IN THE DISTRICT COURT OF THE UNITED STATES FOR THE MIDDLE DISTRICT OF ALABAMA, EASTERN DIVISION

MICHAEL BRUCE, an individual; and TANYA BRUCE, an individual,	)	
Plaintiffs,	)	
v.	)	**CIVIL ACTION NO. 3:13cv221-MHT (WO)**
JOSHUA McDONALD, an individual; et al.,	)	
Defendants.	)	

OPINION

Plaintiffs Michael and Tanya Bruce filed this lawsuit against defendants Joshua McDonald, James R. McKoon, Jr., and Melissa B. Thomas and her law firm, asserting interception, disclosure, and use of electronic communications in violation of the Wiretap Act of 1968, as amended, 18 U.S.C. § 2511. Jurisdiction is proper under 28 U.S.C. § 1331 (federal question). Currently pending before the court are the parties' various cross-motions for summary judgment. Because the court concludes that there has been no "interception" as

required under § 2511, summary judgment will be entered in favor of the defendants and against the plaintiffs.

I. SUMMARY-JUDGMENT STANDARD

"A party may move for summary judgment, identifying each claim or defense--or the part of each claim or defense--on which summary judgment is sought. The court shall grant summary judgment if the movant shows that 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). The court must view the admissible evidence in the light most favorable to the non-moving party and draw all reasonable inferences in favor of that party. Matsushita Elec. Indus. Co. Ltd. v. Zenith Radio Corp., 475 U.S. 574, 587 (1986).

II. BACKGROUND

This case, like so many civil suits alleging the unauthorized access of personal electronic information,

arises out of a contentions divorce and child-custody dispute. Tanya Bruce and Joshua McDonald used to be married.[1] They were separated in 2009 and divorced in 2010. At that time, they were awarded evenly split custody of their only child. Mrs. Bruce began dating and later married Michael Bruce.

At issue in this case is Mr. McDonald's access to three electronic accounts: first, Mrs. Bruce's individual email account hosted by Yahoo.com; second, the joint email account the Bruces shared; and third, a joint account the Bruces shared on a website called "Adult Friend Finder" (or "AFF").

Mr. McDonald first gained access to Mrs. Bruce's individual Yahoo account. There is some dispute about how, exactly, Mr. McDonald did so. The record contains evidence that Mrs. Bruce may have logged into her individual account on Mr. McDonald's computer and failed

---

1. Mrs. Bruce's prior married name was Tanya McDonald. She initially filed this lawsuit under that name, but with the parties' consent the docket was amended to reflect her new married name.

to log out; or that Mr. McDonald may have observed her enter her password for that account; or that Mrs. Bruce may have given Mr. McDonald the login information for that account on one occasion for the limited purpose of printing tickets for a joint activity with their child.[2] In any event, Mr. McDonald has acknowledged that he had no permission to read the emails in Mrs. Bruce's individual account, with the possible exception of printing the tickets. Dep. of Joshua McDonald (Doc. No. 45-12) at 49.

Mr. McDonald later also gained access to the joint Yahoo account and the AFF account. He located an email from Mr. Bruce to Mrs. Bruce, in her individual account, which contained their joint AFF login information. He used that information to access private messages in the AFF system (which functions in a similar way as email, but only among AFF users). Id. at 71-72, 75-77. The

---

2. There is no allegation that Mr. McDonald used a key-logging program or any similar means of gaining the login information. A professional examination of the Bruces' computers found no improper software.

record does not clearly indicate how Mr. McDonald gained access to the joint Yahoo account. However, that he accessed all three accounts is clear because he printed out hundreds of pages of emails and documents from the three accounts. See, e.g., Emails (Doc. No. 45-18); id. (Doc. No. 45-19) at 10-12; AFF Documents (Doc. No. 45-21) at 92; id. (Doc. No. 45-22) at 59-74.

The documents Mr. McDonald obtained and printed relate to mostly the Bruces', within their committed relationship, engaging in sexual conduct with other individuals, commonly referred to as "swinging." The documents and photos are very sexually explicit. A packet of the documents was anonymously sent to the Alabama Board of Pharmacy and allegedly played a role in adverse action regarding Mrs. Bruce's pharmacist's license. See Dep. of Tanya Bruce (Doc. No. 45-5) at 119-20. The Bruces believe that Mr. McDonald sent the packet and also that information about their sexual lifestyle was disclosed to other individuals, including Mr.

McDonald's co-workers and current wife; the defendants dispute this. It is, however, undisputed that Mr. McDonald provided copies of all the documents to his attorney in the child-custody case, Melissa B. Thomas, who is the principal of the Thomas law firm. Ms. Thomas, in turn, engaged another attorney, James R. McKoon, Jr., as co-counsel.

The attorneys concluded that they could lawfully use that evidence in the custody case. Ms. Thomas produced the documents to Mrs. Bruce's counsel in discovery in the state matter. The parties obtained a protective order from the state-court judge governing the use of the documents. Ms. Thomas marked and referred to some of the documents as exhibits at Mrs. Bruce's deposition in that case and alluded to the information contained in them in argument to the state judge; she may have also disclosed them to the mediator during the course of mediation. The parties reached a new agreement as to custody. This agreement resulted in increased custody time for Mr.

McDonald, specific limitations on Mrs. Bruce's sexual activities, and other terms benefitting Mr. McDonald.

The Bruces then brought this lawsuit, alleging that Mr. McDonald illegally intercepted their electronic communications and that Mr. McDonald, Attorney McKoon, and Attorney Thomas and her law firm illegally disclosed and used those communications. All parties seek summary judgment on all the claims.

III. DISCUSSION

In 1986, Congress amended the Wiretap Act of 1968 to protect electronic communications as well as traditional wire communications (such as telephone calls).[3] As amended by Title I of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986), the Wiretap Act now imposes criminal and civil liability on any person who "intentionally intercepts ... any ... electronic communication." 18 U.S.C.

3. The Act is formally known as Title III of the Omnibus Crime Control and Safe Streets Act of 1968.

§ 2511(1)(a). The Wiretap Act also imposes liability on any person who "intentionally discloses," 18 U.S.C. § 2511(1)(c), or "intentionally uses," 18 U.S.C. § 2511(1)(d), the contents of an electronic communication "knowing or having reason to know" the communication was intercepted in violation the Wiretap Act. Thus, "interception" is a necessary element for each type of violation.

The Bruces have alleged violations of all three sections. In essence, they argue that Mr. McDonald "intercepted" their personal emails and AFF messages by logging into the three accounts without their authorization. The defendants all argue that there has been no interception within the meaning of the Wiretap Act. The court agrees with the defendants.

The Wiretap Act defines "intercept" broadly, 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." 18 U.S.C.

§ 2510(4). However, the Eleventh Circuit Court of Appeals has adopted a "narrow reading" of "interception" in the context of electronic communications. United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003). In Steiger, the appellate court concluded that to constitute an interception, the electronic communications must have been acquired "contemporaneously with their transmission." Id. at 1049; see also id. at 1048-49 ("we hold that a contemporaneous interception--i.e., an acquisition during 'flight'--is required to implicate the Wiretap Act with respect to electronic communications").

In Steiger, a criminal case, the court rejected a motion to suppress certain documents and information a hacker had obtained without permission from the defendant's computer and subsequently had provided to the police.[4] Applying the "contemporaneous" test to those

4. The Wiretap Act is implicated in a variety of cases: civil litigation for damages under the Act, such as this case; criminal charges for violations of the Act; and motions to suppress evidence obtained by the government in other kinds of criminal cases pursuant to (continued...)

facts, the court found no interception:

> "In this case, there is nothing to suggest that any of the information provided [by the hacker] was obtained through contemporaneous acquisition of electronic communications while in flight. Rather, the evidence shows that the source used a Trojan Horse virus that enabled him to access and download information stored on Steiger's personal computer. This conduct, while possibly tortious, does not constitute an interception of electronic communications in violation of the Wiretap Act."

Id. at 1050.

The Bruces argue that Steiger is factually distinguishable from the instant case. In this case, they note, Mr. McDonald was not accessing files stored on the Bruces' computers, but was repeatedly accessing their web-based email and AFF accounts over an extended period of time. The Bruces point to three out-of-circuit cases, along with dicta in Steiger, to support their view that this conduct is enough to establish "interception."

4(...continued)
the Act's suppression provision, 18 U.S.C. § 2515.

The strongest support for the Bruces' position comes from United States v. Szymuszkiewicz, 622 F.3d 701, 706 (7th Cir. 2010). In Szymuszkiewicz, the Seventh Circuit Court of Appeals upheld the defendant's conviction under the "interception" provision of the Wiretap Act for setting up a process whereby the defendant's supervisor's emails were automatically forwarded to the defendant's email account for an extended period of time. The defendant had argued that there was no "interception" because the forwarding happened only after each email arrived in the supervisor's inbox. The court found, first, that the jury could have concluded, as a factual matter, that this was not so; indeed, the evidence indicated that the email server, rather than the supervisor's computer, duplicated each message. But the court went on to find that even if the supervisor's computer did copy each message, that would not change the outcome of the case:

> **"Either the server in Kansas City or [the supervisor's] computer made copies**

> **of the messages for Szymuszkiewicz within a second of each message's arrival and assembly; if both Szymuszkiewicz and [the supervisor] were sitting at their computers at the same time, they would have received each message with no more than an eyeblink in between. That's contemporaneous by any standard."**

Id. at 706.

The Bruces argue that, because Mr. McDonald had access to the email accounts on a continuous basis, he could have viewed any given message sent or received by those accounts as soon as it hit the inbox (or the sent-mail folder). Thus, hypothetically, "if both [Mr. McDonald] and [Mrs. Bruce] were sitting at their computers at the same time, they would have received each message with no more than an eyeblink in between." Id. But this argument ignores the critical distinction: in Szymuszkiewicz, the evidence showed that each email actually was forwarded to the defendant's account contemporaneously with its transmission. In this case, the Bruces argue that Mr. McDonald had access to the

accounts and could have accessed some particular email contemporaneously with transmission. But there is no evidence in the record to indicate that he ever actually did so. Cf. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 557 (S.D.N.Y. 2008) (Katz, J.) ("[T]here is no evidence that the ... e-mails were intercepted at the same time that they were delivered. Rather, the evidence indicates that Brenner periodically accessed Fell's e-mail accounts and printed e-mails after they had been delivered.").

The Bruces also point to dicta in Steiger, which in turn was a quotation from a law review article, suggesting that "'a duplicate of all of an employee's messages [being] automatically sent to the employee's boss'" would constitute interception. Steiger, 318 F.3d at 1050 (quoting Jarrod J. White, E–Mail @Work.com: Employer Monitoring of Employee E–Mail, 48 Ala. L. Rev. 1079, 1083 (1997)) (alteration in original). Unfortunately for the Bruces, the full quotation points

to exactly the distinction between actual forwarding and mere access described above:

> **"'[T]here is only a narrow window during which an E-mail interception may occur--the seconds or mili-seconds before which a newly composed message is saved to any temporary location following a send command. Therefore, unless some type of automatic routing software is used (for example, a duplicate of all of an employee's messages are automatically sent to the employee's boss), interception of E-mail within the prohibition of [the Wiretap Act] is virtually impossible.'"**

Id. (alternation in original, emphasis added). In other words, even assuming that the Eleventh Circuit really intended to endorse the particular scenario described in the law review article as an instance of interception, that scenario explicitly contemplated actual automatic forwarding, such as was the case in Szymuszkiewicz, not mere access, as is the case here.

The other cases to which the Bruces cite are even less persuasive. In re Pharmatrak, Inc., 329 F.3d 9, 22 (1st Cir. 2003), involved code implanted on the computers

of visitors to pharmacy websites that "automatically duplicated" information and sent it to the defendant, a third-party marketing firm, as well as the pharmacies. The court found interception, in part by analogy to the email forwarding example in Steiger. Because the duplication in Pharmatrak, like the forwarding rule in Szymuszkiewicz, was automatically contemporaneous, it is likewise distinguishable from this case.

Finally, the Bruces point to a footnote in Hall v. EarthLink Network, Inc., 396 F.3d 500, 503 n.1 (2d Cir. 2005). In that case, the plaintiff had sued his internet service provider under the Wiretap Act for having continued to receive emails sent to his email address after the provider had cancelled his account. The court held that the provider was exempt from liability under a statutory exception for conduct by such a provider in the ordinary course of its business; this exception is obviously not at issue in the instant case. In the cited footnote, the court in dicta rejected a separate argument

made by the provider that an interception could occur only while messages were in transit. The court noted that this argument failed because the allegation in that case was of continued receipt of messages rather than acquisition of stored messages. This court is admittedly somewhat perplexed by the phrasing of this footnote, but in any event the difference between that case and this one is clear: for each message the provider continued to receive, it actually received that message contemporaneously to its transmission. Thus, even if the Hall court had found an interception under those circumstances, which it did not, that case would not imply that an interception exists here.

On the contrary, in a consistent string of cases courts have held time and again that unauthorized access to an email account, standing alone, does not constitute interception. See Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003) (no interception where company searched employee's email without authorization);

Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 639 (E.D. Va. 2009) (Ellis, J.) (allegations that husband accessed wife's email account without authorization insufficient to state claim of interception); Pure Power Boot Camp, 587 F. Supp. 2d at 558 (no interception where ex-employer accessed three of ex-employee's personal, web-based email accounts without authorization); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 981 (M.D. Tenn. 2008) (Trauger, J.) (continued access of work email system by ex-employee not interception); Bailey v. Bailey, 2008 WL 324156 (E.D. Mich. 2008) (Cox, J.) (no interception where husband accessed wife's web-based email accounts without authorization).

Indeed, one of those cases, Bailey, echos this case in nearly every respect. The defendant in that case had obtained his wife's login information without any authorization, through the use of a device that logs every keystroke on a computer. He then monitored her

web-based email addresses for months, eventually sharing information he obtained from her accounts with his attorney in child-custody proceedings. The attorney used the information during the course of those proceedings. The plaintiff lost custody and thereafter sued both her ex-husband and his attorney under the Wiretap Act. Despite continuous access to the accounts, the Bailey court's conclusion was clear: "Defendant Bailey did not obtain the emails or messages contemporaneously with their transmission, and thus, the Wiretap Act does not apply." Bailey, 2008 WL 324156 at * 5.

The court finds this long and consistent string of cases entirely persuasive. The Eleventh Circuit has adopted a construction of "interception" requiring that electronic communications must be acquired contemporaneously with their transmission. Logging into and acquiring messages from another individual's email account does not necessarily happen contemporaneously with their transmission. Rather, it almost always

happens after the transmission of those messages, whether by minutes or by days or by years. Thus the cases cited above which found no interception in the case of email access are entirely consistent with the cases the Bruces cite finding interception in case of automatic duplication. For in the latter cases, but not necessarily in the former, there was evidence of actual acquisition contemporaneous with transmission.

This is not to say that mere access, without some duplication device, could never amount to interception. If the Bruces could establish that Mr. McDonald had actually acquired even one message contemporaneously with its transmission, they might be able to show interception. That question is not before the court because there is simply no such evidence in this case.[5]

---

5. Nor is there any evidence that Mr. McDonald acquired any particular message before Mrs. Bruce had read that same message. Thus the court need not reach the question of whether that conduct, if proven would constitute interception. Cf. Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994) (finding that seizure of still-unread messages on

(continued...)

"Rather, the evidence indicates that [Mr. McDonald] periodically accessed [the] accounts and printed e-mails [and other documents] after they had been delivered." Pure Power Boot Camp, 587 F. Supp. 2d at 557.[6] That is insufficient to establish an interception.

The defendants have raised a number of other arguments against liability in this case.[7] However, because the court has determined that there was no

---

5(...continued)
electronic bulletin board was not an interception).

6. The court also need not reach the question of whether Mr. McDonald's conduct was "tortious," Steiger, 318 F.3d at 1050, or violated Title II of the Electronic Communications Privacy Act, also known as the Stored Communications Act. See 18 U.S.C. § 2701. The Bruces have asserted no claims apart from those under the Wiretap Act.

7. Specifically, some or all of the defendants raise the following arguments, among others: the Wiretap Act's statute of limitations, 18 U.S.C. § 2520(e); that this case is foreclosed by the settlement agreement in the custody matter; and that any use in court was sanctioned by the state court's protective order. The parties agree that an additional argument, based on Rooker/Feldman doctrine, is now moot.

interception within the meaning of the Wiretap Act, it need not reach these other issues.

****

Accordingly, for the above reasons, summary judgment will be entered in favor of Mr. McDonald, Attorney McKoon, and Attorney Thomas and her law firm and against the Bruces. An appropriate judgment will be entered.

DONE, this the 10th day of March, 2014.

/s/ Myron H. Thompson
UNITED STATES DISTRICT JUDGE