5113 TEH

4

JS 44 (Rev. 12/07) (cand rev 1-16-08)

# CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON PAGE TWO OF THE FORM.)

**I. (a) PLAINTIFFS**

Dan Valentine,
(see additional plaintiffs attached at 1(a))

**DEFENDANTS**

NEBUAD, INC., a Delaware Corporation; (see additional defendants attached at 1(b))

(b) County of Residence of First Listed Plaintiff Cook County, Illinois
(EXCEPT IN U.S. PLAINTIFF CASES)

County of Residence of First Listed Defendant San Mateo, California
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED.

(c) Attorney's (Firm Name, Address, and Telephone Number)

Alan Himmelfarb, KamberEdelson, LLC
2757 Leonis Blvd., Vernon, California 90058-2304
Telephone: (323) 585-8696
ahimmelfarb@kamberedelson.com

Attorneys (If Known)

**II. BASIS OF JURISDICTION** (Place an "X" in One Box Only)

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

**III. CITIZENSHIP OF PRINCIPAL PARTIES** (Place an "X" in One Box for Plaintiff and One Box for Defendant)
(For Diversity Cases Only)

| | PTF | DEF | | PTF | DEF |
|---|---|---|---|---|---|
| Citizen of This State | ☐ 1 | ☒ 1 | Incorporated or Principal Place of Business In This State | ☐ 4 | ☐ 4 |
| Citizen of Another State | ☒ 2 | ☐ 2 | Incorporated and Principal Place of Business In Another State | ☐ 5 | ☐ 5 |
| Citizen or Subject of a Foreign Country | ☐ 3 | ☐ 3 | Foreign Nation | ☐ 6 | ☐ 6 |

**IV. NATURE OF SUIT** (Place an "X" in One Box Only)

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

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

**TORTS**

**PERSONAL INJURY**
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury

**PERSONAL INJURY**
- ☐ 362 Personal Injury—Med. Malpractice
- ☐ 365 Personal Injury — Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

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

**CIVIL RIGHTS**
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 444 Welfare
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 440 Other Civil Rights

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

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

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

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

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

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

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

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

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

**V. ORIGIN** (Place an "X" in One Box Only)

☒ 1 Original Proceeding | ☐ 2 Removed from State Court | ☐ 3 Remanded from Appellate Court | ☐ 4 Reinstated or Reopened | ☐ 5 Transferred from another district (specify) | ☐ 6 Multidistrict Litigation | ☐ 7 Appeal to District Judge from Magistrate Judgment

**VI. CAUSE OF ACTION**

Cite the U.S. Civil Statute under which you are filing (**Do not cite jurisdictional statutes unless diversity**):
28 U.S.C. § 1332

Brief description of cause:
Installation and operation of undisclosed compute program without notice, authorization or consent.

**VII. REQUESTED IN COMPLAINT:**

☒ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

**VIII. RELATED CASE(S) IF ANY**

PLEASE REFER TO CIVIL L.R. 3-12 CONCERNING REQUIREMENT TO FILE "NOTICE OF RELATED CASE". Thomas v. Electronic Arts, Inc., C08-04421 PVT

**IX. DIVISIONAL ASSIGNMENT (CIVIL L.R. 3-2)**
**(PLACE AND "X" IN ONE BOX ONLY)**

☒ SAN FRANCISCO/OAKLAND ☐ SAN JOSE

DATE
November 10, 2008

SIGNATURE OF ATTORNEY OF RECORD

## Civil Cover Attachment

1(a) Additional plaintiffs

Dale Mortensen, Melissa Becker, Samuel Green, Sherron Rimpsey, Charlotte Miranda, Frank Miranda, Saul Dermer, Wayne Copeland, Crystal Reid, Andrew Paul Manard, Kathleen Kirch, Terry Kirch, Neil Deering, Paul Driscoll, individuals, on behalf of themselves and all others similarly situated,

1(b) Additional defendants

BRESNAN COMMUNICATIONS, a New York Corporation; CABLE ONE, a Delaware Corporation; CENTURYTEL, a Texas Corporation; EMBARQ, a Delaware Corporation; KNOLOGY, a Delaware Corporation; WOW!, a Delaware Corporation; AND JOHN DOES 1-20, corporations Defendants.

Alan Himmelfarb - SBN 90480
KAMBEREDELSON, LLC
2757 Leonis Boulevard
Vernon, California 90058
Telephone: (323) 585-8696

Joseph H. Malley
TX SBN: 12865900
LAW OFFICE OF JOSEPH H. MALLEY, P.C.
1045 North Zang Boulevard
Dallas, Texas 75208
Ph. (214) 943-6100
Fax (214) 943-6170

*Counsel for Plaintiffs*



TEH

**IN THE UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF CALIFORNIA**
**SAN FRANCISCO DIVISION**

CV 08 5143

DAN VALENTINE, DALE MORTENSEN, MELISSA BECKER, SAMUEL GREEN, SHERRON RIMPSEY, CHARLOTTE MIRANDA, FRANK MIRANDA, SAUL DERMER, WAYNE COPELAND, CRYSTAL REID, ANDREW PAUL MANARD, KATHLEEN KIRCH, TERRY KIRCH, NEIL DEERING, PAUL DRISCOLL, individuals, on behalf of themselves and all others similarly situated,

Plaintiffs

v.

NEBUAD, INC,, a Delaware Corporation; BRESNAN COMMUNICATIONS, a New York Corporation; CABLE ONE, a Delaware Corporation; CENTURYTEL, a Texas Corporation; EMBARQ, a Delaware Corporation; KNOLOGY, a Delaware Corporation; WOW!, a Delaware Corporation; AND JOHN DOES 1-20, corporations Defendants.

Defendants.

CASE No.

JURY DEMAND

COMPLAINT FOR:

1. Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510;
2. Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
3. Violation of California's California Invasion Of Privacy Act,, California Penal Code § 631;
4. Violation of California's Computer Crime Law, Penal Code § 502
5. Aiding and Abetting
6. Civil Conspiracy
7. Unjust Enrichment

## CLASS ACTION COMPLAINT

Plaintiffs, Dan Valentine, Dale Mortensen, Melissa Becker, Samuel Green, Sherron Rimpsey, Charlotte Miranda, Frank Miranda, Saul Dermer, Wayne Copeland, Crystal Reid, Andrew Paul Manard, Kathleen Kirch, Terry Kirch, Neil Deering, Paul Driscoll, on behalf of themselves and all others similarly situated, by and through their attorneys, KamberEdelson, LLC, and Law Office of Joseph H. Malley, P.C., as and for their complaint, allege as follows upon information and belief, based upon, inter alia, investigation conducted by and through their attorneys, which are alleged upon knowledge, sues Defendants NebuAd, Inc., Fair Eagle Inc., Bresnan Communications, Cable One, CenturyTel, Embarq, Knology, WOW, and John Does, corporations and states:

## NATURE OF THE ACTION

1. This is a class action lawsuit, brought by, and on behalf of, similarly situated internet users whose privacy and computer security rights were violated by NebuAd, Inc. including its subsidiary, Fair Eagle, Inc.; (hereinafter referred to collectively as "NebuAd"), and at least six NebuAd Activated ISP Affiliates ("NAISPs"), which were Internet Services Providers ("ISPs") affiliated in a joint venture with NebuAd, using Deep Packet Inspection, to intentionally intercept, without notice or consent, the online transmissions of the NAISP subscribers.

2. This class action lawsuit does not involve corporations that affiliated with NebuAd, but did not activate NebuAd's appliance, products, and/or services to intercept online transmission of their subscribers.

3. NebuAd and the NAISPs acted both independently and jointly, in that they knowingly authorized, directed, ratified, approved, acquiesced, or participated by accessing and

disclosing sensitive information ("SI"), personal identifying information ("PII"), personal information ("PI"), and non-personal indentifying information ("Non-PII") derived from the intentional interception of the NAISP subscriber's online transmissions, without authority or consent of the NAISP subscriber.

4. The purpose of the Joint Venture was not in the normal course of business for the NAISP, and was instead to monetize the subscriber's data for advertisement purposes. The NAISPs allowed, permitted, encouraged and aided NebuAd in accessing their subscriber's online transmissions.

5. NebuAd is not an ISP, nor was NebuAd authorized by the NAISP's subscribers to allow NebuAd access to their online transmissions, nor did such subscribers permit their NAISP to allow NebuAd access to their online transmissions.

6. The class action period, ( the "Class Period"), pertains to the period NebuAd and/or the NAISP activated the NebuAd Appliance which permitted interception of subscriber data, to the date NebuAd and/or NAISP deactivated NebuAd Appliance, a period that roughly approximates on or about November 1, 2007 to July 1, 2008.

7. The conduct of NebuAd, Inc., and the various NAISPs, individually and jointly, constituted one (1) or more of the following:

- Violation of Electronic Communications Privacy Act, 18 U.S.C. § 2510;
- Violation of Computer Fraud and Abuse Act, 18 U.S.C. § 1030;
- Violation of California's California Invasion Of Privacy Act,, California Penal Code § 631;
- Violation of California's Computer Crime Law, Penal Code § 502.

**JURISDICTION AND VENUE**

8. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332. The aggregate claims of plaintiff and the proposed class members exceed the sum or value of $5,000,000.00.

9. NebuAd is a California corporation headquartered in California and is a citizen only of the state of California. Plaintiffs are citizens and residents of Illinois, Montana, Alabama, Kansas, and Georgia, and assert claims of behalf of a proposed class whose members are scattered throughout the fifty states (including the 49 states besides California) and the U.S. territories: there is minimal diversity of citizenship between proposed class members and the Defendant.

10. This Court also has personal jurisdiction over defendant because (a) a substantial portion of the wrongdoing alleged in this complaint took place in this state, (b) defendant NebuAd's principle place of business is located in this state, and (c) defendant is authorized to do business here, has sufficient minimum contacts with this state, and/or otherwise intentionally availed itself of the markets in this state through the promotion, marketing, and sale of its product in this state, to render the exercise of jurisdiction by this Court permissible under traditional notions of fair play and substantial justice.

11. Venue is proper in this District under 28 U.S.C. §1391(b) and (c). A substantial portion of the events and conduct giving rise to the violations of law complained of herein occurred in this District, defendant NebuAd's principal executive offices and headquarters are located in this District at 901 Marshall Street, Redwood City, CA 94063-2026, and defendant conducts business with consumers in this District.

12. This Court has personal jurisdiction over the Defendant NebuAd under Cal. Code Civ. Proc. § 410.10 because NebuAd was incorporated in, maintains its corporate

headquarters in, and the acts alleged herein were committed in California.

13. The following corporations are citizens of states other than California; however, each of the acts upon which liability is alleged herein were committed by the corporations listed in this paragraph in the state of California:

1. Bresnan Communications;
2. Cable One;
3. CenturyTel;
4. Embarq;
5. Knology;
6. WOW!

The basis of the conduct complained of involved the interception, copying, transmission, collection, storage, usage, and altering of personal, private data of the class members. This conduct was devised, developed, implemented, and directed from within in this judicial district in California. The actual information and data from each of the NAISP Subscribers was, without exception, transmitted to NebuAd / Fair Eagle in California. Therefore, substantial, if not all evidence of wrongdoing as alleged in this complaint is located in this judicial district.

**INTRADISTRICT ASSIGNMENT**

14. Defendant NebuAd Inc.'s principle executive offices and headquarters are located in this District at 901 Marshall Street, Redwood City, CA 94063-2026. Intra-district assignment to the San Francisco Division is proper pursuant to Local Civil Rule 3-2(d).

**PARTIES**

15. Plaintiff Dan Valentine ("Valentine"), is a citizen and resident of Streamwood, Illinois, (Cook County). At all relevant times herein, Valentine was a subscriber to the WOW!

internet service provider, in the city and at the time that WOW! implemented its NebuAd Deep Packet Inspection of subscriber internet communications.

16. Plaintiff Dale Mortensen ("Mortensen"), is a citizen and resident of Billings, Montana (Yellowstone County). At all relevant times herein, Mortensen was a subscriber to the Bresnan Communications internet service provider, in the city and at the time that Bresnan Communications implemented its NebuAd Deep Packet Inspection of subscriber internet communications.

17. Plaintiff Melissa Becker ("Becker"), is a citizen and resident of Billings, Montana (Yellowstone County). At all relevant times herein, Becker was a subscriber to the Bresnan Communications internet service provider, in the city and at the time that Bresnan Communications implemented its NebuAd deep packet inspection of subscriber internet communications.

18. Plaintiff Samuel Green ("Green"), is a citizen and resident of Anniston, Alabama (Calhoun County). At all relevant times herein, Green was a subscriber to the Cable One internet service provider, in the city and at the time that Cable One implemented its NebuAd deep packet inspection of subscriber internet communications.

19. Plaintiff Sherron Rimpsey ("Rimpsey"), is a citizen and resident of Anniston, Alabama (Calhoun County). At all relevant times herein, Rimpsey was a subscriber to the Cable One internet service provider, in the city and at the time that Cable One implemented its NebuAd deep packet inspection of subscriber internet communications.

20. Plaintiff Charlotte Miranda ("Charlotte Miranda"), is a citizen and resident of Columbus, Georgia (Muscogee County). At all relevant times herein, Charlotte Miranda was a subscriber to the Knology internet service provider, in the city and at the time that Knology

implemented its NebuAd deep packet inspection of subscriber internet communications.

21. Plaintiff Frank Miranda ("Frank Miranda"), is a citizen and resident of Columbus, Georgia (Muscogee County). At all relevant times herein, Frank Miranda was a subscriber to the Knology internet service provider, in the city and at the time that Knology implemented its NebuAd deep packet inspection of subscriber internet communications.

22. Plaintiff Saul Dermer ("Dermer"), is a citizen and resident of Columbus, Georgia (Muscogee County). At all relevant times herein, Dermer was a subscriber to the Knology internet service provider, in the city and at the time that Knology implemented its NebuAd deep packet inspection of subscriber internet communications.

23. Plaintiff Wayne Copeland ("Copeland"), is a citizen and resident of Columbus, Georgia (Muscogee County). At all relevant times herein, Copeland was a subscriber to the Knology internet service provider, in the city and at the time that Knology implemented its NebuAd deep packet inspection of subscriber internet communications.

24. Plaintiff Crystal Reid ("Reid"), is a citizen and resident of Columbus, Georgia (Muscogee County). At all relevant times herein, Reid was a subscriber to the Knology internet service provider, in the city and at the time that Knology implemented its NebuAd deep packet inspection of subscriber internet communications.

25. Plaintiff Andrew Paul Manard ("Manard"), is a citizen and resident of Columbus, Georgia (Muscogee County). At all relevant times herein, Manard was a subscriber to the Knology internet service provider, in the city and at the time that Knology implemented its NebuAd deep packet inspection of subscriber internet communications. .

26. Plaintiff Kathleen Kirch ("Kathleen Kirch"), is a citizen and resident of Gardner, Kansas (Johnson County). At all relevant times herein, Kathleen Kirch was a subscriber to the

Embarq internet service provider, in the city and at the time that Embarq implemented its NebuAd deep packet inspection of subscriber internet communications.

27. Plaintiff Terry Kirch ("Terry Kirch"), is a citizen and resident of Gardner, Kansas (Johnson County). At all relevant times herein, Terry Kirch was a subscriber to the Embarq internet service provider, in the city and at the time that Embarq implemented its NebuAd deep packet inspection of subscriber internet communications.

28. Plaintiff Neil Deering ("Deering"), is a citizen and resident of Kalispell, Montana (Flathead County). At all relevant times herein, Deering was a subscriber to the CenturyTel internet service provider, in the city and at the time that CenturyTel implemented its NebuAd deep packet inspection of subscriber internet communications.

29. Plaintiff Paul Driscoll ("Driscoll"), is a citizen and resident of Elgin, Illinois (Cook County). At all relevant times herein, Driscoll was a subscriber to the WOW! internet service provider, in the city and at the time that WOW! implemented its NebuAd deep packet inspection of subscriber internet communications.

30. Defendant NebuAd, Inc. (hereinafter "NebuAd"), is a California corporation which maintains its headquarters at 901 Marshall Street, 2nd Floor, Redwood City, California 94063-2026. Defendant NebuAd, Inc., does business throughout the United States, and in particular, does business in State of California and in this County.

31. Defendant Bresnan Communications, Inc. (hereinafter "Bresnan Communications"), is a New York corporation which maintains its headquarters at One Manhattanville Road, Purchase, New York, 10577-2596. Defendant Bresnan Communications, Inc., knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and altering of personal, private data of its

subscribers to this county in the state of California;

- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the transmission, usage, and altering of personal, private data of its subscribers from this county in the state of California.

32. Defendant Cable One, Inc. (hereinafter "Cable One"), is a Delaware corporation which maintains its headquarters at 1314 North 3rd Street, Phoenix, Arizona 85004. Defendant Cable One knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and altering of personal, private data of its subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the transmission, usage, and altering of personal, private data of its subscribers from this county in the state of California.

33. Defendant CenturyTel Communications, Inc. (hereinafter "CenturyTel"), is a Texas corporation which maintains its headquarters at 100 Century Drive, Monroe, Louisiana 71203. Defendant CenturyTel, Inc., knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and altering of personal, private data of its subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the transmission, usage, and altering of personal, private data of its subscribers from

this county in the state of California.

34. Defendant Embarq, Inc. (hereinafter "Embarq"), is a Delaware corporation which maintains its headquarters at 5454 W. 110th Street, Overland Park, Kansas 66211. Defendant Embarq, Inc., knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and altering of personal, private data of its subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the transmission, usage, and altering of personal, private data of its subscribers from this county in the state of California.

35. Defendant Knology, Inc. (hereinafter "Knology"), is a Delaware corporation which maintains its headquarters at 1241 OG Skinner Drive, West Point, Georgia 31833. Defendant Knology, Inc., knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and altering of personal, private data of its subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the transmission, usage, and altering of personal, private data of its subscribers from this county in the state of California.

36. Defendant WideOpenWest Holdings, LLC, currently doing business as WOW! (hereinafter "WOW"), privately owned by Avista Capital Partners, LLC, is a Delaware corporation which maintains its headquarters at 2025 Research Parkway, Suite D, Colorado

Springs, Colorado 80920. Defendant Wide Open West knowingly and expressly allowed, permitted, aided, encouraged, and assisted in:

- the interception, copying, transmission, and altering of personal, private data of its subscribers to this county in the state of California;
- the copying collection, storage, usage, of personal, private data of its subscribers in this county in the state of California; and
- the transmission, usage, and altering of personal, private data of its subscribers from this county in the state of California.

37. Defendants, John Does 1-20, are corporations similarly situated to the NebuAd Activated ISP Affiliates, who activated and had operating on their ISP the NebuAd Device, products, or services that affected the Plaintiffs herein. The contractual obligations of NebuAd may require NebuAd to provide notice to the NebuAd Activated ISP Affiliates of this matter so as to appear and protect their interests, or these NebuAd Activated ISP advertisers may provide notice to confirm their NebuAd Program activity independent of NebuAd. In either case, when the identity of these NebuAd Activated ISP advertisers who are sued as Doe defendants are identified, Plaintiffs will amend their complaint to name such parties as NebuAd Activated ISP Affiliates.

## STATEMENT OF FACTS

38. NebuAd, Inc. is a privately owned corporation, headquartered in California, which operates as an online advertising company. "NebuAd," and NebuAd, Inc." are the registrants for the domain name: "nebuad.com."

39. NebuAd's website, http://www.nebuad.com, states in regard to the company's proposed 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."

40. Fair Eagle is a division of NebuAd, Inc.. Fair Eagle utilizes the website www.faireagle.com. Fair Eagle's website states, in regard to the company's proposed business model: "Fair Eagle is a division of the analytical company NebuAd, Inc. Fair Eagle is dedicated to enhancing the browsing experience of users through our innovative behavioral analysis solutions. Fair Eagle has partnered with your Internet Service Provider (ISP) to leverage our behavioral analysis solutions to provide you with the most relevant advertising possible while you are online without the use of any personally identifiable or sensitive information."

41. Although both entities talk in terms of "consumer activity data" and "behavioral analysis solutions," what the companies do not say is exactly *how* they are obtaining this "data."

**The Internet Service Provider**

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

passes through the conduit that the ISP provides.

43. Paul Ohm, Associate Professor of Law, Computer Crime Law, Information Privacy, Criminal Procedure, Intellectual Property, University of Colorado Law School observed:

> **The Greatest Threat to Privacy: The Internet Service Provider**
>
> I have recently posted on SSRN the article that ate my summer, *The Rise and Fall of Invasive ISP Surveillance*. I make many claims in this article, but the principal one, and the one I want to spend a few posts elaborating and defending, is found in the first sentence of the abstract: "Nothing in society poses as grave a threat to privacy as the Internet Service Provider (ISP)." In this first post, let me explain why ISPs pose an enormous threat to privacy:
>
> Simply put, your ISP has the means, motive, and opportunity to scrutinize nearly every communication departing from and arriving to your Internet-connected computer:
>
> **Opportunity:** Because your ISP serves as the gateway between your computer and the rest of the Internet, every e-mail message, IM, and tweet you send and receive; every web page and p2p-traded file you download; and every VoIP call you place travels first through your ISP's routers.
>
> **Means:** A decade ago, your ISP lacked the tools to efficiently analyze every communication crossing its network, because computers were relatively slow and networks were relatively fast. I use the analogy of the policeman on the side of the road, scrutinizing the passing cars. If the policeman is slow and the road is wide and full of speeding cars, the policeman won't be able to keep up.
>
> Over the past decade, while network bandwidth has increased, computer processing power has increased at a faster rate, and your ISP can now analyze more information, more inexpensively than before. The roads are wider today, but the policemen are smarter and more efficient. An entire industry--the deep-packet inspection industry--has arisen to provide hardware and software tools for massive, widespread, automated surveillance.
>
> **Motive:** Third-parties are placing pressure on ISPs to spy on users in unprecedented ways. Advertisers are willing to pay higher rates for behavioral advertising. For example, Ikea will pay more to place an ad in front of people who have been recently surfing furniture websites. To enable behavioral advertising, companies like NebuAd and Phorm have been trying to convince ISPs to collect user web-surfing data they do not collect today. Similarly, the copyrighted content

industries seem willing to pay ISPs to detect, report, and possibly block the transfer of copyrighted works.

**Paul Ohm September 03, 2008**
http://www.concurringopinions.com/archives/2008/09/the_greatest_th_1.html

44. ISPs are allowed, within their normal course of business as a necessary incident to the rendition of their services, to inspect a subscriber's datastream for reasons such as: viruses, spam, searching for non-protocol compliance, securing their network, police bandwidth, and maintain the overall "health" of their network; however conducting Deep Packet Inspection for subscriber content is not within those rights.

45. ISPs require subscribers to consent to an Acceptable Use Policy when they initially subscribe to their services. None of the Acceptable Use Policies of the defendant ISP's specifically provided details concerning the monitoring of their online communications for sale to advertisers, or the activities of NebuAd with respect to their online communications.

**Traditional Online Advertising Model**

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

47. Commercial websites use online advertising in order to promote content to the consumers without charge and require online advertising to support this objective. Commercial websites, known as "publishers" allow portions of their web page to be sold to online advertising networks, which act as an intermediary between "publishers" and the "advertisers."

48. Publishers desired to identify and track users while they were on their site; therefore "first party" tracking devices, "session cookies," and "persistent cookies" were

implemented. Cookies were a parcel of text sent by a publisher server to the user's browser, so that the user could be identified when they re-entered and navigated the publisher's site.

49. Online advertising companies desired a tracking system to gauge their advertising activity while the user navigated online in and out of their ad networks, and "third-party cookies" accomplished this goal.

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

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

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

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

54. Online advertisements, targeted or otherwise, were disfavored by consumers. As software programs that filtered online activity and deleted browser cookies developed in sophistication and availability, the consumer gained control over advertising strategies and advertiser attempts at data collection. Without the ability to maintain the accurate collection of user data, online advertising, contextual or behavioral, was not accurate.

55. The ultimate goal for online advertising networks became to obtain a complete digital dossier of all consumers, including all data pertaining to their sensitive information, personal identifying information and non-personal indentifying information. The only restraints to achieving this objective was governmental regulatory bodies, privacy laws, and consumer backlash.

**WIRETAPPING, FORGERY, AND BROWSER HIJACKING**

**A. Deep packet inspection "DPI"**

56. The Internet consists of a network of inter-connected computers in which data are broken down into small, individual packets and forwarded from one computer to another until they reach their destinations.

57. A packet can be thought of as a Russian nesting doll. Packets are built up in successive layers of information -- each one wrapped around all of the "inner" layers that have come before through a process called encapsulation. The innermost layer is usually what is considered to be the "content" of the message—such as the body of the e-mail message or the digital photograph being downloaded from the web. Outer layers contain a number of things that are non-content—such as the addresses used to deliver a message (although outer layers may include content as well).

58. Shallow Packet Inspection might provide information on the origination and destination IP addresses of a particular packet, and it can see what port the packet is directed towards.

59. Deep Packet Inspection, however, looks at the payload of the packet – the actual content of the communication. Whereas Shallow Packet Inspection might reveal a consumer accessing a travel–related website, Deep Packet Inspection would reveal the travel destination,

whether the consumer was comparing prices, or buying a ticket, how many people were traveling, what they paid, and the credit card information used to make the payment.

**B. The Device**

60. NebuAd obtained its data by tapping directly into the consumer's ISP connection. In cooperation with the named ISPs, NebuAd placed a hardware interception device directly into the data hub of the ISP. Each device can monitor all of the information going to and from 30,000 to 50,000 users. Multiple devices are used to insure capture of all data transmitted between the consumer and the internet. The device associates the information it sees with the I.P. address of the user, along with uniquely identifying information about a users' computer in order to identify the particular consumer when an I.P. address is changed.

61. Because ISPs route all of their customers' traffic, it is a uniquely perfect vantage point from which to monitor all the traffic to and from a consumer using Deep Packet Inspection (DPI).

62. For each of the I.P. addresses it is monitoring, the NebuAd system analyzes the Web traffic including the addresses of the pages visited, the search terms entered, and keywords that appear on those pages. The system keeps track of how often and how recently users visit the webpages the NebuAd system tracks.

63. NebuAd, Inc., filed the following patent with the U. S. Patent and Trademark office:

> U.S. Patent & Trademark Office:
> **USPTO Application #:** 20070233857
> **Title:** Network device for monitoring and modifying network traffic between an end user and a content provider
> **Abstract:** A network device for monitoring and modifying data traffic between a client device and a server device is disclosed. The network device is configured to provide targeted advertisements to a user based on some or all of the data traffics generated the user. Different from a proxy

server, the network device operates transparently from both perspectives of a computer being used by the user and a website being visited by the user. The network device is disposed in line between the computer and the network so that all data traffics are examined. 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 of delivering transparently the targeted commercial information.
Inventors: CHENG, Lebin; (Fremont, CA); Tikhman, Anatoly (Hillsborough, CA)
Correspondence Name and Address: Silicon Valley Patent Agency, 7394 Wildflower Way, Cupertino, CA 95014
**Assignee Name and Address:** NEBUAD, Inc., Redwood City, CA
**Serial No.:** 693719
**Series Code:** 11
**Filed:** March 30, 2007

64. NebuAd designed the hardware device to be installed into an ISP's network. The patent, and actions of the NebuAd device, are described by Robert Topolski, *Free Press and Public Knowledge*, "NebuAd and Partner ISPs: Wiretapping, Forgery and Browser Hijacking," July 18, 2008, as follows. The device has three purposes:

1. *Unique Identification:* The NebuAd device ties a customer's individual record maintained by the ISP to an alphanumeric code (called a "hash code"). This method allows NebuAd to uniquely and persistently identify individuals without needing any additional information from the ISP (i.e. billing records).

2. *User Monitoring:* The NebuAd system monitors user's Web browsing activity. The device sees the pages visited, the search terms entered, and words that appear on the pages. Stored information is indexed to the end user's hash code.

3. *Cookie Preloading:* The NebuAd device ensures that a Web browser is always preloaded with cookies providing unique identifying codes representing the ISP's subscriber. A cookie is a parcel of text placed by a server on a Web client (usually a

browser) and then sent back by the client each time the client accesses that server.

**C. The Utilization Of The NebuAd Hardware Device To Intercept And Alter A Subscriber's Communications With The Internet**

65. Web page code is normally entirely downloaded from servers to clients over a single TCP connection. Once the page is downloaded, the downloaded code is executed by the client. The execution of this code is what causes the additional operations necessary to download images and other page resources. This code is considered safe to execute because it purportedly came from a source trusted by the user.

66. NebuAd's device was not merely a passive collector of information. It was purposefully designed to not only intercept communications between the consumer and the internet, but to alter them.

67. The NebuAd device:

a. Monitors and -- at exactly the right time -- intercepts the communications between end points.

b. Impersonates the IP address and ports of the end-point server and communicates with the client.

c. Prevents the end-point client and server from continuing to directly communicate with each other over those ports.

d. Synchronizes certain integrity counters used by the TCP protocol to prevent the receiver from rejecting the packets.

68. In other words, through its partnership with the ISPs, NebuAd's advertising hardware monitors, intercepts, and then *modifies* the contents of internet packets using Transmission Control Protocol on Internet Protocol (TCP/IP). In doing so, NebuAd commandeers users' Web browsers and collects uniquely identifying tracking cookies to

facilitate its advertising model. Neither the consumers nor the affected Web sites are provided with any notice of NebuAd's interceptions and modifications.

69. NebuAd's code injected into another's page source is a cross-site exploit (XSS) and the subsequent behavior of loading cookies that the page normally would not load is called a browser hijack. NebuAd accomplished its cross-site exploit by effectively using what can be called a man-in-the-middle attack, described below in the context of a typical user's interaction with a common website, Google:

1) User navigates to http://www.google.com/ (or yahoo, or msn). His browser sends an HTTP "GET" request to fetch the page. Transmission is carried by the ISP.

2) Because the NebuAd device is in the ISP's network, transmission is sent thru and disclosed to NebuAd's device.

3) After leaving NebuAd's device and the ISP's network, the request traverses the Internet and reaches Google's server. (In total: from user's machine, ISP, NebuAd's device, some transit provider(s), to Google)

4) The response from Google's server (the HTML code to render the home page on the user's browser) is returned along the same route (from Google, some transit providers, NebuAd's device, ISP, to user's machine).

5) When the response hits NebuAd's device, it is in "x" amount of packets (e.g. Google used 5 packets). NebuAd appends an additional packet that contains JavaScript code. A forgery takes place to make the user's machine receive all of the packets -- both original and appended (e.g. 6 packets), all appearing to come from Google.

6) When that appended JavaScript code is executed, it causes the user's browser to load cookies for NebuAd's advertising partners which will be later used to identify the user as a NebuAd user when the user is surfing).

70. NebuAd exploits normal browser and platform security behaviors by forging IP packets, allowing their own JavaScript code to be written into source code trusted by the Web browser. NebuAd and the ISPs together cooperate in this attack against the intentions of the consumers, the designers of their software, and the owners of the servers that they visit. NebuAd actually alters, interferes with, and changes the data it captures. NebuAd intercepted, modified, and altered the contents of the Internet packets that were being sent and received while consumers were surfing.

71. NebuAd faked an additional packet of data that appeared to be the last part of the downloaded webpage – and that additional packet of data was received as if the source *was* the downloaded webpage. The extra packet included NebuAd-written JavaScript that directed user's browsers to the NebuAd-owned domain faireagle.com, where the company dropped tracking cookies from other domains and companies on the user's computer. These cookies were later used to deliver customized ads based from analyses of where consumers had gone on the web or what search terms they may have used.

72. With NebuAd's cookies on board, the consumer surfs normally. Up to this point, if the consumer noticed anything at all, it might be that the browser might have taken a few moments longer to load the page (due to the cookie-loading behavior). From this point on:

1) The user surfs normally. However, everything the consumer sees and does on the net is being captured and sent NebuAd's offsite servers for analysis into several interest categories.

2) If and when consumer happens upon a page used by one of NebuAd's ad partners which has purchased space on the page, the ad partner reads the cookie that NebuAd placed there, and based on the cookie information, substitutes one of NebuAd's ads instead of the random or contextual ad it would have normally shown.

73. Thus, every time a consumer's communicated information is going through the ISP installed NebuAd Deep Packet Inspection device, that data stream is being intercepted, collected, and processed, and, in many cases, altered.

74. The NebuAd-appended JavaScript identifies each unique subscriber to the NebuAd system. Thus, with a consistent subscriber ID, it is difficult for someone to evade profiling or targeted ads. The system will always inject the same codes. In this way the NebuAd system circumvents the bane of many Internet advertisers: cookie deletion. Cookie deletion is, of course, the conscious and deliberate act of the consumer to remove tracking and identification information from their computer as it relates to websites the consumer has visited. The NebuAd system deliberately and intentionally negates a consumer's efforts to remove this data.

**The Intercepted Data and the Altered WebPages**

75. All of the data the NebuAd devices intercept from the ISPs is collected and transmitted directly to its data analysis center in California.

76. All of the business of NebuAd is transacted in and from its headquarters in California. The information is collected, stored, and processed on NebuAd's servers in California. The analysis of the captured information that was intercepted at the ISP took place in California. The determination of the ads that Fair Eagle (NebuAd's advertising division) sought to place on the consumer's web browsing page were introjected from its headquarters in California. The alteration of the consumer's webpage from the one that the website would

ordinarily present to the one that NebuAd changes it to is altered and orchestrated from its headquarters in California.

77. All of the activities complained of herein from which the ISPs gained profit as a partner with NebuAd took place by and through NebuAd's headquarters in California.

78. By virtue of NebuAd's interception of data scheme, NebuAd struck a deal with the NAISPs that allows NebuAd / Fair Eagle to receive the contents of the individual Web traffic streams of each of the NAISP's customers. NebuAd analyzed the content of the traffic in order to create a record of the individual's online behaviors and interests. As customers of the NAISPs surfed the Web and visited sites where an ad network may have purchased ad space through NebuAd / Fair Eagle, they see advertisements targeted based on their previous Internet behavior.

79. This scheme allowed the NAISPs to open up new avenues of revenue aside from the traditional model of internet service provider, allowing the NAISPs to make "several dollars per month" per customer.

80. The CEO of NebuAd, Bob Dykes, stated: "The ISPs have not been able to share in the ad revenue and wealth creation around the publishing side of the Internet: They see their role as a valuable and a key role in the Internet, but many of them are making no money, are regulated and see this as a way of funding their capital requirements..."

81. On information and belief, all class members engaged in electronic communications with host websites all over the world, but on at least one occasion during the class period, each class members engaged in at least one or more communications with one or more websites whose servers are or were based in the state of California during the class period. Thus, data sent from the host website based in California to the class member in their home state was subject to the interception and alteration as alleged in this complaint. Data sent to the host

website based in California from the class member in their home state was subject to the interception and alteration as alleged in this complaint.

**Anonymization Of Data**

82. The collection of data by the NebuAd device was wholesale and all-encompassing. All data passing though the hub was swept up without discrimination as to the kind, type, nature, or sensitivity of the data. Like a vacuum cleaner, everything passing through the pipe of the consumer's internet connection was sucked up, copied, and forwarded to the California processing center. Regardless of any representations to the contrary -- all data – whether sensitive, financial, personal, private, complete with all identifying information, and all personally identifying information, was recorded and transmitted to the California NebuAd facility.

83. Any alleged anonymization of subscriber's identity and data, if in fact any such occurred, occurred after the phase of initial interception ("Interception- phase 1") which provides the basis of this class action lawsuit.

84. Any alleged anonymization of subscriber's identity during any phases after the point of initial interception of the online communication, such as analysis of the data ("Analysis-phase 2"), use ("Use-phase 3"), dissemination ("Dissemination-phase 4"), and storage ("Storage-phase 5") of the intercepted communication did not "anonymize" the intentional initial interception of online communication.

**Opting Out**

85. In *no* case as alleged in this complaint, was adequate, informed notice provided to any class member of the true nature and function of the NebuAd service.

86. In *all* cases where *some* notice was provided, that notice was insufficient,

misleading, and inadequate. Consent under such circumstances is impossible.

87. In *any* case where the opportunity of 'opting out' of the NebuAd service *was* provided, such 'opt out' rights were misleading, untrue, and deceptive.

88. 'Opting out' only affected the provision of advertisements to the consumer who opted out (what the consumer saw). In no case was the collection of all internet communication data between the consumer and the internet halted or affected in any way. All data was still collected. The 'opt out' only affected what advertisements the consumer was shown. Thus, the provision of the opportunity for opting out was, itself, totally misleading.

**The Congressional Privacy Inquiry**

89. On August 1, 2008, a Congressional inquiry about customization was sent to 33 internet based companies from the House Energy and Commerce Committee. This letter stated:

> We are writing with respect to the growing trend of companies tailoring Internet advertising based upon consumers' Internet search, surfing, or other use.
>
> As you may know, questions have been raised regarding the applicability of privacy protections contained in the Communications Act of 1934, the Cable Act of 1984, the Electronic Communications Privacy Act, and other statutes to such practices, and whether legislation is needed to ensure that the same protections apply regardless of the particular technologies or companies involved. We are interested in the nature and extent to which you engage in such practices, and the impact it could have on consumer privacy.
>
> In order for us to better understand how companies may be engaged in efforts to target Internet advertising, the impact of such efforts on consumers, and broader public policy implications, we respectfully request that you provide specific answers to each of the following questions:
>
> 1. Has your company at any time tailored, or facilitated the tailoring of, Internet advertising based on consumers' Internet search, surfing, or other use?
>
> 2. Please describe the nature and extent of any such practice and if such practice had any limitations with respect to health, financial, or other sensitive personal data, and how such limitations were developed and implemented.

3. In what communities, if any, has your company engaged in such practice, how were those communities chosen, and during what time periods was such practice used in each? If such practice was effectively implemented nationwide, please say so.

4. How many consumers have been subject to such practice in each affected community, or nationwide?

5. Has your company conducted a legal analysis of the applicability of consumer privacy laws to such practice? If so, please explain what that analysis concluded.

6. How did your company notify consumers of such practice? Please provide a copy of the notification. If your company did not specifically or directly notify affected consumers, please explain why this was not done.

7. Please explain whether your company asked consumers to "opt in" to the use of such practice or allowed consumers who objected to "opt out." If your company allowed consumers who objected to opt out, how did it notify consumers of their opportunity to opt out? If your company did not specifically or directly notify affected consumers of the opportunity to opt out, please explain why this was not done.

8. How many consumers opted out of being Subject to such practice?

9. Did your company conduct a legal analysis of the adequacy of any opt-out notice and mechanism employed to allow consumers to effectuate this choice? If so, please explain what that analysis concluded.

10. What is the status of consumer data collected as a result of such practice? Has it been destroyed or is it routinely destroyed?

11. Is it possible for your company to correlate data regarding consumer Internet use across a variety of services or applications you offer to tailor Internet advertising? Do you do so? If not, please indicate what steps you take to make sure such correlation does not happen. If you do engage in such correlation, please provide answers to all the preceding questions with reference to such correlation. If your previous answers already do so, it is sufficient to simply cross-reference those answers.

Thank you in advance for your attention to this matter. We respectfully request a response by Friday, August 8, 2008.

**A. <u>DEFENDANT BRESNAN COMMUNICATIONS RESPONSE</u>**

90. Bresnan Communications Response:

We conducted one limited trial with NebuAd from April, 2008 to June 26, 2008.

We entered into a limited trial with NebuAd. We were assured that the system would not use. track or store personally identifiable information, and would only aggregate users anonymously into broad interest categories (such as "auto shopper") and then send relevant ads to those groups of users when they click on an affiliated web site. We received assurances from NebuAd that any interest category data would not be based on health, financial or other sensitive personal information. We also received assurances that no specific online activity data, such as browsing records, would be stored or retained. As additional protection, we notified our customers and offered an easy-to-use opt-out mechanism as recommended by the FTC.

We conducted the test in a small segment of our Billings, Montana market. The Billings market was chosen due to its close proximity to our network operations center and our engineering resources. The test commenced on April 1, 2008 and was concluded on June 26, 2008.

The trial was limited to approximately 6,000 Bresnan OnLine customers.

We sent an email message to our customers' Bresnan OnLine email accounts, posted a web page describing the trial, and described such practices in our privacy policy. We also provided customers an easy opt-out mechanism.

How many consumers opted out of being subject to such practice?

Eighteen consumers opted out.

We used an opt-out notice and opt-out mechanism as recommended by NebuAd. We relied on assurances from NebuAd that an opt-out notice and mechanism was an acceptable and standard practice.

William J. Bresnan
Chairman & Chief Executive Officer

**B. <u>DEFENDANT CABLE ONE RESPONSE</u>**

91. Cable One, Inc. Response:

We have not deployed on a commercial basis technology that tailors online advertising based on the Web browsing activities of our customers, and we recognize that such technology has consumer privacy implications.

We initiated a small-scale test late last year of technology that provided a discrete

set of customers with tailored advertisements based on anonymized network traffic grouped into certain categories of subscriber interests.

WE ULTIMATELY DECIDED TO NOT DEPLOY THE TECHNOLOGY COMMERCIALLY ON OUR SYSTEMS, AND WE WOULD NOT HAVE DONE SO WITHOUT TAKING ADDITIONAL STEPS TO PROTECT OUR CUSTOMERS' PRIVACY, INCLUDING CONFIRMING THEIR INTEREST IN RECEIVING TAILORED ADVERTISEMENTS AND BY SECURING AN ADDITIONAL OPT-IN CONSENT FROM THEM.

Late last year, Cable One was approached by a third-party vendor about a new technology that replaces existing online advertisement with advertisements of greater relevance to users based on anonymized data collected about certain commercial categories of interest. This opportunity for Cable One customers to see more relevant advertising, and for this new technology to potentially help subsidize users' Internet access or other services and applications, prompted Cable One to conduct a small-scale test of the technology to assess its viability. At that time, Cable One insisted upon and received assurances that this technology relied on anonymous identifiers that could not be used to identify a specific Cable One customer. At the conclusion of the test, Cable One decided to not deploy the technology.

Cable One demanded and received assurances that the limitations built into the technology ensured our customers' privacy and security would be respected during the test.

The test commenced in Anniston, Alabama, on November 20, 2007, and continued for 180 calendar days.

The system in Anniston, Alabama, serves roughly 14,000 cable modem customers.

Cable One notifies customers in several different ways about the terms governing their use of its cable service. Included among these terms is that their Internet usage may be monitored and that data about them may be used to deliver customized information. For example:

The Acceptable Use Policy ("AUP") governing use of Cable One's service to which all users consent (users are required to review and affirmatively accept the policy by checking an opt-in box) when signing up for cable modem service — makes clear that Cable One may monitor the online activity of its customers.

• The annual Privacy Notice sent to customers states that Cable One may collect "cable modem technical data and information about aggregate cable modem usage for service offering analysis." It also provides that "when cable modem subscribers access the Cable One Internet portal page or other Cable One

websites, Cable One, its affiliates, partners and advertisers may use various software devices to collect information to allow participation in certain online activities or to facilitate online access."

Cable One customers opted in to our monitoring of their Internet usage and content consistent with this third-party test when they agreed to our Acceptable Use Policy. We routinely conduct tests to improve network security, enhance the performance of our network, and determine whether to make available new service offerings. Cable One provides notice and obtains consent from customers for these types of limited network and product tests and does not offer customers an additional opportunity to opt out of these tests because doing so would stifle our ability to test new technologies that have the potential to offer significant benefits to our customers.
In contrast to a small-scale test, Cable One does not intend to deploy commercially a technology that collects user data (even if anonymous) to deliver tailored advertising without taking several additional steps beyond what the law requires. First, we would provide our customers with an updated notice that describes the service in more detail. Second, we would confirm our customers' interest in receiving tailored advertising by obtaining additional affirmative consent from them in the form of an opt-in check box. Third, we would give customers a continuous ability to opt out of having their information used for this purpose. We would take these additional steps because we take seriously our obligations to protect our customers' privacy.

**How many consumers opted out of being subject to such practice?**

**Please refer to our response to Question 7, above.**

We have received assurances from the vendor that all such data was deleted from its system after the test ended.

Philip P. Jimenez
Associate General Counsel
Cable One, Inc.

## C. DEFENDANT CENTURYTEL RESPONSE

92. CenturyTel Response:

NebuAd's CPM test equipment was installed in an aggregated data POP (point of presence) in Kalispell, Montana. The majority of the consumers served by this POP were located in Kalispell, Montana; however; due to the configuration of the POP, a small number of consumers in surrounding communities in Montana, Idaho and Wyoming were served as well. The site was chosen because of the small size of the POP and because of its proximity to qualified technical staff working at or near that facility. CenturyTel's test of NebuAd's CPM technology

began in late November 2007, and use of the technology was stopped completely in June 2008. CenturyTel's use of CPM technology was never implemented beyond the test market.

During the test period, the aforementioned data pop served approximately 20,000 high-speed Internet subscribers included in the test.

CenturyTel sent notifications to consumers via email.

Eighty-two (82) subscribers opted out of Century Tel's test of CPM technology.

No raw or identifiable consumer data was collected or utilized by CenturyTel during the test. After extensive discussions with NebuAd - before, during, and after the test - it is our understanding that the only data collected during the test consisted of codes representing categories of interest that were derived anonymously via software. It is further our understanding that each interest category had a short pre-programmed lifespan, after which it was automatically deleted. Once the test was complete, all such data that had not otherwise expired was destroyed.

Is it possible for your company to correlate data regarding consumer Internet use across a variety of services or applications you offer to tailor Internet advertising? Do you do so? If not, please indicate what steps you take to make sure such correlation does not happen. If you do engage in such correlation. Please provide answers to all the proceeding questions with reference to such correlation. If your previous answers already do so, it is sufficient to simply cross-reference those answers.

In theory, it may be possible for any company to correlate data regarding consumer Internet use in the manner described. In practice, however, such correlation would be overly burdensome from both a technical and cost standpoint, and would likely prove to be of little value to the company engaging in such practice.

Glen F. Post, III, Chairman and Chief Executive Officer

**D. <u>DEFENDANT EMBARQ RESPONSE</u>**

93. Embarq Response:

The test was conducted in a single data POP (point of presence) in Gardner, Kansas.

During the test period, the data POP served approximately 26,000 high-speed Internet subscribers.

Two weeks before the test began; Embarq posted a notice in the Privacy Policy that appeared on the Embarq website.

Based on information provided to us by our test technology vendor, 15 subscribers opted out.

No raw or identifiable customer data was collected or utilized during the test.

Tom Gerke, President and Chief Executive Officer

**E. DEFENDANT KNOLOGY RESPONSE**

94. Knology, Inc. Response:

Knology recently worked with NebuAd in a trial of NebuAd's behavioral advertising system.

We notified customers of the NebuAd trial and their ability to opt out through our Customer Service Agreement. This Agreement is posted on-line on Knology's website, as well as provided to customers when initiating service with Knology.

The method and content of the notice were required by NebuAd as part of our testing agreement.

Our test of the NebuAd system began, on a limited basis, in January 2008 in West Point, Georgia, chosen due to its physical proximity to Knology's headquarters and the technical group responsible for the product test. The trial slowly expanded to Columbus, Georgia in February 2008 and to Augusta, Georgia in March 2008. The bulk of the trial was not executed until late April and early May when it was tested in Panama City, Florida and Knoxville, Tennessee, and in June 2008, when it was tested in a small part of our Huntsville, Alabama market.

Knology discontinued the trial in all markets on July 14, 2008, in order to study the issues raised about the NebuAd system by your Committee, privacy advocates, and others. After we discontinued our test last month, we were assured by NebuAd that it had destroyed all interest summaries created during the testing period. Out systems did not receive data from NebuAd or any information on interest summaries or targeted advertising during or after the trial and, therefore, we are unable to quantify how many customers actually received targeted advertising as a result of the trial.

Rodger L. Johnson
Chairman of the Board and CEO Knology, Inc.

**F. DEFENDANT WOW! RESPONSE**

95. WOW! Response:

WOW is a competitive provider of cable and broadband-related services with operations limited to selected communities in or proximate Chicago, IL,

Detroit, MI, Columbus, OH, Cleveland, OH, and Evansville, IN. WOW, like a number of other providers of cable and broadband-related services from whom you have requested information, engaged the services of a third party provider of tailored advertising services, NebuAd, Inc.

For approximately four months (beginning in early March, 2008 and terminating throughout WOW's service areas on July 8, 2008) NebuAd Services (described in further detail in response to Question2) were available to WOW's high speed data ("HSD") customer base of approximately 330,000. Beginning approximately two months prior to this deployment period, an evaluation and testing phase was conducted followed by installation of the NebuAd platform on a region by region basis.

As represented by NebuAd, NebuAd Services use non-personally identifiable information (NPII) to serve targeted Internet advertising to HSD users. Prior to any deployment of the servicer, NebuAd assured WOW that: (i) there would be no collection or use of personally-identifiable information.

Approximately four weeks prior to full commercial deployment of the NebuAd Services, the following notifications were provided: (1) Customer Terms of Service and Internet Privacy Policy were modified; (2) a "Third Party Advertisers" link was added to WOW's website; (3) WOW's online FAQs were updated. [Note- "full" 2-3 months before done to "not full" common areas!]

NebuAd did not track the number of consumers opting out; rather, their reports showed over the course of deployment of the NebuAd Services 3,355 opt-outs, with an indeterminate number of those opt-outs being exercised by the same customer.
"Is it possible for your company to correlate data regarding consumer Internet use across a variety of services or applications you offer to tailor Internet advertising? Do you do so? If not, please indicate what steps you take to make sure such correlation does not happen. If you do engage in such correlation, please provide answers to all the preceding questions with reference to such correlation. If your previous answers already do so, it is sufficient to simply cross-reference those answers."

D. Craig Martin, General Counsel

## CLASS ALLEGATIONS
### Allegations as to Class Certification

96. Plaintiffs bring this Complaint on behalf of themselves and the following class:

All NAISP Subscribers whose internet communications were monitored,

intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

97. Additionally and/or alternatively, Plaintiffs bring this Complaint on behalf of themselves and the following subclasses:

i) All Bresnan Communications subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

ii) All Cable One subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

iii) All CenturyTel subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

iv) All Embarq subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

v) All Knology subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

vi) All WOW subscribers whose internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used at any time by or through a NebuAd device.

98. Plaintiffs reserve the right to revise these definitions of the classes based on facts

they learn during discovery.

99. The classes are brought pursuant to Federal Rule of Civil Procedure 23 (the "Classes"). Excluded from the Classes 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) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest and their current or former employees, officers and directors; and 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.

100. **Numerosity:** Individual joinder of all members of the Class is impracticable. The class and each subclass includes thousands of individuals. Upon information and belief, class members can be identified by the electronic records of defendants.

101. **Class Commonality:** Common questions of fact and law exist as to all Class members and predominate over the questions affecting only individual Class members. All class members were subscribers of one of the NAISPs during the time that the NAISP engaged in the activities herein alleged. All class members' internet communications were monitored, intercepted, accessed, copied, transmitted, altered and/or used by defendants.

102. Common questions include:

a. What was the NebuAd device and how did it work?

a. What information did the NebuAd device collect and what did it do with that information?

b. Was there proper notice, *or any notice*, of the operation of the NebuAd device to consumers?

c. Was there proper opportunity, *or any opportunity,* to decline the operation of the NebuAd device provided to consumers?

d. Whether NAISP subscribers, by virtue of their subscription, had pre-consented to the operation of the NebuAd device;

e. Did the operation, function, and/or implementation of the NebuAd device violate the ECPA?

f. Did the operation, function, and/or implementation of the NebuAd device violate California's Computer Crime Law, Cal. Penal Code § 502?

g. Did the operation, function, and/or implementation of the NebuAd device violate the Federal Computer Fraud And Abuse Act, 18 U.S.C. §§ 1030(A)(2)(C) & (A)(5)?

h. Did the operation, function, and/or implementation of the NebuAd device violate the Violation of the California Invasion of Privacy Act?

i. Did the operation, function, and/or implementation of the NebuAd device unjustly enrich the defendants herein?

j. Are the NAISPs liable under a theory of aiding and abetting, or conspiracy, for NebuAd's violations of the statutes listed herein?

k. Did the NebuAd device transmit "personally identifying information?"

l. Are class members entitled to damages as a result of the operation, function, and/or implementation of the NebuAd device, and, if so, what is the measure of those damages?

103. Defendants 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.

104. The injuries sustained by the class members flow, in each instance, from a common nucleus of operative facts. In each case, the Defendant NAISPs permitted the monitoring, interception, access, coping, transmission, alteration and/or use of their private personal communications by or through the NebuAd device. NebuAd itself, installed and monitored, intercepted, accessed, copied, transmitted, altered and/or used said communications through the use of the NebuAd device without adequate notice, consent, or opportunity to opt out provided to the NAISP subscribers.

105. **Typicality:** Plaintiffs' claims are typical of the claims of other members of the Class, as the Plaintiffs and other Class members were all subjected to Defendants' identical wrongful conduct based upon the same transactions which occurred uniformly to the Plaintiffs and to the public.

106. **Adequacy**: Plaintiffs will fairly and adequately protect the interests of the class. Plaintiffs are familiar with the basic facts that form the bases of the proposed class members' claims. Plaintiffs' interests do not conflict with the interests of the other class members that they seek to represent. Plaintiffs have retained counsel competent and experienced in class action litigation and intend to prosecute this action vigorously. Plaintiffs' counsel has successfully prosecuted complex actions including consumer protection class actions. Plaintiffs and Plaintiffs' counsel will fairly and adequately protect the interests of the class members.

107. **Superiority**: The class action device is superior to other available means for the fair and efficient adjudication of the claims of Plaintiffs 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 Defendants. 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.

108. Individual litigation of the legal and factual issues raised by the conduct of Defendants 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.

109. Given the similar nature of the class members' claims and the absence of material differences 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.

110. The court may be requested to also incorporate subclasses of Plaintiffs, defendants, or both, in the interest of justice and judicial economy.

111. 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 adjudication with respect 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 substantially impair or impede their ability to protect their interests; and

c) Defendants have acted or refused to act on grounds generally applicable to the class, thereby making appropriate final and injunctive relief with respect to the members of the class as a whole.

**Count I:**
**VIOLATIONS OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT**
**Against All Defendants**

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

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

114. The federal Electronic Communications Privacy Act of 1986 ("ECPA", at 18 U.S.C. § 2511(1) makes it unlawful for a person to "willfully intercept[], endeavor[] to intercept, or procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 USC 2520(a) provides a civil cause of action to "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of the ECPA.

115. The transmission of data by Plaintiffs and the Class between their computers and the internet constitute "electronic communications" within the meaning of 18 U.S.C. §2510.

116. Defendants have intentionally obtained and/or intercepted, by device or otherwise, these electronic communications without Plaintiffs' or Class members' knowledge, consent, or authorization and while the communications were still en route.

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

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

119. Defendants exceeded their authorization to access and control private information concerning Plaintiffs' electronic communications, in violation of 18 U.S.C. § 2701.

120. Defendants unlawfully and knowingly divulged Plaintiffs' electronic communication contents and user information, in violation of 18 U.S.C. § 2702.

121. Defendants intentionally acquired and/or intercepted the contents of electronic communications sent by and/or received by Plaintiffs through the use of an electronic device. Defendants intentionally acquired the communications that had been sent from or directed to Plaintiffs through their use of computers and other electronic devices which were part of, and utilized in, Defendants' electronic communications system, in violation of 18 U.S.C. § 2511 and pursuant to 18 U.S.C. § 2520.

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

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

124. Defendants are liable directly and/or vicariously for this cause of action. Plaintiffs therefore seek remedy as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and reasonable attorney's fees and other litigation costs reasonably incurred

125. Plaintiffs and the Class, pursuant to 18 U.S.C. §2520, are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the above-described violations.

**Count II**
**VIOLATION OF CALIFORNIA'S COMPUTER CRIME LAW**
**CAL. PENAL CODE § 502**
**Against All Defendants**

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

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

128. Defendants accessed, copied, used, made use of, interfered, and/or altered, data belonging to class members: (1) in and from the State of California; (2) in the home states of the plaintiffs; and (3) in the state in which the servers that provided the communication link between plaintiffs and the websites they interacted with were located.

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

jurisdiction.

130. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission, altering, and making use of data from Plaintiffs' computers in order to wrongfully obtain valuable private data from Plaintiffs,

131. Defendants have violated California Penal Code § 502(c)(1) by knowingly and without permission, altering, and making use of data from Plaintiffs' computers in order to: (1) deceive Plaintiffs into surrendering private internet communications and activities for defendants' financial gain; and (2) deceive Plaintiffs into accepting and clicking on ads of defendant's creation instead of the ads proffered by the websites they were interacting with.

132. Defendants have violated California Penal Code § 502(c)(2) by knowingly and without permission, accessing and taking data from Plaintiffs computers.

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

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

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

136. Pursuant to California Penal Code § 502(b)(10) a "Computer contaminant" means any set of computer instructions that are designed to . . . record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information.

137. Defendants have violated California Penal Code § 502(c)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and defendants.

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

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

**Count III**
**VIOLATION OF FEDERAL COMPUTER FRAUD AND ABUSE ACT**
**18 U.S.C. §§ 1030(a)(2)(C) & (a)(5)**
**Against All Defendants**

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

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

142. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2)(C), by intentionally accessing a computer used for interstate commerce or communication, without authorization or by exceeding authorized access to such a computer, and by obtaining information from such a protected computer.

143. Defendants have violated the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(i) by knowingly causing the transmission of a program, information, code, or command and as a result causing a loss to one or more persons during any one-year period aggregating at least $5,000 in value.

144. Plaintiffs have suffered loss by reason of these violations, including, without limitation, violation of the right of privacy, disclosure of affiliation and business relationships between Plaintiffs and internet product and service providers, and disclosure of specific purchase and transactional information that otherwise is private, confidential, and not of public record.

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

**Count IV**
**VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT,**
**Penal Code section 630 et seq.**
**Against All Defendants**

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

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

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

> Any person who, . . . or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message,

> report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable . . .

149. On information and belief, each plaintiff, and each class member, during one or more of their interactions on the internet during the class period, communicated with one or more web entities based in California, or with one or more entities whose servers were located in California.

150. Communications from the California web-based entities to plaintiffs and class members were sent from California. Communications to the California web-based entities from plaintiffs and class members were sent to California.

151. Plaintiffs and class members did not consent to NebuAd's nor any of the NAISPs actions in intercepting, reading, and/or learning the contents of their communications with such California-based entities.

152. Plaintiffs and class members did not consent to NebuAd's nor any of the NAISPs actions in using the contents of their communications with such California-based entities.

153. NebuAd is not a " public utility engaged in the business of providing communications services and facilities . . ."

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

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

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

157. The Defendant NAISPs directly participated in the interception, reading, and/or learning the contents of the communications between plaintiffs, class members and California-based web entities.

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

159. Pursuant to Section 637.2 of the California Penal Code, Plaintiffs and the class have been injured by the violations of California Penal Code section 631. Wherefore, plaintiffs, on behalf of themselves and on behalf of a similarly situated Class of consumers, seek damages and injunctive relief.

**Count V:**
**AIDING AND ABETTING VIOLATIONS OF:**
**--The Electronic Communications Privacy Act**
**--California's Computer Crime Law Cal. Penal Code § 502, And**
**--The Federal Computer Fraud And Abuse Act 18 U.S.C. §§ 1030(A)(2)(C) & (A)(5)**
**--The California Invasion of Privacy Act**
**Against Bresnan Communications, Cable One, CenturyTel, Embarq, Knology, Wow!, and John Does 1-9 ("NAISP Defendants")**

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

161. As fully described above, The NAISP Defendants had full knowledge or should have reasonably known of the true nature of the wrongful conduct conducted by NebuAd.

162. The NAISP Defendants knew that, through the implementation of NebuAd's Deep Packet Inspection of its subscribers' internet communications, NebuAd would, in real time, receive personally identifying information along with sensitive, financial, personal, private, information unknowingly transmitted and communicated by its subscribers who had no adequate notice that their communications were being intercepted, all in violation of the Electronic Communications Privacy Act; California's Computer Crime Law Cal. Penal Code § 502; the Federal Computer Fraud And Abuse Act 18 U.S.C. §§ 1030(A)(2)(C) & (A)(5); and California's Invasion of Privacy Act.

163. The NAISP Defendants aided and abetted such wrongful conduct, including providing the means and the access to violate these state and federal statutes.

164. The NAISP Defendants knew, or should have known, that the conduct NebuAd engaged in by use of Deep Packet Inspection of its subscribers' data transmissions and communications was unlawful and that the NAISP's provision of access to their subscribers' internet communications was the means by which that unlawful conduct took place.

165. The NAISP Defendants knew, or should have known, at all relevant times herein, of their role as part of an overall illegal or tortious activity at the time that the NAISPs provided their assistance.

166. As a direct and proximate result of the aiding and abetting of these acts, Plaintiffs have suffered injury and harm and loss, including, but not limited to, loss of the user's privacy with respect to their actions on the internet (where class members shop, what they buy and look at, where they browse, and what goods and services they seek), loss of privacy with

respect to their associational relationships on the internet); and loss of privacy with respect to their interests, hobbies, and activities on the internet. The wrongful conduct aided and abetted by the NAISP Defendants was a substantial factor in causing this harm.

167. The NAISP Defendants' intentional aiding and abetting to commit, and commission of, these wrongful acts was willful, malicious, oppressive, and in conscious disregard of Plaintiffs' rights, and Plaintiffs are therefore entitled to an award of punitive damages to punish their wrongful conduct and deter future wrongful conduct.

**Count VI**
**CIVIL CONSPIRACY ON BEHALF OF THE CLASS**
**Against The NAISP Defendants**

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

169. The NAISP Defendants willfully, intentionally, and knowingly agreed and conspired with NebuAd to engage in the alleged wrongful conduct, including NebuAd violations of the Electronic Communications Privacy Act, and California's Computer Crime Law Cal. Penal Code § 502, the Federal Computer Fraud And Abuse Act 18 U.S.C. §§ 1030(A)(2)(C) & (A)(5), and California's Invasion of Privacy Act.

170. The NAISP Defendants did the acts alleged herein pursuant to, and in furtherance of, that agreement and/or furthered the conspiracy by cooperating, encouraging, ratifying, or adopting the acts of the others.

171. As a direct and proximate result of the aiding and abetting of these acts, Plaintiffs have suffered injury and harm and loss, including, but not limited to, loss of the user's privacy with respect to their actions on the internet (where class members shop, what they buy and look at, where they browse, and what goods and services they seek), loss of privacy with

respect to their associational relationships on the internet); and loss of privacy with respect to their interests, hobbies, and activities on the internet.

172. The wrongful conduct committed pursuant to the conspiracy was a substantial factor in causing this harm.

173. The NAISP Defendants' intentional agreement to commit, and commission of, these wrongful acts was willful, malicious, oppressive, and in conscious disregard of Plaintiffs' rights, and Plaintiffs are therefore entitled to an award of punitive damages to punish their wrongful conduct and deter future wrongful conduct.

**Count VII**
**Unjust Enrichment**
**Against All Defendants**

174. Plaintiffs incorporate by reference the foregoing allegations.

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

176. A benefit has been conferred upon all defendants by Plaintiffs and the Class. On information and belief, Defendants, directly or indirectly, have received and retain information regarding communications between Plaintiffs and internet product and service providers, and has received and retains information regarding specific purchase and transactional information that is otherwise private, confidential, and not of public record, and/or have received revenue from the provision of such information.

177. Defendants appreciate or have knowledge of said benefit.

178. Under principles of equity and good conscience, Defendants should not be permitted to retain the information and/or revenue which they acquired by virtue of their unlawful conduct. All funds, revenues, and benefits received by Defendants rightfully belong to

Plaintiffs and the Class, which Defendant has unjustly received as a result of its actions.

**Prayer for Relief**

WHEREFORE, Plaintiffs respectfully pray 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 Defendants from engaging in the acts alleged above; (ii) requiring Defendants to disgorge all of their ill-gotten gains to Plaintiffs and the other Class members, or to whomever the Court deems appropriate; (iii) requiring Defendants to delete all data surreptitiously or otherwise collected through the acts alleged above; (iv) requiring Defendants to provide Plaintiffs and the other class members a means to easily and permanently decline any participation in any data collection activities by means of the NebuAd device or any similar device, in any present or future iteration of the NebuAd device; (v) awarding Plaintiffs and class members full restitution of all benefits wrongfully acquired by Defendant by means of the wrongful conduct alleged herein; and (vi) ordering an accounting and constructive trust imposed on the data, funds, or other assets obtained by unlawful means as alleged above, to avoid dissipation, fraudulent transfers, and/or concealment of such assets by Defendants;

c) For a preliminary and permanent injunction restraining Defendants, their officers, agents, servants, employees, and attorneys, and those in active concert or participation with any of them from

(1) transmitting any information about Plaintiffs or class member's 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;

(2) transmitting any information about Plaintiffs or class member's 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 Plaintiffs 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**

The Plaintiffs hereby demand a trial by jury of all issues so triable.

Respectfully submitted,

DATED this 10th day of November, 2008.

By: Alan Himmelfarb

Alan Himmelfarb
KamberEdelson, LLC
2757 Leonis Blvd.
Vernon, California 90058-2304
Telephone: (323) 585-8696
ahimmelfarb@kamberedelson.com

Scott A. Kamber

KamberEdelson, LLC
11 Broadway, 22nd Floor.
New York, NY. 10004
Telephone: (212) 920-3072
Fax: (212) 202-6364
skamber@kamberedelson.com *(Pro Hac Vice Pending)*

Joseph H. Malley
Law Office of Joseph H. Malley
1045 North Zang Boulevard
Dallas, Texas 75208
Ph. (214) 943-6100
Fax (214) 943-6170
malleylaw@gmail.com *(Pro Hac Vice Pending)*