No. _____

In The
Supreme Court of the United States

KATHLEEN AND TERRY KIRCH,

Petitioners,

v.

EMBARQ MANAGEMENT COMPANY AND
UNITED TELEPHONE COMPANY OF EASTERN KANSAS,

Respondents.

ON PETITION FOR WRIT OF CERTIORARI TO
THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

PETITION FOR WRIT OF CERTIORARI

Scott A. Kamber
Counsel of Record
David A. Stampley
KAMBERLAW LLC
100 Wall Street, 23rd Floor
New York, New York 10005
(212) 920-3072
skamber@kamberlaw.com
dstampley@kamberlaw.com

Counsel for Petitioners

Joseph H. Malley
LAW OFFICE OF
JOSEPH H. MALLEY
1045 North Zang Boulevard
Dallas, Texas 75208
(214) 943-6100
malleylaw@gmail.com

Counsel for Petitioners

Dated: March 28, 2013

THE LEX GROUP[DC] ♦ 1825 K Street, N.W. ♦ Suite 103 ♦ Washington, D.C. 20006
(202) 955-0001 ♦ (800) 856-4419 ♦ Fax: (202) 955-0022 ♦ www.thelexgroup.com

QUESTIONS PRESENTED

1. Does an ISP acquire the contents of its customers' electronic communications within the meaning of the ECPA when the ISP uses a device intentionally to redirect the customers' communication to a third party without the consent of any party to the communications.

2. Does the fact that an ISP transmits customers' electronic communications in its ordinary course of business mean that an ISP acts within the ordinary course of business and therefore does not engage in interception when it reconfigures its network intentionally to redirect customers' communications to a third party without the consent of any party to the communications.

TABLE OF CONTENTS

Page

APPENDIX

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

OTHER AUTHORITIES

PETITION FOR WRIT OF CERTIORARI

Petitioners Kathleen and Terry Kirch respectfully petition for a writ of certiorari to review the judgment of the United States Court of Appeals for the Tenth Circuit in this case.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Tenth Circuit is published at 702 F.3d 1245 and reproduced at Pet.App.1a. The district court's unreported opinion is reproduced at Pet.App.20a.

JURISDICTION

The Tenth Circuit exercised jurisdiction under 28 U.S.C. § 1291, entering judgment on December 28, 2012. The time for filing a petition for rehearing elapsed 45 days later, on February 11, 2013. Fed. R. App. P. 35(c), 40(a)(1). This Court has jurisdiction under 28 U.S.C. § 1254(1).

RELEVANT STATUTORY PROVISIONS

Pertinent portions of the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, are reproduced in the appendix to this petition.

STATEMENT OF THE CASE

This case presents the important federal question of whether an ISP's wholesale redirection of its customers' Internet communications to an

unintended recipient without customer consent lies outside the ISP's ordinary course of business and constitutes interception under the ECPA.

Here, Internet services provider Embarq, unbeknownst to its customers, installed a device in its Internet services network facility to transmit all customer Internet communications to an online advertising network. As part of that installation, Embarq recabled its network to redirect customers' communications through the device before resuming the path to their intended, Internet-connected recipients. The third-party ad network paid Embarq for its access to the Embarq customer communications.

The Tenth Circuit held Embarq did not engage in interception because Embarq did not, itself, extract any substantive content from the communications and therefore did not acquire the communications within the meaning of ECPA. The court further held that, to the extent the ISP acquired or accessed communications, its ordinary course of business as an ISP was to transmit communications and, since it did not extract anything from them, its conduct constituted no more than the ordinary course of business.

A. Statutory Background.

1. Electronic communications.

"The Electronic Communications Privacy Act [ECPA] amends Title III of the Omnibus Crime Control and Safe Streets Act of 1968—the Federal

wiretap law—to protect against the unauthorized interception of electronic communications." S. Rep. No. 99-541, p. 43 (1986), U.S. Code Cong. & Admin. News 1986, p. 3555. "The bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." *Id.*

An electronic communication includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectric, or photooptical system that affects interstate or foreign commerce," with certain exceptions unrelated to this case. 18 U.S.C. § 2510(12). Under the definition of "electronic communications" adopted in the ECPA, "[c]ommunications consisting solely of data, for example, . . . are electronic communications." S. Rep. No. 99-541, p. 43 (1986), U.S. Code Cong. & Admin. News 1986, p. 3568. Congress deliberately choose a broad, functional definition because, as key sponsor Representative Kastenmeier noted at the time:

> [T]he Electronic Communications Privacy Act, is an attempt to react to and anticipate problems with the interception and privacy of new communications technologies. . . . Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today—that is, cellular phones and electronic mail—is destined to be outmoded in a few years.

132 Cong. Rec. H4039-01 (June 23, 1986) (statement of Rep. Kastenmeier).

The ECPA provides a civil remedy for any person whose electronic communication is wrongfully intercepted. 18 U.S.C. § 2520(a) and § 2510(4). "[T]he same civil remedies are available whether the communication was 'oral,' 'wire,' or 'electronic,' as defined by 18 U.S.C. § 2510." *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001).

2. ECPA, ISPs and the Internet.

"When you send an email or other data over the Internet, you send it first to the ISP with which you have service." Steven R. Morrison, *What The Cops Can't Do, Internet Service Providers Can: Preserving Privacy in Email Contents*, 16 VA. J.L. & TECH. 253, 263 (2011). "Everything we say, hear, read, or do on the Internet first passes through ISP computers." Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (2009). As a result, "[t]he potential threat to privacy from unchecked ISP surveillance surpasses every other threat online." *Id.* at 1420

Congress clearly recognized the unique threat posed by service providers possessing such considerable access to our electronic communications. For example, the ECPA provides that, aside from a few specific exclusions (such as disclosures necessary to the provision of services or actually consented to by a user):

> [A] person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

18 U.S.C. § 2511(3)(a). In other words, absent disclosures that are necessary, an ISP's divulging the contents of its customers' communication is statutorily excluded from the scope of its ordinary business. *Id.*

Communications protected under the ECPA include data in transmission on the Internet. "The ECPA adopts a 'broad, functional' definition of an electronic communication." *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003), quoting *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995); *see also Szymuszkiewicz*, 622 F.3d at 705, citing *United States v. Councilman*, 418 F.3d 67, 69 (1st Cir. 2005) (en banc) (definition of interception under the Wiretap Act includes packet-switch technology as well as circuit-switch technology).

B. Material Facts.

1. Embarq redirected the Kirches' Internet communications to a third-party.

Respondents—United Telephone Co. of Eastern Kansas dba Embarq and Embarq Management Co. (collectively "Embarq")—are an Internet Service Provider (ISP). Petitioners Kathleen and Terry Kirch were customers of Embarq's Internet services in Gardner, Kansas. This case concerns a 90-day period in the first half of 2008, when Embarq diverted virtually all Internet communications of the Kirches and its other 26,000 Gardner customers to a third party, NebuAd. NebuAd, an online advertising company, paid Embarq $29,143 for redirecting the data, which Embarq analyzed and used to serve behaviorally targeted online advertisements. The Kirches alleged they did not consent to the redirection of their communications.

2. Embarq reconfigured its network indiscriminately to redirect all Internet communications of its customers.

Embarq accomplished the redirection by licensing from NebuAd a device, called an Ultra Transparent Appliance (UTA), and physically installing the device in the network through which Embarq provided Internet services to customers. Embarq rerouted the cables carrying its customers' Internet traffic so that "*[a]ll Internet traffic* that

passed through [Embarq's] Gardner point of presence flowed through NebuAd's UTA." Pet.App.27a (emphasis added).[1]

C. Proceedings Below.

1. The Kirches file suit.

The present putative class action was filed by the Kirches against Embarq in 2010 in the United States District Court for the District of Kansas.[2] Jurisdiction was based on both 28 U.S.C. § 1331 (for federal claims arising under ECPA) as well as 28 U.S.C. § 1332(d)(2). The Kirches seek damages and other relief for themselves and a class of other customers of Embarq's Internet services who had their Internet communications diverted by Embarq to NebuAd in violation of the ECPA.

2. The district court grants Embarq's summary judgment motion.

Embarq moved for summary judgment arguing: (1) it did not acquire the contents of its

---

[1] The district court's statement quoted above was, in turn, a verbatim quote from Embarq's own statements of undisputed facts in support of its motion for summary judgment. As explained by an Embarq expert witness, "The device was placed on [Embarq's] network in such a way that *all Internet traffic* streaming through [Embarq's] network would also pass through the UTA." Pet.App.13a (emphasis added).

[2] An earlier-filed action in the Northern District of California was dismissed for lack of personal jurisdiction over Embarq. Pet.App.22a. That case proceeded as to claims against NebuAd (PetApp.22a) and was later resolved by a settlement. Pet.App.8a.

customers' Internet communications; (2) the customers consented to disclosing their communications; or (3) the disclosures were not interceptions because the UTA device was being used by Embarq in the ordinary course of its business.

The district court granted the motion. Pet.App.21a. The district court acknowledged that the Kirches were asserting "Embarq intercepted communications by routing them to NebuAd's UTA." Pet.App.35a. Nonetheless, according to the district court, "[P]laintiffs' theory rests on the notion that the NebuAd System extracted the contents of the communications." Pet.App.36a. Applying this "notion," the court decided that Embarq did not acquire the contents of the Kirches' Internet communications. Pet.App.36a-37a.

The district court also found that the Kirches "gave or acquiesced their consent to any monitoring or interception of their Internet activity." Pet.App.42a. The district court did not reach the suggestion that Embarq used the UTA to divert communications in the ordinary course of its business.

3. The Tenth Circuit affirms on limited grounds.

The Tenth Circuit affirmed the summary judgment. Pet.App.1a. Like the district court, the Tenth Circuit focused on whether Embarq acquired the contents of information compiled *by* NebuAd (as opposed to whether, under the ECPA, Embarq

acquired the contents of its customers' Internet communications when it redirected them to NebuAd). Pet.App.3a, 7a-8a, 12a-15a. The Tenth Circuit observed that Embarq merely "had access to users' data that it necessarily had as an ISP" and that "NebuAd's use of the UTA gave Embarq access to no more of its users' electronic communications than it had in the ordinary course of its business as an ISP." Pet.App.14a.

The Kirches also appealed the district court's ruling as to consent. However, the Tenth Circuit did not adjudicate this issue. Pet.App.12a.

REASONS THE WRIT SHOULD BE GRANTED

The present case illustrates the significant harm to societal interests in communication privacy if an ISP is considered to be permitted, in the ordinary course of its business, to sell its customer's private communications to the highest bidder. The Tenth Circuit, in allowing an ISP to escape liability for redirecting the Internet communications of the ISP's customers to a third party simply because the ISP did not, itself, read or extract information from the communications, has raised an important question of federal law that has not been, but should be, settled by this Court.

This case presents an important federal law question of whether ISPs, the universally relied upon purveyors of Internet communications, may freely transmit those communications to parties other than the intended recipients. The answer to this question affects nothing less than the privacy of

communications in what has perhaps become our society's most heavily trafficked avenue of communication. As Justice Rehnquist observed:

> Technology now permits millions of important and confidential conversations to occur through a vast system of electronic networks. These advances, however, raise significant privacy concerns. We are placed in the uncomfortable position of not knowing who might have access to our personal and business e-mails, our medical and financial records, or our cordless and cellular telephone conversations.

Bartnicki v. Vopper, 532 U.S. 514, 542 (2001) (Rehnquist, J., dissenting) (quoting S. Rep. No. 1097, at 69, U.S. Code Cong. & Admin. News 1968, pp. 2112, 2156); *see also U.S. v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("[p]eople disclose . . . the books, groceries, and medications they purchase to online retailers").

Given the entrusted role ISPs play in daily communications, both personal and business, it is critical that the ECPA be interpreted as prohibiting ISPs from redirecting communications at will rather than, as in this case, excusing redirection by adding new elements to the ECPA and, as a backstop, excusing it as the ordinary course of business. If ISPs are allowed to escape liability simply because they redirect communications without first reading them, the ECPA effectively provides *no protection* against ISPs' routinely selling customer

communications to the highest bidder, either in bulk, or even for premiums based on particular, highly valued customers.

Paul Olm's article *The Rise and Fall of Invasive ISP Surveillance*, succinctly captures the heightened privacy concerns that arise under the particular facts presented in this matter:

> [N]othing in society poses as grave a threat to privacy as the ISP, not even Google, a company whose privacy practices have received an inordinate amount of criticism and commentary. Although Google collects a vast amount of personal information about its users, an ISP can always access even more because it owns and operates a privileged network bottleneck, the only point on the network that sits between a user and the rest of the Internet. Because of this fact about network design, a user cannot say anything to Google without saying it first to his ISP, and an ISP can also hear everything a user says to any other websites like Facebook or eBay, things said that are unobtainable to Google. The potential threat to privacy from unchecked ISP surveillance surpasses every other threat online.

Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (2009).

Further, the decision below conflicts with circuits that have recognized that one can only redirect what one has already acquired. As has been stated, "Redirection presupposes interception." *See*, *e.g.*, *United States v. Rodriguez*, 968 F.2d 130, 136 (2d Cir.), *cert. denied*, 506 U.S. 847 (1992) and *U.S. v. Luong*, 471 F.3d 1107, 1109 (9th Cir. 2006). The decision below also conflicts with circuits that have recognized the distinction between the initial capture of a communication and subsequent listening to it. *See*, *e.g.*, *United States v. Shields*, 675 F.2d 1152, 1156 (11th Cir.), *cert. denied*, 459 U.S. 858 (1982); *United States v. Turk*, 526 F.2d 654, 659 (5th Cir.), *cert. denied*, 429 U.S. 823 (1976). The Tenth Circuit's decision is antithetical to the requirement, in government searches and seizures, that a warrant be issued to install a device to collect communications, not merely to listen to communications that have already been collected through such as device. *See*, *e.g.*, *Katz v. U.S.*, 389 U.S. 347, 358-59 (1967) (warrant required for surveillance by placing wiretap on outside of phone booth).

Privacy of communication is an important interest. The ECPA helps to protect the "right to be let alone" as well as promote "the interest . . . in fostering private speech." *Bartnicki*, 532 U.S. at 536 (Breyer, J., concurring), quoting *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). As this Court has recognized, "fear of public disclosure of private conversations might well have a chilling effect on private speech." *Bartnicki*, 532 U.S. at 532-533. Even a plausible threat to communications strike at core values in our society:

> In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger, *even without the reality of such activity,* can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas.

Id. at 533 (quoting President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society 202 (1967)); *see also*, *id.* at 543 (Rehnquist, J., dissenting) (same). It is entirely appropriate that Congress has prohibited unauthorized interception of communicative content that the interceptor does not, itself, read, hear, or extract, or access. Here, Embarq was able to provide a complete version of the communications to an unintended party and that is enough.

Pervasively, Americans trust their ISPs to deliver all manner of personal and business communications to the intended recipients. "[T]he content on the Internet is as diverse as human thought." *Reno v. American Civil Liberties Union*, 521 U.S. 844, 870 (1997). The necessary trust placed in an ISP, and its necessary access to communications, justifies the Congressional prohibition against its redirection of communications. *See* 18 U.S.C. § 2511(3)(a). Allowing ISPs to divert Internet communications under the circumstances at issue here will have far-reaching and negative consequences for a society that values the privacy of communications.

A. An electronic communication is intercepted when, without lawful purpose, the whole of it is redirected to an unintended recipient, regardless of whether communicative content is subsequently extracted from it.

Without discussion, the Tenth Circuit began with an unfounded distinction between communications consisting of data and "information the NebuAd System extracted from the communications" that Embarq diverted. Pet.App.3a, 7a-8a, 10a. The court wrongly presumed that information must be extracted from communications for the contents to have been acquired under the statute. *See*, *e.g.*, Pet.App.3a ("NebuAd acquired various information about Embarq users . . . Embarq's access to ***that*** information . . . .") (emphasis added). In fact, the data redirected by Embarq and provided to NebuAd (*i.e.*, all Internet traffic) obviously contained the contents of the Internet communications included within. Indeed, as a practical matter, when Embarq installed the UTA device and reconfigured the Internet traffic in its network facility, the full traffic stream, including communicative content, had no place to go but where Embarq redirected it; were that not so, those contents would never have reached NebuAd as they obviously did.

Because the Tenth Circuit proceeded from the erroneous premise that interception could only be predicated on acquisition that reaches the point of extraction, the court improperly focused on the fact that Embarq did not acquire extracted content *from*

NebuAd. Pet.App.3a, 13a-14a. However, the interception in this case occurred when Embarq redirected the Kirches' Internet communications, in their entirety, *to* NebuAd. In other words, the Tenth Circuit's imposition of a new, extraction requirement caused it to look in the wrong direction.

NebuAd was not the intended recipient of the Kirches' communications. Embarq did not have the Kirches' consent to redirect their communications to NebuAd, or anyone else. Embarq thus violated the ECPA by using a device to intentionally redirect such communications. 18 U.S.C. § 2510(4).

The ECPA's prohibition against unauthorized interception requires no inquiry into whether or how intercepted communications are used. *Id*. As the Seventh Circuit said of one interception defendant, "He did not learn anything worthwhile. But an intentional interception is enough; the prosecutor need not show that the spy obtained valuable information." *Szymuszkiewicz*, 622 F.3d at 703; *see also U.S. v. Townsend*, 987 F.2d 927, 931 (2d Cir. 1993) ("[a]ll that is relevant is that Townsend intentionally intercepted communications between two unknowing and unconsenting individuals").

Contrary to the Tenth Circuit's opinion below, an interception in violation of the ECPA does not require that an electronic communication be read, heard, or extracted. 18 U.S.C. § 2510(4). Rather, an interception occurs "when the contents . . . are captured or redirected in any way." *Rodriguez*, 968 F.2d at 136.

> The statute does not specify precisely where an interception is deemed to occur. It seems clear that when the contents of a wire communication are captured or redirected in any way, an interception occurs at that time. Such an interception plainly occurs at or near the situs of the telephone itself, for the contents of the conversation, whether bilateral as is usually the case, or multilateral as is the case with a conference call, are transmitted in one additional direction. *Redirection presupposes interception.*

Id. at 136 (emphasis added); *see also Luong*, 471 F.3d at 1109 (citing *United States v. Ramirez*, 112 F.3d 849, 852 (7th Cir. 1997) and *United States v. Denman*, 100 F.3d 399, 403 (5th Cir. 1996)). In the present case, it is clear that Embarq intentionally caused the Kirches' Internet communications to be transmitted to NebuAd, that is, as the Second Circuit put it in *Rodriguez*, "transmitted in one additional direction."

Even construing the far more narrow term "aural acquisition," courts have agreed that listening to the communication is not required to intercept. *See Shields*, 675 F.2d at 1156 (holding interception under the statute "occurred at the time the recording was made, not when persons listened to the tape"), *cert. denied*, 459 U.S. 858 (1982); *see also United States v. Nelson*, 837 F.2d 1519, 1527 (11th Cir.) ("the term 'intercept' as it relates to 'aural acquisitions' refers to the place where a

communication is initially obtained regardless of where the communication is ultimately heard"), *cert. denied*, 488 U.S. 829 (1988); *United States v. Turk*, 526 F.2d at 659 ("we conclude that no new and distinct interception occurs when the contents of a communication are revealed through the replaying of a previous recording"). In short, "the term 'intercept' as it relates to an 'acquisition' refers to the place where a communication is initially obtained" and "[w]hether the communication is heard by the human ear is irrelevant." *Amati v. City of Woodstock*, Ill., 829 F. Supp. 998 (N.D. Ill. 1993).

For example, in *Jacobson v. Rose*, 592 F.2d 515 (9th Cir. 1978), the court rejected an argument that a phone company should not be liable for its part in an illegal wiretap where the police, not the phone company, listened to the conversations.

> Nevada Bell contends that because none of its employees actually listened to tapped conversations, it has not violated the statute.
>
> . . .
>
> [W]e do not believe that Congress meant to allow those tapping phones to determine the possible scope of civil liability by their limiting who among them would listen to the tapes.

Id. at 522. It is equally clear that Congress did not mean to allow parties to escape liability for redirecting electronic communications by their limiting who among them would read or extract information from the diverted communications.

If Congress had intended wiretap liability to depend on reading or extracting information rather than mere control over the transmittal of the communication sufficient to have acquired it, Congress clearly would have provided a very different definition of interception. As one court has recognized, when deciding that aural acquisition does not require listening:

> If Congress had intended the phrase "aural or other acquisition" to mean "overheard," it certainly could have employed the simpler term. The section's additional requirement that a conversation be acquired "through the use of any electronic, mechanical, or other device" suggests that it is the act of diverting, and not the act of listening, that constitutes an "interception."

In re State Police Litigation, 888 F. Supp. 1235, 1264 (D. Conn. 1995).

The statute simply does not require reading or *visual* acquisition of the contents of an electronic communication. Indeed, beyond "aural acquisition," which does not require listening, the far broader term, "or other acquisition" was added by Congress for the specific purposes of protecting even communications consisting solely of data. S. Rep. No. 99-541, 99th Cong., 2d Sess., U.S. Code Cong. & Admin. News 1986, p. 3568. The new language extended privacy protection to new forms of computer-to-computer communications. *Rodriguez*, 968 F.2d at 136, citing S. Rep. No. 99-541, 99th

Cong., 2d Sess., U.S. Code Cong. & Admin. News 1986, pp. 3555, 3555-57, 3562-65, 3567. "This amendment clarifies that it is illegal to intercept the non-voice portion of a wire communication. For example, it is illegal to intercept the data or digitized portion of a voice communication." *Id.* at 3567.

The very nature of the technologies involved renders communications unintelligible to human eyes and ears while in transmission on the Internet, precisely when such communications might be intercepted under the ECPA. Thus, if the contents of electronic communications are to be protected from interception while in transmission, they must be protected without requiring proof of inspection or extraction. The Tenth Circuit, by assuming that electronic communications must be extracted to have been intercepted, improperly added a requirement that the statute was designed to avoid.

Additionally, if the Tenth Circuit decision stands and extraction becomes a prerequisite for a finding of interception, then a violation of the statute could occur *every time* the same raw data is translated into an intelligible form—*i.e.*, a new violation each time a particular computer file is opened. Of course, "[t]his cannot be what Congress intended." *See In re State Police Litigation*, 888 F. Supp. at 1265 ("Defendants' proposed interpretation, in contrast, leads to bizarre results. If an interception occurs only when a defendant actually listens to a recorded conversation, a violation of the Act could occur on every subsequent occasion when that recording is replayed.") (citing *Turk*, 526 F.2d at 658.)

Construed properly, the ECPA's prohibition against unauthorized interception of an electronic communication while in transmission requires that the interceptor acquire, that is, possess or exercise control over the communication, including its contents; interception does not require the extraction, translation, reading, or use of the contents. 18 U.S.C. § 2510(4); *see*, *e.g.*, *Klumb v. Goan*, 884 F. Supp. 2d 644, 661 (E.D. Tenn. 2012) (interception occurred when computer program caused duplicate of e-mail "to be rerouted automatically through the Internet to a third party address"); *Shefts v. Petrakis*, 758 F. Supp. 2d 620, 630 (C.D. Ill. 2010) (interception occurred when surveillance software "acquired and logged Plaintiff's text messages" and not when the defendants subsequently accessed them).

Embarq has suggested the data it redirected was like a letter inside a sealed envelope that Embarq did not read. One problem with Embarq's envelope analogy is that it ignores the facts of this case. Here, it would be somewhat more fitting to analogize that Embarq was entrusted to deliver a postcard to the intended recipient. However, before it did so, Embarq copied the postcard and sent the copy to NebuAd. Under the ECPA, it does not matter whether Embarq "peeked" at the postcard while copying it. It is enough that, just as Embarq acquired the postcard enough to send it on its lawful way, it was Embarq's acquisition that enabled Embarq to redirect it. Otherwise, if Embarq did not acquire the contents of the Kirches Internet communications, those communications could not have reached NebuAd as well as intended recipients.

Embarq obviously did acquire the contents of the communications at issue, or it could not have redirected them. *Rodriguez*, 968 F.2d at 136 ("[r]edirection presupposes interception"). If Embarq had examined the contents, but for some lawful purpose, it still would not excuse its redirection; the fact that Embarq did not examine the communications before redirecting them is irrelevant to any analysis under the ECPA.

B. The ECPA presupposes an ISP's acquisition of customers' electronic communications.

An ISP necessarily acquires its customers' Internet communications, in their entirety, including contents, by assuming control over those communications to transmit them. When ISPs help those communications reach their intended destination, there is obviously no interception under the ECPA. Indeed, the ECPA provides that an ISP may direct a communication to others whose job it is to "forward such communication to its destination." 18 U.S.C. § 2511(3)(b)(iii). However, it is an entirely different matter when an ISP, instead, intentionally redirects a customer's communication to a third party that is not the intended recipient and who has nothing to do with forwarding the communication to its destination. *See* 18 U.S.C. § 2511(3)(a) (ISP "shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient.").

The Tenth Circuit held that "NebuAd's use of the UTA gave Embarq access to no more of its users' electronic communications than it had in the ordinary course of its business as an ISP." Pet.App.14a-15a. Of course, as an ISP, Embarq had essentially total access to its customers' Internet communications. Embarq clearly had sufficient access to the communications at issue to be able to redirect them to a third party. As explained in the previous section of this petition, the definition of interception is satisfied when one takes sufficient control of an electronic communication such that it communication is "transmitted in one additional direction." *Rodriguez*, 968 F.2d at 136. Because Embarq clearly had sufficient control and possession of the Internet communications to redirect them to NebuAd, no further inquiry into acquisition is necessary.

If the Tenth Circuit meant that Embarq redirected these communications in the ordinary course of its business as an ISP, such a holding would be directly contrary to the ECPA. Other than matters that are necessary to providing service, the ECPA specifically excludes redirecting communications from the ordinary business of an ISP:

> [A] person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any

> person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

18 U.S.C. § 2511(3)(a). In other words, aside from specific and limited exceptions not applicable here, one thing that Congress has excluded from being part of ISP's ordinary business is redirecting its customers' communications. *Id.* Although, hypothetically, a necessary redirection might be considered part of an ISP's ordinary business, there has been no argument or evidence in this case that Embarq's redirection of communications to NebuAd was necessary to Embarq's provision of services to customers or any other business necessity.

The Tenth Circuit failed to point to any provision of the ECPA or any case law that actually supports the notion that, by virtue of an ISP's mere access to customer communications in the ordinary course of business, the ISP may intentionally redirect those communications, without consent, to third parties not designated as recipients.

Ironically, the single case cited by the court as supporting its conclusion is *Hall v. EarthLink Network, Inc.*, 396 F.3d 500 (2005). *Hall* does not involve an ISP redirecting communications to an unintended third party. In fact, *Hall* does not even involve a third party. Rather, the case involves an ISP and a user. The ISP stored emails at the user's old address on the ISP's system. The emails were not redirected to any third party. As explained by the district court in the case, the ISP "merely received

and stored e-mails precisely where they were sent—to an address on the Earthlink system." *Hall v. Earthlink Network, Inc.*, No. 98 Civ. 5489 (RO), 2003 WL 22990064 (S.D.N.Y. December 19, 2003). Unsurprisingly, the court held that storing emails "precisely where they were sent" was done by the ISP in the ordinary course of business.

In the present case, the ISP did the exact opposite of directing communications precisely where they were sent. Here, Embarq intentionally redirected its customers' communications to NebuAd. *Hall* does not support the conclusion reached by the Tenth Circuit in the present case. Nothing in the ECPA supports that conclusion either.

C. Remand is necessary.

Because of the Tenth Circuit's erroneous construction of "interception" under the ECPA, it never reached the question of whether Embarq established as a matter of law that the Kirches consented to the interception at issue. Petitioners respectfully request that this court grant this petition, reverse the court of appeals, and remand this case to the court of appeals to address the issue of consent.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

SCOTT A. KAMBER
DAVID A. STAMPLEY
KAMBERLAW LLC
100 Wall Street, 23rd Floor
New York, NY 10005
(212) 920-3072
skamber@kamberlaw.com
dstampley@kamberlaw.com

JOSEPH H. MALLEY
LAW OFFICE OF JOSEPH H. MALLEY
1045 North Zang Boulevard
Dallas, TX 75208
(214) 943-6100
malleylaw@gmail.com

Counsel for Petitioners
Kathleen and Terry Kirch

March 28, 2013

APPENDIX

APPENDIX TABLE OF CONTENTS

[ENTERED: December 28, 2012]

PUBLISH

UNITED STATES COURT OF APPEALS

TENTH CIRCUIT

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

Plaintiffs - Appellants,

v. No. 11-3275

EMBARQ MANAGEMENT CO., a Delaware corporation; UNITED TELEPHONE COMPANY OF EASTERN KANSAS, a Delaware corporation,

Defendants - Appellees,

and

DOE DEFENDANTS 1-5,

Defendants.

APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE DISTRICT OF KANSAS (D.C. NO. 2:10-CV-02047-JAR-GLR)

Rahul Ravipudi, Panish, Shea & Boyle, LLP, (Paul A. Traina, Steven J. Lipscomb, Engstrom, Lipscomb & Lack, with him on the briefs), Los Angeles, California, for Plaintiffs - Appellants.

Matthew E. Price, Jenner & Block, LLP, Washington, D.C., (David A. Handzo, Jenner & Block LLP and J. Emmett Logan, Stinson Morrison Hecker LLP, Kansas City, Missouri, with him on the brief), for Defendants - Appellees.

Before **MURPHY**, **HARTZ**, and **HOLMES**, Circuit Judges.

HARTZ, Circuit Judge.

Plaintiffs Kathleen and Terry Kirch appeal the district court's grant of summary judgment in favor of Defendants United Telephone Company of Eastern Kansas and Embarq Management Company (collectively "Embarq") on the Kirches' claim that Embarq intercepted their Internet communications in violation of the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848. Embarq is an Internet service provider (ISP). The alleged interceptions occurred when Embarq authorized NebuAd, Inc., an online

advertising company, to conduct a technology test for directing online advertising to the users most likely to be interested in the ads. Exercising jurisdiction under 28 U.S.C. § 1291, we affirm the district court's judgment. Although NebuAd acquired various information about Embarq users during the course of the technology test, Embarq cannot be liable as an aider and abettor. And it was undisputed that Embarq's access to that information was no different from its access to any other data flowing over its network. Because this access was only in the ordinary course of providing Internet services as an ISP, this access did not constitute an interception within the meaning of the statute.

I. STATUTORY FRAMEWORK

The ECPA prohibits the interception of "electronic communication," 18 U.S.C. § 2511(1), and imposes criminal and civil liability, *see id.* §§ 2511(4) (criminal penalties); § 2520 (civil liability for damages). Traffic on the Internet is electronic communication. *See id.* § 2510(12) (defining *electronic communication* as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system").

The statute defines *intercept* as "the aural or other acquisition of the contents of any wire, electronic, or oral communication *through the use of any electronic, mechanical, or other device*." *Id.* § 2510(4) (emphasis added). No "interception," and hence no violation of the ECPA, occurs if the

contents of a communication are acquired in the ordinary course of business of an ISP because the Act's definition of *electronic, mechanical, or other device* excludes "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business . . . ." *Id.* § 2510(5)(a); *see Hall v. Earthlink Network, Inc.*, 396 F.3d 500, 503–05 (2d Cir. 2005). An interception to which a party to the communication consents also is not prohibited. *See id.* § 2511(2)(d) ("It shall not be unlawful under this chapter for a person . . . to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception . . . .")

The ECPA imposes civil liability on those who unlawfully intercept electronic communications. It states:

> Except as provided in section 2511(2)(a)(ii) [relating to the Foreign Intelligence Surveillance Act of 1978], 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*, other than the United States, *which engaged in that violation* such relief as may be appropriate.

18 U.S.C. § 2520(a) (emphasis added). This language does not encompass aiders or abettors. The only

persons liable are those who engaged in "that violation." And the natural reading of "that violation" is the "intercept[ion], disclos[ure], or intentional[] use[] . . . in violation of [the statute]." In other words, "the person or entity . . . which engaged in that violation" is the person or entity that "intercepted, disclosed, or intentionally used" the communication. The provision includes no aiding-and-abetting language. As the Supreme Court has said:

> Congress has not enacted a general civil aiding and abetting statute . . . . Thus, when Congress enacts a statute under which a person may sue and recover damages from a private defendant for the defendant's violation of some statutory norm, there is no general presumption that the plaintiff may also sue aiders and abettors.

Cent. Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A., 511 U.S. 164, 182 (1994).

Any temptation to read the statute as imposing aider-and-abettor liability is overcome by the illuminating statutory history of the civil-liability provision. The 1968 predecessor to the ECPA imposed both criminal and civil liability for those who procured an interception. The criminal provision, codified as 18 U.S.C. § 2511(1)(a) (1968), held responsible "any person who . . . willfully intercepts, endeavors to intercept, or *procures* any other person to intercept or endeavor to intercept, any wire or oral communication." Pub. L. No. 90-351,

Title III § 802, 82 Stat. 197, 213 (1968) (emphasis added). (Later paragraphs made it a crime to willfully disclose or use unlawfully intercepted communications. *See* 18 U.S.C. § 2511(1)(c), (d) (1968).) Similarly, the civilliability provision stated: "Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall . . . have a civil cause of action against any person who intercepts, discloses, or uses, or *procures* any other person to intercept, disclose, or use such communications." *Id.*, 82 Stat. at 223 (emphasis added) (enacting former 18 U.S.C. § 2520). When the ECPA was enacted in 1986, the criminal provision was changed only to replace "willfully" by "intentionally" and to add "electronic" communications to "wire" and "oral" ones. *See* 18 U.S.C. § 2511(1)(a). But the civil provision was altered in additional ways, including deletion of the "procures" clause. We presume that this deletion was intended to change the statute's meaning. *See Stone v. INS*, 514 U.S. 386, 397 (1995); Antonin Scalia & Bryan A. Garner, Reading Law: The Interpretation of Legal Texts § 40 (2012) ("If the legislature amends or reenacts a provision other than by way of a consolidating statute or restyling project, a significant change in language is presumed to entail a change in meaning."). Accordingly, almost all courts to address the issue have held that § 2520 does not impose civil liability on aiders or abettors. *See Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th Cir. 2000); *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, No. 09-02030, 2012 WL 4054141, *8 (D.D.C. Sept. 17, 2012) (collecting cases). *But see Lonegan v. Hasty*, 436 F. Supp. 2d 419, 427–28 (E.D.N.Y 2006).

II. THE TECHNOLOGY TEST

In November 2007 Embarq entered into an agreement with NebuAd to conduct a test of what is referred to as the NebuAd System. The physical components of the system were an Ultra Transparent Appliance (UTA) and remote servers (apparently in California) hosted by NebuAd. The system's purported purpose was to "allow[] for placement of optimized advertisement on Trial customers' internet browser screens." Aplt. App., Vol. I at 92. The test began in mid-December 2007 and ended in March 2008. Under the agreement the UTA was installed in Embarq's network in Gardner, Kansas, where the Kirches were customers of Embarq. Embarq's Gardner users were connected to the UTA, which was connected to the rest of Embarq's network. According to the Kirches, the Internet traffic that passed through the UTA was sent to the NebuAd servers in its system. NebuAd used the UTA to track what websites an Embarq user visited, and to deliver online advertising thought likely to interest users who visited those websites.

Embarq asserts that the NebuAd System collected only information about customer requests for highly trafficked commercial websites, and obtained only three pieces of information about such requests: the requested Uniform Resource Locator (URL, known in common parlance as a web page's "address"), the "referer URL" (the last URL visited before the request), and an advertising network

cookie.[1] Because cookies are typically encrypted, the NebuAd System did not extract any information from them. Users' computers were assigned identification numbers based on these cookies, and the information about past Internet usage was associated with a user's computer only through this number. The Kirches contend, however, that the UTA "intercepted and analyzed" all Internet traffic from affected customers, *id.* at 61, not only their requests for highly trafficked commercial websites.

III. PROCEEDINGS IN DISTRICT COURT

The Kirches sued Embarq in the United States District Court for the District of Kansas on behalf of themselves and other Embarq customers. They asserted four claims arising out of the NebuAd test: unlawful interception of communications in violation of the ECPA; accessing plaintiffs' computers without authorization, in violation of the Computer Fraud and Abuse Act, *see* 18 U.S.C. § 1030(a), (g); invasion of privacy under Kansas state law; and trespass to chattels under Kansas state law. The latter three claims were dismissed with prejudice by joint stipulation of the parties.[2]

Embarq then moved for summary judgment on the unlawful-interception claim. It argued that

---

[1] "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." Aplt. App., Vol. II at 278.

[2] The Kirches sued NebuAd in a separate proceeding. At oral argument we were informed that the case was settled.

(1) the NebuAd System had not intercepted users' communications, because the limited information it acquired about their Internet communications did not include the contents of those communications; (2) even if user communications were intercepted by the NebuAd System, it was not Embarq that had intercepted the communications, because Embarq did not have access to the data collected by the NebuAd System or the user profiles that NebuAd developed; (3) the Kirches had consented to any alleged interception by agreeing to the terms of Embarq's privacy policy, which gave users notice that their Internet communications could be shared with third parties to the extent that the NebuAd test had done so; and (4) if Embarq had acquired the contents of any of its users' communications, it had done so only in the ordinary course of its business activities as an ISP, and so was not liable under the ECPA.

The district court granted Embarq's motion in August 2011. It first ruled that Embarq had not intercepted the Kirches' communications. It explained:

> 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.[] "Contents" is defined to mean "the substance, purport, or meaning of that communication." Although the term "acquisition" is not defined by the

statute, "to acquire" commonly means "to come into possession, control, or power of disposal." 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. 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 [apparently, traffic to websites whose addresses begin with "http://"]. 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 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.

Mem. & Order at 13–14 (footnotes omitted), *Kirch v. Embarq Mgmt. Co.*, No. 10-2047-JAR (D. Kan. Aug. 19, 2011)(Aplt. Br., Ex. A at 13–14). The court then rejected the argument that Embarq could be liable on a theory of aiding and abetting NebuAd. In the alternative, the court ruled that the Kirches had consented to any interception by agreeing to the terms of Embarq's privacy policy.

IV. DISCUSSION

We review de novo the district court's summary-judgment decision, evaluating the evidence in the light most favorable to the party opposing summary judgment. *See Vaughn v. Epworth Villa*, 537 F.3d 1147, 1150 (10th Cir. 2008). A district court can grant summary judgment only if "there is no genuine dispute as to any material fact" and "the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a).

Like the district court, we need not address whether NebuAd intercepted any of the Kirches' electronic communications. Because the ECPA creates no aiding-and-abetting civil liability, Embarq is liable only if it itself intercepted those

communications. Also, although the district court relied on consent as an alternative ground for summary judgment, we need not consider the issue because we hold that there was no interception.

We largely agree with the district court's analysis. As we explain below, it is undisputed that the only access Embarq had to the data extracted by NebuAd was in its capacity as an ISP, not because of any special relationship with NebuAd or the technology test. We need not decide where to draw the line between *access* to data and *acquisition* of data, because Embarq's access was in the ordinary course of its core business as an ISP transmitting data over its equipment. Even if such access might be deemed an acquisition, Embarq did not engage in an "interception" under the ECPA because of the ordinary-course-of-business exclusion from the definition of *interception*. *See* 18 U.S.C. §§ 2510(4) (defining *intercept* as the "acquisition of the contents of any . . . electronic . . . communication" by use of an "electronic, mechanical or other device"); 2510(5)(a)(ii) (excluding from the definition of "electronic, mechanical or other device" any equipment "used by a provider of wire or electronic communication services in the ordinary course of its business").

The relevant facts were established in the summary-judgment proceedings. In its motion for summary judgment, Embarq asserted that it was undisputed that "Embarq did not have access to the data collected by the NebuAd System." Aplt. App., Vol. II at 280. To support this contention, Embarq cited several statements in the record: (1) The

Kirches' expert, Alissa Cooper, was asked at her deposition, "Did the ISP obtain access to raw data from NebuAd in any way other than an ISP ordinarily has the raw data, which is to say that it flows through the ISP's network?" She responded, "I don't think so." *Id.* at 450. (2) The Kirches' expert Andrew Case said at his deposition that Embarq did not have access to "the raw data collected by NebuAd." *Id.* at 468. And (3) Embarq's expert Dr. Ellis Horowitz stated in his report that Embarq "neither purchased, leased, nor paid for the UTA, which at all times was owned and controlled by NebuAd. The device was placed on [Embarq's] network in such a way that all Internet traffic streaming through [Embarq's] network would also pass through the UTA." *Id.* at 376.

In a summary-judgment proceeding a party's assertion of undisputed facts is ordinarily credited by the court unless properly disputed by the opposing party. *See* Fed. R. Civ. P. 56(e) ("If a party . . . fails to properly address another party's assertion of fact . . . , the court may . . . (2) consider the fact undisputed for purposes of the motion . . . ."); *Nahno-Lopez v. Houser*, 625 F.3d 1279, 1283–84 (10th Cir. 2010) (opponent's response to summary-judgment motion must raise a factual dispute that is material to the motion); D. Kan. Rule 56.1(b)(1) (memorandum in opposition to a motion for summary judgment must "contai[n] a concise statement of material facts as to which the party contends a genuine issue exists[,] . . . refer[ring] with particularity to those portions of the record upon which the opposing party relies"); *id.* at 56.1(e) ("All

responses must fairly meet the substance of the matter asserted.").

The Kirches' response did not adequately dispute Embarq's assertion. It stated only: "Undisputed that Embarq did not have access to the data after it was collected by NebuAd servers. However, Embarq did have access to the raw data when it flowed through their network." Aplt. App., Vol. I at 64. In support, the Kirches cited only the following exchange in the Cooper deposition:

> Q: Did the ISP get any of the raw data that NebuAd may have looked at?
>
> A: I don't know.
>
> Q: Do you have any reason to think that it did?
>
> A: Well, the raw data is just flowing over its network, so it has access to the raw data.

Id., Vol. II at 450. Thus, the Kirches' only qualification to their acceptance of the alleged undisputed fact was that Embarq had access to users' data that it necessarily had as an ISP.

In other words, the undisputed facts establish that NebuAd's use of the UTA gave Embarq access to no more of its users' electronic communications than it had in the ordinary course of its business as an ISP. Embarq is therefore protected from liability by the statutory exemption for activities conducted

in the ordinary course of a service provider's business. *See* 18 U.S.C. § 2510(5)(a)(ii).

Supporting our conclusion is the Second Circuit's decision in *Hall v. Earthlink Network, Inc.*, 396 F.3d 500 (2005). Hall used Earthlink as his ISP. *See id.* at 502. Later his account was closed, but several hundred emails were sent to his Earthlink address after the closure and stored in Earthlink servers. *See id.* Hall sued, claiming that Earthlink had unlawfully intercepted this mail "by intentionally continuing to receive messages sent [to his closed email address] after the termination of his account." *Id.* The court held that Earthlink was not liable. It explained that "Earthlink acquired the contents of electronic communications but did so in the ordinary course of business," so there was no "interception" within the statutory definition. *Id.* at 504–05.[3]

The Kirches seek to escape the import of the undisputed facts by asserting that Embarq had "control and possession of the UTA" during the time it was installed on Embarq's network. Aplt. Br. at

---

[3] The court said that "[i]f ISPs were not covered by the ordinary course of business exception, ISPs would constantly be intercepting communications under ECPA because their basic services involve the 'acquisition of the contents' of electronic communication." *Hall*, 396 F.3d at 505. As we stated above, however, we need not decide where to draw the line between access and acquisition of data.

The *Hall* court's statement was made during its explanation of its holding that the course-of-business exception applies not only to telephone or telegraph equipment used by an ISP, but also to any other equipment used by an ISP. *See id.* at 504–05. That issue has not been raised in this appeal, so we need not address it.

16. But control and possession of the device is not the test. If such control or possession gave Embarq access to the contents of communications beyond what it acquired in the ordinary course of business, the Kirches needed to provide evidence of such access in response to Embarq's assertion of undisputed fact.

The Kirches also point to two letters to Congress submitted by Embarq in July 2008, describing the NebuAd technology test and Embarq's role in the test. These letters asserted that the test had not captured users' confidential information and stated that the test was conducted in accordance with Embarq's privacy policies, industry standards, and agency guidance. The Kirches rely on portions of the letters (1) stating that "Embarq conducted a brief, small-scale test of customer preference advertising utilizing a new technology," Aplt. App., Vol. I at 111; (2) referring to "our consumer preference marketing test," *id.* at 115; and (3) stating that "we have no plans for more tests or for general deployment of this technology," *id.* at 118. The Kirches characterize these statements as a "clear party admission" that it was Embarq, not NebuAd, that used the UTA and thereby intercepted its users' communications. Aplt. Br. at 17. We disagree. The Kirches read too much into the letters. The letters did not attempt to delineate the division of responsibility between Embarq and NebuAd. Indeed, they never mention NebuAd. The letters were in response to Congressional inquiries about the type of advertising examined in the technology test. The concern was about the nature of the technology and the conduct of the test. There was no

need or reason for Embarq's letters to be lengthened by a description of who was responsible for what. The letters are consistent with Embarq's account of the technology test in the district court and do not contradict the undisputed fact that Embarq's only access to data collected by the UTA was in the ordinary course of its business as an ISP.

V. CONCLUSION

We AFFIRM the judgment of the district court.

[ENTERED: December 28, 2012]

UNITED STATES COURT OF APPEALS

FOR THE TENTH CIRCUIT

KATHLEEN KIRCH; TERRY KIRCH, indvidually and on behalf of themselves and all others smililary situated,

Plaintiffs - Appellants,

v.

EMBARQ MANAGEMENT CO., a Delaware corporation; UNITED TELEPHONE COMPANY OF EASTERN KANSAS, a Delaware corporation,

Defendants - Appellees,

and

DOE DEFENDANTS 1-5,

Defendants.

No. 11-3275
(D.C. No. 2:10-CV-02047-JAR-GLR)

JUDGMENT

Before **MURPHY**, **HARTZ**, and **HOLMES**, Circuit Judges.

This case originated in the District of Kansas and was argued by counsel.

The judgment of that court is affirmed.

Entered for the Court

/s/ Elisabeth A. Shumaker
ELISABETH A. SHUMAKER, Clerk

[ENTERED: August 19, 2011]

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: 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]

---

[1] Doc. 60, Ex. 1.

[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

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 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

---

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.).

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

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

"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

---

[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)).

simply rest upon its pleadings to satisfy its burden.[11] Rather, the nonmoving party must "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

---

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

[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).

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 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.

---

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

[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).

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 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

---

[19] Doc. 60, Ex. 6.

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

> 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 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

---

[21] *Id.*

[22] *Id.*

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 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,

---

[23] Doc. 60 at Ex. 10.

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 "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 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

---

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

[25] 18 U.S.C. § 2510(4).

[26] 18 U.S.C. § 2510(8).

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 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

---

[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.

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

---

[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).

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 "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.

---

[31] 2001 WL 34517252.

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

[33] *Id*. at *1.

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

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 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

---

[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.").

[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.

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 were then offered the opportunity to opt out by clicking on a hypertext link. Moreover, a preexisting 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 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

---

[39] *Id*. at *2.

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

[41] *Id*.

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]

---

[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).

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

ELECTRONIC COMMUNICATIONS PRIVACY ACT

Title 18 U.S.C. § 2510 provides, in relevant part:

> As used in this chapter—
>
> […]
>
> (4) "intercept" means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.
>
> (5) "electronic, mechanical, or other device" means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—
>
> > (a) any telephone or telegraph instrument, equipment or facility, or any component thereof,
> >
> > > (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used

in the ordinary course of its business; or

(ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties;

[…]

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

[…]

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

(13) "user" means any person or entity who—

(A) uses an electronic communication service; and

(B) is duly authorized by the provider of such service to engage in such use;

(14) "electronic communications system" means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;

(15) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications;

Title 18 U.S.C. § 2511 provides, in relevant part:

> (1) Except as otherwise specifically provided in this chapter any person who –
>
> > (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;
> >
> > […]
> >
> > (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection;
> >
> > (d) intentionally uses, or endeavors to use, the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection; or
> >
> > […]

shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).

(2)(a)(i) It shall not be unlawful under this chapter for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire or electronic communication, to intercept, disclose, or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service, except that a provider of wire communication service to the public shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

(ii) Notwithstanding any other law, providers of wire or electronic communication service, their officers, employees, and agents, landlords, custodians, or other persons, are authorized to provide information, facilities, or technical assistance to persons authorized by law to intercept wire, oral, or electronic communications or to conduct electronic surveillance, as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, if such provider, its officers, employees, or agents, landlord, custodian, or other specified person, has been provided with--

> (A) a court order directing such assistance or a court order pursuant to section 704 of the Foreign Intelligence Surveillance Act of 1978 signed by the authorizing judge, or
>
> (B) a certification in writing by a person specified in section 2518(7) of this title or the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required,

setting forth the period of time during which the provision of the information, facilities, or technical assistance is authorized and specifying the information, facilities, or technical assistance required. No provider of wire or electronic communication service, officer, employee, or agent thereof, or landlord, custodian, or other specified person shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter, except as may otherwise be required by legal process and then only after prior notification to the Attorney General or to the principal prosecuting attorney of a State or any political subdivision of a State, as may be appropriate. Any such disclosure, shall render such person liable for the civil damages provided for in section 2520. No cause of

action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter.

[…]

(3)(a) Except as provided in paragraph (b) of this subsection, a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one to such person or entity, or an agent thereof) while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient.

(b) A person or entity providing electronic communication service to the public may divulge the contents of any such communication--

(i) as otherwise authorized in section 2511(2)(a) or 2517 of this title;

(ii) with the lawful consent of the originator or any addressee or intended recipient of such communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward such communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

[…]

Title 18 U.S.C. § 2520(a) provides, in relevant part:

> Except as provided in section 2511(2)(a)(ii), 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, other than the United States, which engaged in that violation such relief as may be appropriate.