy controls, and affixed with forged origin information designed to defeat Users' security controls.

c. Users expected to be protected in the solitude and seclusion of their communications, and they expected their communications to remain unmo-  
lest by the message carrier to whom they had entrusted their Internet communi-  
cations.

d. Defendant's intrusions in tampering with Users' communica-  
tions and computers extended to all Users to whom it provided services and its  
tampering with computers extended to the personal computers of all Users to  
whom it provided services.

e. Therefore, Cable One's conduct in tampering with Users' communications and personal computers constituted intrusions upon the solitude and seclusion of Users' private affairs, including the privacy and integrity of their communications and personal computers, that were detrimental to Users' interests and that would be highly offensive and objectionable to a reasonable person.

59. Cable One's conduct alleged in this complaint constituted an ongoing course of conduct that harmed Users and caused them to incur financial losses, in that:

a. Cable One, which was compensated by NebuAd for its performance under the Cable One-NebuAd agreement, realized significant economic benefits from the interception and modification of communications that belonged to Users and to which Users enjoyed a superior right of ownership.

b. As a carrier of messages with no authority to engage in the activities for which NebuAd compensated Cable One, Cable One appropriated compensation to itself for access to Users' information, communications, and personal computers when such compensation rightfully belonged to Users.

c. Cable One did so through a novel technology and business model that it implemented in a surreptitious manner and without adequate notice, intentionally deceiving and misleading Users in order to deprive them of the opportunity to realize the economic benefits flowing from the use of their in-

portunity to realize the economic benefits flowing from the use of their information and computers.

d. Therefore, Cable One was unjustly enriched, and Users are entitled to compensation paid or owed to Cable One by NebuAd, or a just and fair portion of such compensation.

e. Further, the diminution in the performance levels of Defendant's services caused by its deployment of the Appliances deprived Users of the utility and quality of service for which they had paid, and Users therefore did not receive the full value of paid-for service.

f. Further, the invasions of privacy perpetrated by Cable One in providing its services deprived users of the quality and character of service for which they had paid, and Users therefore did not receive the fair value of paid-for service.

g. Further, each deployment of an Appliance on one of Defendant's network segments constituted a single act that caused an aggregated loss of at least \$5,000 within a one-year period to each group of Users affected by each Appliance.

60. In Defendant's conduct alleged above, including the allegations of section C, "Tampering with User Communications and Computers," Defendant's

tampering with Users' personal computers and Internet communications caused damage to Users in that:

a. Cable One's interception and processing of intercepted communications consumed resources of and diminished the quality and performance of its Internet connectivity services to users.

b. Cable One's alterations and forgeries of communications diminished the utility, integrity, and value of such communications.

c. The cookie-creating code Cable One transmitted to Users' computers diminished the performance, utility, value, performance, and capabilities of Users' computers.

d. The cookie-creating code and communications with forged origins Cable One transmitted to Users' computers controlled and altered the functioning of Users' computers, including by circumventing Users' security and privacy controls.

e. Cable One's actions caused Users to expend money, time, and resources investigating and attempting to mitigate their personal computers' diminished performance and investigating and attempting to remove the persistently recurring and unauthorized third-party tracking cookies installed on their computers without notice or consent; and, in the process, diminished Users' productivity.

f. Further, these actions interfered with, diminished, and devalued Users' possessory interests in their personal computers and Internet communications, infringed on Users' right to exclude others from unauthorized access to their personal computers, and compromised the integrity and ownership of Users' personal computers.

g. Therefore, Users were economically damaged by Cable One's conduct.

61. Defendant's conduct alleged above, including that alleged in section C, "Tampering with User Communications and Computers," constituted interference with and intermeddling with Users' personal property in that:

a. Users' personal computers were their personal property.

b. Users' Internet communications were their personal property and property in which Users' rights of possession were superior to Defendant's.

c. Users' personal computers were designed to be capable of connecting to the Internet, which connection Defendant provided by means of its networks linked to cable modems installed in Users' homes and connected to Users' personal computers, and for which services and equipment Users paid fees to Defendant.

d. Through Defendant's interception, alteration, and forgery of communications, Defendant accessed and obtained control over communications

sent from User's computers to other Internet-connected parties and those parties' responses.

e. Through Defendant's interception and diversion of communications and through its transmission of commands and codes that caused the creation of unusual and persistent cookies, Defendant diminished the utility, value, speed, and capacity of Users' personal computers.

f. Through Defendant's forgery of communications components, Defendant disabled and nullified the utility of security detection controls and privacy management tools on Users' personal computers, altering and commandeering control of the functioning of Users' personal computers, diminishing the capabilities of Users' personal computers, and compromising the privacy, security, and integrity of Users' personal computers.

g. Further, the consequences of this conduct were devaluations of Users' personal computers and Internet communications; interference with Users' possessory interests in their personal computers and Internet communications; and diminutions in Users' productivity in using their personal computers and Internet communications.

h. Defendant's conduct was unauthorized and in excess of its authority to transmit Users' Internet communications.

i. Therefore, Defendant, without Users' consent, interfered with and intermeddled with Users' personal computers and Internet communications, harming Users' personal property and diminishing its value, quality, condition, and utility, and causing real and substantial damage to Users, including the damages alleged in the preceding paragraph 60.

62. Defendant's conduct alleged in this section F was knowing and intentional and Defendant intended the natural and probable consequences of its acts and omissions.

### **CLASS ALLEGATIONS**

63. Plaintiff brings this class action pursuant to Federal Rule of Civil Procedure 23 on behalf of himself and the following Class:

All individuals who were users of Cable One's Internet services and whose Internet communications traversing Cable One's Internet services network were diverted to a NebuAd Appliance.

64. Plaintiff reserves the right to revise this definition of the Class based on facts he learns during discovery.

65. Excluded from the Class are: (i) any Judge or Magistrate presiding over this action, and the court personnel supporting the Judge or Magistrate presiding over this action, and members of their respective families; (ii) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest and their current or former em-

ployees, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the Class; and (iv) the legal representatives, successors, or assigns of any such excluded persons.

66. *Numerosity*: Individual joinder of all members of the Class is impracticable. The Class includes thousands of individuals. Upon information and belief, Class Members can be identified through the electronic records of Defendant.

67. *Class Commonality*: Common questions of fact and law exist as to all Class Members and predominate over questions affecting only individual Class Members. All Class Members were Users of Defendant during the time that Defendant engaged in the activities alleged in this complaint. All Class Members' Internet communications were diverted, monitored, intercepted, disclosed, divulged, accessed, copied, retained, inspected, analyzed, tampered with, modified, altered, forged, and/or used by Defendant. Common questions for the Class include:

- a. how many Users and User communications were the subject of Defendant's conduct herein alleged;
- b. what Internet communications protocol types were affected by Defendant's conduct herein alleged;
- c. what personally identifying information was included in the intercepted communications;
- d. how intercepted communications were used;
- e. aside from intercepted communications traffic, what User registration, billing, or other User information was disclosed to NebuAd by Defendant;

- f. what effect deployment of the Appliances had on Defendant's service levels;
- g. what authority Defendant had to engage in their uses of Users' electronic communications in the context of their deployment of the Appliance and its relationship with NebuAd;
- h. what User information collected by or as a result of use of the Appliances continues to be retained by Defendant and/or NebuAd;
- i. whether Defendant tortiously intruded upon Users' seclusion and solitude;
- j. whether Defendant tortiously and unjustly enriched itself;
- k. whether Defendant violated the Wiretap Act, Title 18, United States Code, Section 2510, et seq.;
- l. whether Defendant violated the Computer Fraud and Abuse Act, Title 18, United States Code, Section 1030, et seq.
- m. whether Defendant tortiously trespassed upon Users' personal computers;
- n. whether Plaintiff and Class Members are entitled to damages, injunctive relief, and other equitable relief as a result of the consequences of Defendant's conduct; and
- o. if so, what is the measure of those damages and the nature of injunctive and other equitable relief.

68. Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by the Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison to the numerous common questions that dominate.

69. The injuries sustained by the Class Members flow, in each instance, from a common nucleus of operative facts. In each case, without authorization, through an ongoing, routinized, and common course of conduct, Defendant deployed the Appliance and caused Class Members' communications to be intercepted; caused Class Members to be monitored, identified, and tracked in their Internet activity; invaded Class Members' privacy; and tampered with their communications and personal computers.

70. *Typicality*: Plaintiff's claims are typical of the claims of other members of the Class, as the Plaintiff and other Class Members were all subjected to Defendant's identical wrongful conduct based upon the same transactions which occurred uniformly in regards to the Plaintiff and to the Class.

71. *Adequacy*: Plaintiff will fairly and adequately protect the interests of the Class. Plaintiff is familiar with the basic facts that form the bases of the proposed Class Members' claims. Plaintiff's interests do not conflict with the interests of the other Class Members that he seeks to represent. Plaintiff has retained counsel competent and experienced in class action litigation and intends to prosecute this action vigorously. Plaintiff's counsel has successfully prosecuted complex actions including consumer protection class actions. Plaintiff and Plaintiff's counsel will fairly and adequately protect the interests of the Class Members.

72. *Superiority*: The class action device is superior to other available means for the fair and efficient adjudication of the claims of Plaintiff and the proposed Class Members. The relief sought per individual member of the Class is small given the burden and expense of individual prosecution of the potentially extensive litigation necessitated by the conduct of Defendant. Furthermore, it would be virtually impossible for the Class Members to seek redress on an individual basis. Even if the Class Members, themselves, could afford such individual litigation, the court system could not.

73. Individual litigation of the legal and factual issues raised by the conduct of Defendant would increase delay and expense to all parties and to the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale and comprehensive supervision by a single court.

74. Given the similar nature of the Class Members' claims and the material similarity in the state statutes and common laws upon which the Class Members' claims are based, a nationwide class will be easily managed by the Court and the parties.

75. In the alternative, the Class may be certified because:

a. the prosecution of separate actions by the individual members of the Class would create a risk of inconsistent or varying adjudications with re-

spect to individual Class Members, which would establish incompatible standards of conduct by Defendant;

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

c. Defendant has acted or refused to act on grounds generally applicable to the Class as a whole, thereby making appropriate final and injunctive relief with respect to the members of the Class as a whole.

## **COUNT I**

### **(Invasion of Privacy by Intrusion Upon Seclusion: On Behalf of the Class)**

76. Plaintiff incorporates the above allegations as if fully set forth herein.

77. Defendant's interception and inspection of Users' Internet communications and its identification and monitoring of individual Users, as alleged above, including the allegations in section F, "User Consequences," constituted tortious invasion of privacy by its intrusion upon the solitude and seclusion of Users' private affairs that would be highly offensive and objectionable to a reasonable person.

78. Defendant's tampering with Users' communications and personal computers as alleged above, including the allegations in section F, "User Conse-

quences,” constituted tortious invasion of privacy by its intrusion upon the solitude and seclusion of Users’ private affairs that would be highly offensive and objectionable to a reasonable person.

79. Plaintiff and Class Members were harmed in the loss of the seclusion and solitude in their ability to communicate via the Internet and the seclusion and solitude of their Internet communications, and of which harm Defendant was the cause.

80. Accordingly, for Defendant’s invasions of privacy by its intrusion upon Plaintiffs’ and Class Members’ solitude and seclusion, Plaintiff and Class Members seek the injunctive relief of an order requiring Defendant to cease and refrain from resuming such conduct; the equitable relief of an accounting of the precise nature, duration, and extent of Defendant’s intrusion; such other equitable or declaratory relief as may be just and proper; and all such other relief as the Court may deem just and proper.

**COUNT II**  
**(Violations of the Electronic Communications Privacy Act,  
18 U.S.C. § 2510 *et seq.*: On Behalf of the Class)**

81. Plaintiff incorporates the above allegations as if fully set forth herein.

82. Defendant’s conduct, including that alleged in section A, “Defendant’s Deployment of Appliance“ and section B, “Interception and Use of Personally Identifiable Information,” above, was in violation of Title 18, United States Code,

Section 2511(1)(a) because Defendant intentionally intercepted and endeavored to intercept Plaintiff's and Class Members' electronic communications and procured NebuAd to intercept and endeavor to intercept Plaintiff's and Class Members' electronic communications.

83. Defendant's conduct, including that alleged in section A, "Defendant's Deployment of Appliance" and section B, "Interception and Use of Personally Identifiable Information," above, 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's 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).

84. Through Defendant's interception, endeavoring to intercept, use, and endeavoring to use Class Members' electronic communications, their electronic communications were in fact intercepted and intentional used in violation of Title 18, United States Code, Chapter 119. Accordingly, Class Members are entitled to:

a. such preliminary and other equitable or declaratory relief as may be just and proper;

b. damages computed as the greater of (i) the sum of the actual damages suffered by Plaintiff and Class Members plus Defendant's profits made through the violative conduct alleged in this complaint; (ii) statutory damages for

each Class Member of \$100 a day for each day of violation; or (iii) statutory damages of \$10,000 per User;

- c. punitive damages; and
- d. reasonable attorneys' fees and other litigation costs reasonably

incurred.

**COUNT III**  
**(Violations of the Computer Fraud and Abuse Act,  
18 U.S.C. § 1030 *et seq.*: On Behalf of the Class)**

85. Plaintiff incorporates the above allegations as if fully set forth herein.

86. Defendant's conduct, including that alleged in section C, "Tampering with User Communications and Computers" and section F, "User Consequences," above, was in violation of Title 18, United States Code, Section 1030, *et seq.*

87. Specifically, Defendant's conduct was in violation of Title 18, United States Code, Section 1030(a)(2)(A) in that Defendant intentionally accessed computers without authorization and exceeded authorized access and thereby obtained information that, as alleged above, including in paragraph 24(d), consisted of and included the financial records of financial institutions; of card issuers, as defined in Title 15, United States Code, Section 1602(n); and from the files of consumer reporting agencies on consumers, as defined in the Fair Credit Reporting Act, Title 15, United States Code, Section 1681, *et seq.*

88. Defendant's conduct was in violation of Title 18, United States Code, Section 1030(a)(5)(A) in that Defendant knowingly caused the transmission of programs, information, codes, or commands, and as a result of such conduct, intentionally and recklessly caused damage, without authorization, to protected computers and, as a result of such conduct, caused damage and loss.

89. Defendant's conduct was in violation of Title 18, United States Code, Section 1030(a)(5)(B) in that Defendant intentionally accessed protected computers without authorization, and as a result of such conduct, recklessly caused damage, and such damage resulted in an aggregated loss of at least \$5,000 within a one-year period to each group of Plaintiff and Class Members affected by each Appliance.

90. Defendant's conduct was in violation of Title 18, United States Code, Section 1030(a)(5)(C) in that Defendant intentionally accessed protected computers without authorization, and as a result of such conduct, caused damage and loss.

91. Accordingly, for Defendant's conduct in violation of the Computer Fraud and Abuse Act, Plaintiffs and Class Members are entitled to compensation for Plaintiff's and Class Members' economic damages and such injunctive and other equitable relief as may be just and proper.

**COUNT IV**  
**(Trespass to Chattels: On Behalf of the Class)**

92. Plaintiff incorporates the above allegations as if fully set forth herein.

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

94. Defendant, in its conduct alleged in this complaint, including the allegations in section F, "User Consequences," Defendant, in a relationship as a paid Internet service provider to Plaintiff and Class Members and without authority or consent, interfered with and intermeddled with Plaintiff's and Class Members' personal computers and Internet communications.

95. Defendant's conduct harmed Plaintiff's and Class Members' personal property and diminished its value, quality, condition, and utility, and causing real and substantial damage to Plaintiff and Class Members.

96. Defendant's acts constituted repeated and persistent trespass, nuisance, and intentional interference with Plaintiff's and Class Members' use and enjoyment of their computers and communications, in violation of common law.

97. Plaintiff, on behalf of himself and the Class, seeks injunctive relief restraining Defendant from trespass to chattels, an award of damages to be determined at trial, and such other and further relief as the Court may deem just and

proper.

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff respectfully prays for the following:

- (a) with respect to all counts, declaring the action to be a proper class action and designating Plaintiffs and their counsel as representatives of the Class;
- (b) as applicable to the Class *mutatis mutandis*, awarding injunctive and equitable relief including, *inter alia*:
  - (i) prohibiting Defendant from engaging in the acts alleged above;
  - (ii) requiring Defendant to disgorge all of its ill-gotten gains to Plaintiff and the other Class Members, or to whomever the Court deems appropriate;
  - (iii) requiring Defendant to delete all data wrongfully collected and retained through the acts alleged above;
  - (iv) requiring Defendant to provide Plaintiff and the other Class Members a reasonably clear, conspicuous, effective, and permanent means to decline to participate in any data collection activities by means of the Appliance and any similar device, in any present or future iteration, whether connected to NebuAd or any other third party;
  - (v) awarding Plaintiff and Class Members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged in this complaint; and
  - (vi) ordering an accounting and constructive trust imposed on the data, funds, and other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and concealment of such assets by Defendant;
- (c) for a preliminary and permanent injunction restraining Defendant and Defendant's officers, agents, servants, employees, and attorneys, and those in active concert or participation with any of them from:

- (i) transmitting any information about Plaintiffs' or Class Members' activities on the internet for advertising purposes to any other websites, without fair, clear and conspicuous notice of the intent to transmit information, including a full description of all information potentially and/or actually available for transmission;
- (ii) transmitting any information about Plaintiff's or Class Members' activities on the internet for advertising purposes to any other websites, without fair, clear and conspicuous opportunity to decline the transmittal prior to any transmission of data or information;
- (d) awarding damages, including statutory damages where applicable, to the Class in an amount to be determined at trial;
- (e) awarding Plaintiff reasonable attorney's fees and costs;
- (f) awarding pre- and post-judgment interest; and
- (g) granting such other and further relief as the Court may deem just and proper.

### **JURY TRIAL DEMAND**

Plaintiff request trial by jury of all claims that may be so tried.

Dated: January \_\_, 2010

Respectfully submitted,

SAMUEL GREEN, individually  
and on behalf of all others simi-  
larly situated

By

  
One of Their Attorneys  
Joey K. James (ASB-9672-S76J)

OF COUNSEL:

Bunch & James

210 E. Tennessee Street

Florence, Alabama 35630

Telephone: (256) 764-0095

Facsimile: (256) 767-5705

joey@bunchandjames.com

SCOTT A. KAMBER

skamber@kamberlaw.com

DAVID A. STAMPLEY

dstampley@kamberlaw.com

KAMBERLAW, LLC

11 Broadway, Suite 2200

New York, New York 10004

Telephone: (212) 920-3071

Facsimile:(212) 920-3081

BRIAN J. PANISH

panish@psblaw.com

RAHUL RAVIPUDI

ravipudi@psblaw.com

PANISH, SHEA & BOYLE, LLP

11111 Santa Monica Boulevard, Suite 700

Los Angeles, California 90025

Telephone: (310) 477-1700

Facsimile:(310) 477-1699

JOSEPH H. MALLEY

malleylaw@gmail.com

LAW OFFICE OF JOSEPH H. MALLEY, P.C.

1045 North Zang Boulevard

Dallas, Texas 75208

Telephone: (214) 943-6100

Facsimile:(214) 943-6170

DAVID C. PARISI  
dcparisi@parisihavens.com  
PARISI & HAVENS LLP  
15233 Valleyheart Drive  
Sherman Oaks, California 91403  
Telephone: (818) 990-1299  
Facsimile: (818) 501-7852