lml

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS

KATHLEEN KIRCH and TERRY KIRCH,
individually, and on behalf of themselves
and all others similarly situated,

Plaintiffs,

v.

EMBARQ MANAGEMENT CO., a
Delaware Corporation, and UNITED
TELEPHONE COMPANY OF EASTERN
KANSAS, a Delaware Corporation, and
DOE DEFENDANTS 1-5,

Defendants.

Case No. 10-2047-JAR

MEMORANDUM AND ORDER

Kathleen and Terry Kirch filed this putative class action against Internet service providers Embarq Management Company and United Telephone Company of Eastern Kansas (collectively, "Embarq"). Plaintiffs allege common law claims for invasion of privacy and trespass to chattels, as well as claims for violation of the Computer Fraud and Abuse Act ("CFAA") and the federal Electronic Communications Privacy Act ("ECPA"). All claims relate to Embarq's collection and diversion of its customers' Internet communications to a third party Internet advertising company, NebuAd, Inc. ("NebuAd"), who used the information to target the customers with advertising. Per stipulation, plaintiffs agreed to dismiss Counts I, III and IV (invasion of privacy, CFAA and trespass to chattels).[1] Before the Court are two motions:

[1] Doc. 60, Ex. 1.

plaintiffs' Motion to Certify Class (Doc. 31) and defendants' Motion for Summary Judgment (Doc. 59) seeking to dismiss the remaining ECPA claim. Oral argument was held July 15, 2011, at which time the Court took the motions under advisement. After considering the parties' arguments and submissions, the Court is ready to rule. For the reasons set forth in detail below, the Court grants defendants' Motion for Summary Judgment and denies plaintiffs' Motion to Certify Class as moot.[2]

I. Procedural Background

In November, 2008, plaintiffs Kathleen and Terry Kirch, as well as others, brought suit in the Northern District of California against NebuAd, Embarq, and several other Internet service providers ("ISPs"), alleging violations of the ECPA.[3] Embarq moved to dismiss on multiple grounds, and the California court dismissed the complaint against Embarq and the other ISPs for lack of personal jurisdiction. Plaintiffs refiled against Embarq in the District of Kansas; other plaintiffs refiled against other ISPs in Montana, Alabama, Georgia, and Illinois, using common counsel in Los Angeles. Plaintiffs continue to pursue their case against NebuAd in California.

II. Summary Judgment Standard

Summary judgment is appropriate if the moving party demonstrates that there is "no

[2] The Complaint also names Doe Defendants 1-5, who are identified as "entities associated with Embarq and/or UTC, possibly with contractual obligations with Defendants, that may require Defendants to provide notice to the Does of this matter so as to appear and represent their interests. When the identities of any Does who are sued as Does are identified, Plaintiffs will amend their complaint to name such parties." Although a plaintiff may generally plead claims against unknown defendants, he must "provide [] an adequate description of some kind which is sufficient to identify the person involved so process eventually can be served." *Fisher v. Okla. Dep't of Corr. Unknown State Actor and/or Actors*, 213 F. App'x 704, 708 n.2 (10th Cir. 2007) (quoting *Roper v. Grayson*, 81 F.3d 124, 126 (10th Cir. 1996)). Here, the Complaint does not allege with any specificity which claims involve the Doe defendants or what roles those unknown individuals might have played in this matter, nor have plaintiffs moved to amend the Complaint to name such parties. Because all other claims against Embarq are dismissed below, the Court dismisses these Doe defendants as well.

[3] *Valentine et al. v. NebuAd Inc., et al.*, No. 3:08-cv-05113 (N.D. Cal.).

genuine dispute as to any material fact" and that it is "entitled to a judgment as a matter of law."[4] In applying this standard, the court views the evidence and all reasonable inferences therefrom in the light most favorable to the nonmoving party.[5] A fact is "material" if, under the applicable substantive law, it is "essential to the proper disposition of the claim."[6] An issue of fact is "genuine" if "there is sufficient evidence on each side so that a rational trier of fact could resolve the issue either way."[7]

The moving party initially must show the absence of a genuine issue of material fact and entitlement to judgment as a matter of law.[8] In attempting to meet this standard, a movant that does not bear the ultimate burden of persuasion at trial need not negate the other party's claim; rather, the movant need simply point out to the court a lack of evidence for the other party on an essential element of that party's claim.[9]

Once the movant has met this initial burden, the burden shifts to the nonmoving party to "set forth specific facts showing that there is a genuine issue for trial."[10] The nonmoving party may not simply rest upon its pleadings to satisfy its burden.[11] Rather, the nonmoving party must

[4] Fed. R. Civ. P. 56(a).

[5] *Spaulding v. United Transp. Union*, 279 F.3d 901, 904 (10th Cir. 2002).

[6] *Wright ex rel. Trust Co. of Kan. v. Abbott Labs., Inc.*, 259 F.3d 1226, 1231-32 (10th Cir. 2001) (citing *Adler v. Wal-Mart Stores, Inc.*, 144 F.3d 664, 670 (10th Cir. 1998)).

[7] *Adler,* 144 F.3d at 670 (citing *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986)).

[8] *Spaulding*, 279 F.3d at 904 (citing *Celotex Corp. v. Catrett*, 477 U.S. 317, 322-23 (1986)).

[9] *Adams v. Am. Guar. & Liab. Ins. Co.*, 233 F.3d 1242, 1246 (10th Cir. 2000) (citing *Adler*, 144 F.3d at 671).

[10] *Anderson*, 477 U.S. at 256; *Celotex,* 477 U.S. at 324; *Spaulding*, 279 F.3d at 904 (citing *Matsushita Elec. Indus. Co. v. Zenith Radio Corp.,* 475 U.S. 574, 587 (1986)).

[11] *Anderson*, 477 U.S. at 256; *accord Eck v. Parke, Davis & Co.,* 256 F.3d 1013, 1017 (10th Cir. 2001).

"set forth specific facts that would be admissible in evidence in the event of trial from which a rational trier of fact could find for the nonmovant."[12] To accomplish this, the facts "must be identified by reference to an affidavit, a deposition transcript, or a specific exhibit incorporated therein."[13] Rule 56(c)(4) provides that opposing affidavits must be made on personal knowledge and shall set forth such facts as would be admissible in evidence.[14] The non-moving party cannot avoid summary judgment by repeating conclusory opinions, allegations unsupported by specific facts, or speculation.[15] "

Finally, summary judgment is not a "disfavored procedural shortcut"; on the contrary, it is an important procedure "designed to secure the just, speedy and inexpensive determination of every action."[16] In responding to a motion for summary judgment, "a party cannot rest on ignorance of facts, on speculation, or on suspicion and may not escape summary judgment in the mere hope that something will turn up at trial."[17]

III. Uncontroverted Facts

Consistent with the well-established standard for evaluating a motion for summary judgment, the following facts are either uncontroverted or stated in the light most favorable to the nonmoving party. The Court notes that the majority of the facts set forth by Embarq are

[12] *Mitchell v. City of Moore, Okla.*, 218 F.3d 1190, 1197-98 (10th Cir. 2000) (quoting *Adler*, 144 F.3d at 671).

[13] *Adams*, 233 F.3d at 1246.

[14] Fed. R. Civ. P. 56(c)(4).

[15] *Id.*; *Argo v. Blue Cross & Blue Shield of Kan., Inc.*, 452 F.3d 1193, 1199 (10th Cir. 2006) (citation omitted).

[16] *Celotex Corp. v. Catrett*, 477 U.S. 317, 327 (1986)(quoting Fed. R. Civ. P. 1).

[17] *Conaway v. Smith*, 853 F.2d 789, 794 (10th Cir. 1988).

either undisputed, or that plaintiffs claim to lack information to dispute the facts asserted. With respect to the latter, however, plaintiffs do not assert that relief is appropriate under Fed. R. Civ. P. 56(d), and because Rule 56(e) requires a plaintiff to properly address another party's assertion of fact as required by Rule 56(c), the Court thus considers such facts as undisputed.[18]

United Telephone Company of Eastern Kansas ("UTC") is, among other things, an ISP that provides high-speed Internet services to subscribers in Kansas. At all relevant times, UTC did business under the brand name "Embarq." Embarq Management Company ("EMC") is a corporate affiliate of UTC and provides contracted products, services, and employees to UTC and other CenturyLink subsidiaries. EMC provides no services to the public and has no customer-facing operations.

NebuAd's Role

NebuAd is a company headquartered in California that operated as an online advertising company. NebuAd contracted with a number of ISPs to allow it to install its Ultra-Transparent Appliance ("UTA") on the ISPs' networks. NebuAd sought to deliver advertisements targeted to the interests of individuals who used the ISPs' networks, based on interest profiles constructed by NebuAd's UTA and associated server computers ("the NebuAd System"). The NebuAd System built interest profiles based on information concerning certain websites that users visited.

In November 2007, on behalf of UTC, EMC entered into a Technology Trial Evaluation Agreement with NebuAd to test the UTA. Company personnel performed laboratory tests and determined that routing Internet traffic through the UTA did not affect network integrity or

[18] Fed. R. Civ. P. 56; D. Kan. Rule 56.1(e) (requiring responding party to specifically set forth in detail the reasons why they cannot admit or deny a fact).

performance. After laboratory testing was complete, it was decided to allow NebuAd to field test the UTA in a "live" environment. UTC's Gardner, Kansas point of presence was selected for the test ("the NebuAd test") because it was the smallest point of presence, with approximately 26,000 high-speed Internet subscribers, and it was proximate to qualified technical and product development staff. EMC does not own the network facilities on which the NebuAd equipment was installed; rather, those network facilities are owned and operated by UTC. The NebuAd test began in mid-December 2007 and was stopped completely by the end of March 2008. Embarq received $29,143 from NebuAd as compensation for the NebuAd test.

Plaintiffs' experts admitted that NebuAd's UTA did not degrade the performance of any customer's Internet service, and plaintiffs have stipulated that NebuAd's UTA caused no damage to any Embarq customer's computer. The NebuAd System did not serve pop-up advertisements. The System did not increase the number of advertisements served to a user, but rather, served advertisements only in place of the advertisements that otherwise would have been served to the user. The System was authorized by other advertising networks to replace their advertisements with its own.

All Internet traffic that passed through UTC's Gardner point of presence flowed through NebuAd's UTA. NebuAd's UTA identified the "port number" associated with each internet communication passing through UTC's Gardner point of presence. Different port numbers are associated with different types of Internet communications. Port 80 is associated with "HTTP traffic," and only websites whose addresses begin with "http://" are accessed through Port 80. An IP address is a series of numbers associated with a server or website, and it is used to route traffic to the proper destination on the Internet. The NebuAd System employed a technology called “deep packet inspection” (“DPI”) to identify the URL requested by a user. A URL, which stands for “Uniform Resource Locator,” is the address of a page on the world wide web. URLs specify the host server name, directory, and file name of the Web page that a user seeks to visit.

The NebuAd System also used DPI to access cookies sent to and from advertising networks, as well as the URL of the “referer” page, *i.e.*, the web page received by the user’s computer immediately prior to its request for a new page. A cookie is a piece of text, usually encrypted, that is sent to a user’s computer by a website. When the user later returns to the website, the website recognizes the cookie and thus is able to track a user’s behavior over time. Cookies are regularly used on the Internet to store site preferences, retain a user’s shopping cart contents, or, in the case of advertising networks, allow the advertising network to recognize the same user across a wide array of different websites. The advertising network cookies observed by the NebuAd system were typically encrypted, meaning they would have appeared as a long string of numbers and letters that were unreadable, so the NebuAd System did not extract any information from them.

The NebuAd System used the long string of numbers and letters constituting an advertising network cookie to help create an anonymized identification number it assigned to each user’s computer. The System created a profile linked to the anonymized identification number. Profiles were associated with a user’s computer solely through the anonymized identifier number that the NebuAd System had assigned. NebuAd designed its System with the intention that it would not have been possible to “reverse engineer” its anonymized identifier numbers and identify the actual users associated with them. There is no evidence that anyone ever attempted or succeeded in identifying any actual users associated with the identifier numbers or the profiles created by the NebuAd System. A profile stored information concerning what the NebuAd System had inferred to be a user's market interests, based upon the URLs it obtained. When the NebuAd System saw a URL that had previously been identified as reflecting a certain market interest, the computers in the NebuAd System converted the URL into a code signifying a market interest and then deleted the raw data. The NebuAd System then created or updated a profile to reflect the market interests it observed. The process of converting a URL into a code signifying a market interest and then deleting the raw data likely took microseconds, and no more than a minute. The process of extracting URLs, converting them to predefined market interests, and updating user profiles was entirely automated and involved no human intervention. The targeted advertisements that the NebuAd System served were based upon the de-identified profiles it had constructed.

Embarq's Role

NebuAd remotely configured the UTA to make the device operable. Thereafter, the NebuAd System collected information, created de-identified user profiles and served ads. Plaintiffs' expert, Alissa Cooper, testified that her understanding of Embarq's role with respect to the NebuAd System as the ISP was that Embarq "furnished the connection to the NebuAd equipment, so, it essentially connected its users to the UTA, and it connected the UTA to the rest of its networks." Cooper testified that there was no other involvement by the ISP, other than it was paid, and that Embarq did not serve any advertisements based upon the user profiles developed by the NebuAd System. Cooper further testified that Embarq did not have access to the data collected or the user profiles developed by the NebuAd System, and that any access Embarq had to the raw data was access that any ISP ordinarily has to raw data that flows through the ISP's network.[19]

Consent/Privacy Policy

As a condition of the High-Speed Internet Activation Customer Agreement ("Activation Agreement"), Embarq subscribers were required to agree to the terms of Embarq's Privacy Policy.[20] The Activation Agreement states that

> EMBARQ'S network gathers information about Internet usage such as the sites visited, session lengths, bit rates, and number of messages and bytes passes. EMBARQ uses this information in the aggregate. EMBARQ may share this aggregated information with other parties from time to time. EMBARQ also collects and uses personally identifiable information obtained from you and from other sources for billing purposes, to provide and change service, to anticipate and resolve problems with your service, or to identify, create and inform you of products and services that better meet your needs. Except as otherwise provided in this Section, EMBARQ will not use or disclose any of your personally identifiable information unless compelled by a court order or subpoena, you consent to the use of disclosure, or to protect its broadband services and facilities. . . . EMBARQ's provision of Services to you is also subject to EMBARQ's broadband privacy policies, which are found at http://www.embarq.com/legal/privacy.html/broadbandservices and are hereby incorporated by reference.[21]

The Activation Agreement informed subscribers that "EMBARQ may revise, modify or discontinue any or all aspects of the Services, including but not limited to . . . any terms of this Agreement, upon posting of the new terms on the EMBARQ website at www.EMBARQ.com." The Activation Agreement states that it "is a legally binding contract that should be read in its

[19] Doc. 60, Ex. 6.

[20] Doc. 60, Ex. 2-A.

[21] *Id.*

entirety," and instructs customers to click on the "accept" button if they agree with each and every term set forth in the Activation Agreement.[22]

Embarq's Privacy Policy, effective November 2007, informed subscribers that "[d]e-identified data also might be purchased by or shared with a third party." The Privacy Policy further states that Embarq could disclose to third party business partners "customer proprietary network information," ("CPNI"), which is defined to include "the websites you visit," to enable business partners to assist in providing Embarq's service. The Privacy Policy also states that "EMBARQ does not disclose CPNI and other nonpublic personal information (such as credit card numbers), without your consent or direction, except to business partners involved in providing EMBARQ service to customers or as required or permitted by law." Subscribers were also notified that the Privacy Policy could be updated periodically to reflect changing practices, specifically that "[i]f at any point we decide to use personally identifiable information in a manner that is materially different from what was stated at the time it was collected, we will notify you via posting on this page for 30 days before the material change is made and give you an opportunity to opt out of the proposed use at any time."

Prior to the NebuAd test, Embarq added to the section of its Privacy Policy concerning "USE OF PERSONAL INFORMATION" a paragraph entitled, **"Preference Advertising"** that stated:

> Embarq may use information such as the websites you visit or online searches that you conduct to deliver or facilitate the delivery of targeted advertisements. The delivery of these advertisements will be based on anonymous surfing behavior and will not include

[22] *Id*.

> users' names, email addresses, telephone numbers, or any other Personally Identifiable Information.
>
> You may choose to opt out of this preference advertising service. By opting out, you will continue to receive advertisements as normal; but these advertisements will be less relevant and less useful to you. If you would like to opt out, click here. (embarq.com/adsoptions)

Although all traffic, including that of customers who opted out, flowed through the UTA, by clicking on the "opt out" link in the Privacy Policy, a subscriber could ensure that the NebuAd System would not create a profile of that subscriber and would not serve any targeted advertisements to that subscriber. Plaintiffs did not opt out of the Preference Advertising service. Kathleen Kirch testified that she does not recall reviewing Embarq's Privacy Policy and that she did not make a practice of reviewing privacy policies of any Internet service she signed up for or websites that she visited. Instead, she just clicked "I agree," and continued on to the site. Kirch further testified that she understood that when she did so, she was bound by the terms of the policy.[23]

IV. Discussion

Plaintiffs, representing a putative class, allege that for a period exceeding ninety days in 2008, Embarq, as an ISP, collected and diverted approximately 26,000 of its Gardner, Kansas customers' internet communications to NebuAd, a third-party internet advertising company, who used the information to target the customers with advertisements. Plaintiffs allege Embarq's actions constitute a violation of Title II of the ECPA, which Act amended the Wiretap Act, 18 U.S.C. § 2510 *et seq*. 18 U.S.C. § 2511(1)(a) provides for criminal penalties where a person

[23] Doc. 60 at Ex. 10.

"intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication," as well as where one person "intentionally discloses" to another, or "intentionally uses or endeavors to use, the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the interception of a[n] electronic communication." By contrast, the civil liability provision set forth in 18 U.S.C. § 2520 states that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity which engaged in that violation."

Embarq argues that it cannot be held civilly liable under the ECPA because § 2520(a) does not provide for liability of aiders and abettors and that Embarq itself did not intercept plaintiffs' electronic communications in violation of the ECPA. Alternatively, Embarq argues that even if it had intercepted an electronic communication, plaintiffs consented to the interception and use of their electronic communications. The Court addresses each issue in turn.

A. Secondary Liability

Plaintiffs argue that the NebuAd System violated the ECPA because it intercepted or acquired the "contents" of Embarq's customers' Internet communications. Highly simplified, plaintiffs assert that "the UTA intercepted and analyzed *all* of the traffic that passed through it." Embarq counters that the UTA merely identified the port number of a communication and the URLs acquired by the NebuAd System were functionally no different from a telephone number acquired by a pen register; it is merely the address of the webpage requested by the user, not the webpage itself, and thus is a "means of establishing communication."[24] The Court need not

[24] *See New York Tele. Co.*, 434 U.S. at 167.

resolve this issue, however, because even assuming plaintiffs' position is correct, Embarq cannot be held secondarily liable for having aided and abetted NebuAd's alleged interception.

Plaintiffs argue that Embarq intercepted communications by routing them to NebuAd's UTA. The term "intercept" is specifically defined by the ECPA to mean the "acquisition of the contents" of a communication."[25] "Contents" is defined to mean "the substance, purport, or meaning of that communication."[26] Although the term "acquisition" is not defined by the statute, "to acquire" commonly means "to come into possession, control, or power of disposal."[27] Thus, it follows that in order to "intercept" a communication, one must come into possession or control of the substance, purport, or meaning of that communication. The Court agrees with Embarq that regardless of what information the NebuAd System extracted from the communications traversing through the UTA, it is undisputed that Embarq had no access to that information or to the profiles constructed from that information.[28] As plaintiffs' expert testified, Embarq's role was to install the NebuAd device so as to furnish the UTA connection to NebuAd. In other words, the NebuAd device, or "box," goes into place, then all of the raw data that flows through Embarq is directed to that device, where NebuAd does the analysis and, apparently, separates out the Port 80 traffic. Moreover, plaintiffs cite no authority that Embarq's access to the raw data that flowed through its network constitutes a violation of the ECPA, which requires an entity to

[25] 18 U.S.C. § 2510(4).

[26] 18 U.S.C. § 2510(8).

[27] WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY UNABRIDGED 18-19 (1986).

[28] Incredibly, at oral argument, plaintiffs' counsel went so far as to claim that Embarq employees reviewed the raw data and transported information of their choosing to NebuAd. Plaintiffs do not cite, nor could the Court locate, anything in the record to support this assertion, which is contradicted by testimony of plaintiffs' experts.

actually acquire the contents of those communications. There is nothing in the record that Embarq itself acquired the contents of any communications as they flowed through its network; instead, plaintiffs' theory rests on the notion that the NebuAd System extracted the contents of the communications. Plaintiffs' assertion that Embarq "endeavored to intercept" communications falls short of creating civil liability under the ECPA, which creates liability for actual interception.

In an apparent effort to avoid this result, plaintiffs seek to hold Embarq secondarily liable based upon its contractual relationship with NebuAd, emphasizing that Embarq licensed the UTA owned by NebuAd and allowed NebuAd to access its network. Plaintiffs, in effect, seek to hold Embarq indirectly liable as a procurer, aider, abettor, or co-conspirator of NebuAd's alleged violation of the ECPA. The civil liability provision of the ECPA, however, does not provide for secondary liability, as liability attaches only to the party that actually intercepted a communication.[29] As numerous courts have consistently held, a defendant does not "intercept" a communication merely by allowing or enabling, or even directing, another party to intercept communications.[30] For example, in *In re Toys R Us, Inc., Privacy Litigation,*[31] plaintiffs sought to hold Toys R Us liable under the Wiretap Act for permitting a third party, Coremetrics, to load

[29] 18 U.S.C. § 2520.

[30] *See, e.g., Freeman v. DirectTV, Inc.*, 457 F.3d 1001, 1005-06 (9th Cir. 2006) (rejecting the argument that "a person or entity who aids and abets or who enters into a conspiracy is someone or something that is 'engaged' in a violation."); *Doe v. GTE Corp.*, 347 F.3d 655, 658 (7th Cir. 2003) ("[N]othing in the statute condemns assistants, as opposed to those who directly perpetrate the act."); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 168-69 (5th Cir. 2000) (same); *Reynolds v. Spears*, 93 F.3d 428, 432-33 (8th Cir. 1996); *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001); *Perkins-Carillo v. Systemax, Inc.*, No. 03-2836, 2006 WL 1553957 (N.D. Ga. May 26, 2006); *In re Toys R Us, Inc., Privacy Litig.*, No. 00-2746, 2001 WL 34517252, at *6-7 (N.D. Cal. Oct. 9, 2001).

[31] 2001 WL 34517252.

"Web bugs" onto the computers of visitors to Toys R Us' website.[32] Coremetrics was in the business of tracking Internet users' buying and websurfing habits, and its device enabled it to "monitor, intercept, transmit, and record all aspects of a Webuser's private activity when they access Toys R Us' Webpages or other Webpages."[33] The district court granted Toys R Us' motion to dismiss plaintiffs' Wiretap Act claim, holding that the "plain language of § 2205(a) now limits its applicability to those who 'intercept,' 'disclose,' or 'use' the communications at issue" and that Toys R Us could not be held liable because there was no allegation that Toys R Us itself intercepted any communications.[34] Such is the case here, and plaintiffs cite no authority to the contrary.

Because the record shows that Embarq did not acquire any of the information obtained by the NebuAd System, under the plain language of the ECPA, Embarq did not itself intercept any communications and cannot be held secondarily liable. Accordingly, Embarq is entitled to summary judgment on this ground.

B. Consent

Embarq is also independently entitled to summary judgment based on plaintiffs' consent, which is expressly excluded from the category of "unlawful interceptions."[35] In two other cases brought by plaintiffs' law firm arising out of NebuAd System tests conducted in Montana, the

[32] *Id*. at *6-7.

[33] *Id*. at *1.

[34] *Id*. at *6-7.

[35] 18 U.S.C. § 2511(2)(d) (no liability "where one of the parties to the communication has given prior consent to such interception.").

district court dismissed the ECPA count based on similar language contained in the ISPs' privacy policies.[36] In those cases, the court considered the Terms of Service documents of the ISPs, and found that the plaintiff Internet subscribers were put on notice of the NebuAd monitoring via the defendant ISPs' updates to those terms.[37] As the court explained, because that document indicated that "[u]se of [the ISP's] Internet access services was expressly subject to the [Terms of Service]" and the plaintiff continued to use the Internet, he was bound by the changes to the agreement and impliedly consented to the monitoring of his Internet activity.[38] Likewise, the Court finds that in this case plaintiffs consented to the use by third parties of their de-identified web-browsing behavior when they accessed the Internet under the terms of Embarq's Privacy Policy, incorporated by reference into its Activation Agreement.

Embarq's Activation Agreement informed subscribers that "EMBARQ may revise, modify or discontinue any or all aspects of the Services, including but not limited to . . . any terms of this Agreement, upon posting of the new terms on the EMBARQ website at www.EMBARQ.com." Plaintiffs do not dispute that, in advance of the NebuAd test, Embarq posted a new paragraph in its Privacy Policy entitled "Preference Advertising," in which it informed subscribers that "Embarq may use information such as the websites you visit or online searches that you conduct to deliver or facilitate the delivery of targeted advertisements. The delivery of these advertisements will be based on anonymous surfing behavior." Subscribers

[36] *See Deering v. CenturyTel, Inc.*, No. 10-63-BLG-RFC, 2011 WL 1842859 (D. Mont. May 16, 2011); *Mortensen v. Bresnan Commc'ns, L.L.C.*, No. 10-13-BLG-RFC, 2010 WL 5140454 (D. Mont. Dec. 13, 2010). A similar motion to dismiss on consent grounds is pending in yet another NebuAd case filed in Illinois, *Valentine v. Wideopen West Fin., LLC*, Case No. 09-cv-7653 (E.D. Ill.).

[37] *See Deering*, 2011 WL 1842859, at *1-3, *Mortensen*, 2010 WL 5140454, at *4-5.

[38] *Deering*, 2011 WL 1842859, at *1-3.

were then offered the opportunity to opt out by clicking on a hypertext link. Moreover, a pre-existing paragraph in the Privacy Policy informed subscribers that "[d]e-identified data might be purchased by or shared with a third party." The pre-existing Privacy Policy also explained that Embarq would automatically "log the websites you visit," and that such information, which constitutes CPNI, could be shared with "business partners involved in providing EMBARQ service to customers." Thus, as with the Montana cases, plaintiffs consented to monitoring by using Embarq's Internet service after notice, and that notice and consent defeats their ECPA claim.

Nevertheless, plaintiffs assert several reasons why their use of Embarq's Internet service did not constitute consent to the NebuAd test. The Court will briefly address these arguments, which are without merit. First, plaintiffs argue that the scope of the disclosure was inadequate because NebuAd is not identified specifically as a third party with which information might be shared. Plaintiffs cite no authority requiring such specific disclosure, and fail to address the fact that the Privacy Policy expressly discloses that de-identified data and the websites a subscriber visits might be shared with third parties. While it is true that NebuAd was identified specifically in one of the cases,[39] the Montana court did not appear to make such a distinction, instead focusing on the fact that the terms of the agreements and privacy policies in those cases existed and were in effect before the NebuAd test, and also mentioned third parties generally.[40] Second, plaintiffs' argument that the notice was not conspicuous enough is belied by their admission that the prevailing industry practice among websites is to disclose their relationship with advertising

[39] *Id*. at *2.

[40] *Id*. at *2-3; *Mortensen*, 2010 WL 5140454, at *5.

networks and the type of information those networks collect, in their privacy policies. Plaintiffs cite no authority that such method of disclosure is inadequate, and the Montana case decisions dismissing on the ground of consent hold to the contrary.[41] Finally, plaintiffs' argument that the opt-out mechanism was insufficient because it did not prevent the NebuAd System's collection of data does not negate their consent because they did not attempt to opt out. Plaintiffs do not dispute that the opt-out mechanism was effective in that, by opting out, subscribers did not receive any targeted advertising.

In sum, plaintiffs were required to agree to the terms of the Activation Agreement in order to use Embarq's Internet service; that Agreement incorporated the terms of the Privacy Policy, which informed subscribers that their de-identified data could be shared with third parties; that Agreement informed subscribers that the terms could be changed at any time through posting a new policy at Embarq's website; and Embarq modified those terms in advance of the NebuAd test to add a paragraph regarding preference advertising, with an opt-out mechanism. For these reasons, the Court joins with the Montana court in concluding that plaintiffs gave or acquiesced their consent to any monitoring or interception of their Internet activity, and summary judgment is granted on this ground.[42]

IT IS THEREFORE ORDERED BY THE COURT that defendants' Motion for

[41] *Id.*

[42] Because the Court grants summary judgment on secondary liability and consent grounds, it does not reach the issue of Embarq's alternative "ordinary course of business" defense. The Court notes that this defense also appears to have merit, as plaintiffs have admitted that Embarq conducted the NebuAd test to further legitimate business purposes and that behavioral advertising is a widespread business and is commonplace on the Internet. 18 U.S.C. § 2510(4) requires an interception must take place "through the use of any electronic, mechanical, or other device"; that phrase is defined to exclude "any device or apparatus which can be used to intercept a[n] . . . electronic communication" that is "being used by a provider of wire or electronic communication device in the ordinary course of business." *Id.* § 2510(5)(a)(ii).

Summary Judgment (Doc. 59) is GRANTED;

IT IS FURTHER ORDERED that plaintiffs' Motion to Certify Class (Doc. 31) is DENIED as moot.

IT IS SO ORDERED.

Dated: August 19, 2011

S/ Julie A. Robinson
JULIE A. ROBINSON
UNITED STATES DISTRICT JUDGE