FILED
United States Court of Appeals
Tenth Circuit

December 28, 2012

Elisabeth A. Shumaker
Clerk of Court

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.

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

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 civil-liability 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*

[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.

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) 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

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

> 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]

[3] The court said that "[i]f ISPs were not covered by the ordinary course of (continued...)

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 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](...continued)
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.

(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.