UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF ILLINOIS
PEORIA DIVISION

JAMISON J. SHEFTS,)
)
Plaintiff,)
)
v.) Case No. 10-cv-1104
)
JOHN PETRAKIS, KEVIN MORGAN,)
and HEIDI HUFFMAN,)
)
Defendants.)
)

ORDER & OPINION

This matter is before the Court on Plaintiff's Motion for Summary Judgment on a Major Issue (Intercept) (Doc. 231) and Defendants' Motion for Summary Judgment on Count I of Plaintiff's Complaint (Doc. 229). Defendants have also filed an Objection to Plaintiff's use of the Sixth Supplemental Affidavit of James Feehan in support of his instant Motion for Summary Judgment. (Doc. 245). For the reasons stated below, Plaintiff's Motion for Summary Judgment on a Major Issue (Intercept) is granted in part and denied in part and Defendants' Motion for Summary Judgment on Count I of Plaintiff's Complaint is granted in part and denied in part.

As the general background of this case has been explained multiple times by the parties and the Court over the course of this litigation, it is unnecessary to review it in detail. In his Amended Complaint, Plaintiff raises four counts against Defendants, all related to their monitoring of his electronic communications; the instant Motions concern only Count I, which alleges that Defendants violated the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2511, by intercepting

Plaintiff's emails on his Access2Go-provided email account, his emails on his personal Yahoo! email account, and his text messages on his Blackberry device. In his Motion for Summary Judgment, Plaintiff asks the Court to make a definitive ruling on the issue of whether Defendants "intercepted" these communications within the meaning of the ECPA. In their Motion, Defendants also request a ruling in their favor on Count I, as they argue that they did not, as a matter of law, "intercept" Plaintiff's communications within the meaning of the ECPA. Both Motions therefore turn on the issue of whether an "interception" occurred. Though they are not technically "cross-motions" for summary judgment, the Court considers them concurrently because they raise almost identical factual and legal issues.

The Court has had occasion to consider the issue of "interception" under Count I of this suit in past orders, but the procedural posture of those orders and the evidence presented was such that the Court could not make a definitive finding as to whether an interception occurred. Instead, in denying Plaintiff's first Motion for Summary Judgment, which related only to Plaintiff's text messages, the Court declined to make such a ruling, both because there were other bases for the denial, and because there appeared to be a genuine issue of material fact on the question of when the messages in question were "logged." (Doc. 141 at 3). In their first Motion for Summary Judgment, Defendants assumed for the sake of the Motion that they had "intercepted" the communications within the meaning of the ECPA, and relied instead on issues of consent to monitoring; the Court denied that portion of the Motion because genuine issues of materal fact on the question of consent precluded summary judgment.[1] Now, whether an interception occurred is the issue in contention, and the Court can make a final decision.

Defendants have objected to the admission of portions of an affidavit by James Feehan submitted by Plaintiff. (Doc. 245). Having reviewed their objections, and Plaintiff's response to them, the Court agrees that it is improper for the Court to consider the legal conclusions put forth in certain paragraphs of Mr. Feehan's Sixth Supplemental Affidavit. (Doc. 244, Ex. B). None of these conclusions would have been relied upon by the Court, even if Defendants had not objected, as it is the Court's role to interpret the law in this case. Moreover, the Court notes that other affidavits presented by the parties' experts also contain legal conclusions, upon which the Court does not rely.[2] The Court will not waste time listing each improper legal conclusion by a technical expert; as noted below, the Court specifically lists each fact that it relies on in its Orders, and has not in this or in any other Order allowed an affidavit to usurp its interpretive function. The Court finds the experts' affidavits to be helpful in working through the factual and highly technical details of this case, but does not defer to them on legal issues.

[1] As for Defendant Morgan, the parties appear to agree that he did not personally "intercept" the messages; Plaintiff's claims against him are based on his alleged direction or approval of Petrakis' and Huffman's actions. Morgan's arguments against this theory of liability are raised in another Motion for Summary Judgment, which the Court rules on contemporaneously, in a separate Order.

[2] For example, in his affidavit submitted by Defendants, Jason Gossett opines that text messages are not "intercepted." (Doc. 60, Ex. C at ¶ 23-24, 28). The legal definition of the term "intercept" is a key issue in this case, and the Court does not find that the parties' technical experts are empowered to give binding opinions on the subject.

LEGAL STANDARD

"On cross-motions for summary judgment, the same standard of review in Federal Rule of Civil Procedure 56 applies to each movant." *Continental Cas. Co. v. Nw. Nat. Ins. Co.*, 427 F.3d 1038, 1041 (7th Cir.2005). The United States Court of Appeals for the Seventh Circuit has explained that courts "look to the burden of proof that each party would bear on an issue of trial; we then require that party to go beyond the pleadings and affirmatively establish a genuine issue of material fact." *Diaz v. Prudential Ins. Co. of America*, 499 F.3d 540, 643 (7th Cir.2007) (quoting *Santaella v. Metropolitan Life Ins. Co.*, 123 F.3d 456, 461 (7th Cir.1997)).

Summary judgment should be granted where "the pleadings, the discovery and disclosure materials on file, and any affidavits show that there is no genuine issue as to any material fact and that the movant is entitled to judgment as a matter of law." FED. R. CIV. P. 56(c). In ruling on a motion for summary judgment, the Court must view the evidence on record in the light most favorable to the non-moving party. *SMS Demag Aktiengesellschaft v. Material Sciences Corp.*, 565 F.3d 365, 368 (7th Cir. 2009). All inferences drawn from the facts must be construed in favor of the non-movant; however, the Court is not required to draw every conceivable inference from the record. *Smith v. Hope School*, 560 F.3d 694, 699 (7th Cir. 2009). The Court draws only reasonable inferences. *Id.*

Once the movant has met its burden of showing the Court that there are no genuine issues of material fact, to survive summary judgment the "nonmovant must show through specific evidence that a triable issue of fact remains on issues on which he bears the burden of proof at trial." *Warsco v. Preferred Tech. Group*, 258

F.3d 557, 563 (7th Cir. 2001) (*citing Celotex Corp. v. Catrett*, 477 U.S. 317, 324 (1986)). If the evidence on record could not lead a reasonable jury to find for the non-movant, then no genuine issue of material fact exists and the movant is entitled to judgment as a matter of law. *McClendon v. Indiana Sugars, Inc.*, 108 F.3d 789, 796 (7th Cir. 1997). At the summary judgment stage, however, the court may not resolve issues of fact; disputed material facts must be left for resolution at trial. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 249-50 (1986).

UNDISPUTED MATERIAL FACTS[3]

Access2Go is a Peoria, Illinois-based telecommunications company. From January 1, 2000 to January 1, 2006, Plaintiff owned 100% of the voting stock in Access2Go and was the sole member of its Board of Directors. (Doc. 170, Ex. A ¶¶ 3-6). On January 1, 2006, Plaintiff sold shares of Access2Go to Defendants Petrakis and Morgan, as well as John Tandeski. (Doc. 152, Ex. A at ¶ 4). Plaintiff, Petrakis, and Morgan each owned 30% of the stock, and Tandeski owned 10%. (Doc. 152, Ex. A at ¶ 4). These men constituted the four-member Board of Directors for Access2Go, with each having one vote. (Doc. 152, Ex. A at ¶¶ 4-5; Doc. 170, Ex. A at ¶ 8).

Plaintiff sent and received emails relevant to this suit via the email account provided to him by Access2Go, as well as via a personal web-based Yahoo email account, using the computer assigned to him at Access2Go, and sent and received

[3] As there are two separate Motions for Summary Judgment, there are separate statements of material facts. The Court draws from both, and notes the occasions where the parties raise a genuine dispute as to a material fact. Facts that are immaterial to the issues raised in these motions are not included unless necessary for clarity.

text messages using a Blackberry device.[4] The Access2Go system also included a "BES" server, which enabled Blackberry devices, including Plaintiff's, to be connected to and synchronized with the Access2Go communications system.[5] (Doc. 152, Ex. A at ¶¶ 2).

[4] Defendants are quite insistent that the Blackberry device in question did not belong to Plaintiff, but was actually paid for by Access2Go. The Court finds that payment for and title to the Blackberry is not dispositive of the question of whether the ECPA was violated. There is no rule that communications are automatically exempt from ECPA protection merely because they were made using equipment belonging to the employer. (*See* Doc. 209 at 12-17). Moreover, the Court has already ruled that Access2Go's attempted reimbursement of Plaintiff's Blackberry expenses during this litigation would not be sufficient to show that the Blackberry was not "Plaintiff's." (Doc. 209 at 5 fn 4).

[5] As described in the previous Order on Defendants' first Motion for Summary Judgment, Access2Go's Board of Directors, on June 18, 2008, appointed Petrakis the "Board liaison for security and employee issues per the new employee manual." (Doc. 60, Ex. 1 at 11). On July 2, 2008, the Board of Directors ratified the Employee Manual. (Doc. 170, Ex. A at ¶ 40). As part of the "Theft and Fraudulent Activities Policy," the Employee Manual provides that "[t]he Board of Directors through John Petrakis, who will act as employee liaison to the board, is responsible for the establishment of an adequate system of internal control that is designed to prevent and detect errors or irregularities that may lead to fraudulent activities, and designed to safeguard company resources." (Doc. 170, Ex. 1 of Ex. B ("Employee Manual") at 21). Defendants now also put on evidence that at the June 18, 2008 Board meeting the Board

> discussed at length the expectation that [he] would use [his] authority as the Board's "liaison for security" to review Access2Go's electronic communications system, including the email server and the BES server, and direct the installation of the SpectorPro software as a means of detecting errors or irregularities that may lead to fraudulent activities and safeguarding company resources.

(Doc. 238, Ex. C. at ¶ 5). Plaintiff denies this statement of fact, but cites no evidence to show that this discussion did not take place. (Doc. 244 at 5, ¶ 19).

These actions are a key part of Defendants' arguments that their actions fall within the ECPA's "ordinary course of business" exemption. As discussed further below, the Court rejects the "ordinary course of business" argument raised here, and so finds these facts to be immaterial to the present Motions.

The Court notes that this new evidence of the Board's June 18, 2008 discussion of SpectorPro may significantly undermine Plaintiff's claim to a lack of knowledge that his communications were being intercepted, and may support an

I. Access2Go email and use of "dummy account"

The Access2Go email system operated by sending a "pointer" or "link" to a user's message to the user's email inbox when a new message was received; an actual copy of the message was not delivered to the email inbox.[6] (Doc. 238, Ex. A at

argument that he impliedly consented to such interception after that date, but that issue is not before the Court at this time.

[6] The Court here accepts Defendants' version of how the email system worked, both because the Court concludes that it is the only version a reasonable jury could accept, and because the distinction is immaterial to the outcome of the Court's analysis. Plaintiff initially suggested, based on Mr. Patton's March 31, 2012 affidavit, that both his email account and the dummy account received copies of the messages, but Defendants provided evidence from Mr. Patton clarifying how the system worked. In his Reply brief, Plaintiff indicates that he disputes Defendants' description, which is based on Mr. Patton's April 19, 2012 affidavit, but his dispute is not supported by a citation to evidence.

Mr. Patton, in the April affidavit, explains that the two affidavits differ because the March affidavit was drafted by Plaintiff's counsel, and "were not necessarily the words I would have used to describe facts and matters contained in the affidavits." (Doc. 238, Ex. 1 at ¶ 1). In addition, Plaintiff's attorneys did not ask Mr. Patton to perform any research, and appeared to have ignored his uncertainty about whether "copies" of the messages were actually delivered to the accounts, including that statement in the affidavit. (Doc. 238, Ex. 1 at ¶¶ 4-5). Nevertheless, Mr. Patton signed the affidavit, though he did ask that a paragraph attesting to the accuracy of his prior affidavits be deleted. (Doc. 238, Ex. 1 at ¶¶ 6-7).

Mr. Patton states that after signing the March affidavit for Plaintiff, he further reviewed the manner in which the Access2Go system handles messages, and determined that the account contained in the text above is the most accurate statement of how it worked. (Doc. 238, Ex. 1 at ¶¶ 1-2, 5). It appears that, if asked to testify at trial, Mr. Patton would now testify as to the facts contained in the April affidavit, and would repudiate his prior testimony contained in the March affidavit. As the Court must now determine whether the evidence that would be presented at trial is sufficient for a reasonable jury, the Court must rely on the evidence that would be presented at trial, which appears to be summarized in Mr. Patton's most recent attestation. Plaintiff has presented no evidence outside of Mr. Patton's testimony that would rebut his current account of the email system's operation. Though Mr. Patton's testimony would likely be impeached with his prior inconsistent affidavits, no reasonable jury could find that his March affidavit, based on no research and drafted by Plaintiffs' attorneys, was more accurate than his second affidavit, which was based on research.

¶¶ 10-12). On March 24, 2009, at the direction of Petrakis, Shawn Patton, of Integrated Computer Resources, a division of Klaus Radio, changed the properties of Plaintiff's Access2Go email account, jshefts@acc2go.com to automatically "forward" all messages sent to jshefts@acc2go.com to a new "dummy account." (Doc. 238, Ex. A at ¶ 3-4). Just as did all Access2Go email accounts, the dummy account received only a "pointer" to the message, which resided on the Access2Go server. (Doc. 238, Ex. A at ¶ 12).

II. Yahoo! email and use of SpectorPro

Mr. Patton installed SpectorPro, which was purchased on June 24, 2008, on Plaintiff's desktop computer at Access2Go in June 2008, at Petrakis' direction. (Doc. 232, Ex. E at ¶ 8; Doc. 232, Ex. D at ¶¶ 15, 18). In its relevant functions, SpectorPro takes a "screenshot," or image, of activities on the subject computer, and transmits those images to another computer or stores them for later review. (Doc. 244, Ex. B at ¶ 21, 24-28). When he installed SpectorPro on Plaintiff's computer, Mr. Patton set up another computer as a "monitoring station" outside the offices of Petrakis and Huffman, on which they could view the information gathered by SpectorPro from Plaintiff's computer; this information was transmitted between the two computers via Access2Go's internal network. (Doc. 232, Ex. B at ¶ 8; Doc. 238, Ex. 1 at ¶ 16; Doc. 238, Ex. A at ¶ 6; Doc. 244, Ex. B at ¶24-28).

More importantly, though, under either party's explanation of how the system worked, the Court would find that there had been an interception of Plaintiff's communications. Under Plaintiff's explanation that "copies" of the emails were delivered to both his and the "dummy" accounts, the conduct clearly falls within the ECPA, as explained below. The question is slightly more difficult under Defendants' claim that only "pointers" were sent, so the Court focuses on that argument.

A printout of an email from Plaintiff's personal Yahoo! email account was supplied by Plaintiff as an exhibit with his initial Complaint in this matter; it is of a June 30, 2008 message from Plaintiff to his attorney. (Doc. 1, Ex. A). Both Mr. Feehan, Plaintiff's expert, and Mr. Gossett, Defendants' expert, agree that this message was printed through the SpectorPro program on June 30, 2008, not from within the Yahoo! email service.[7] (Doc. 244, Ex. B at ¶¶ 34-37, 39-42; Doc. 60, Ex. C at ¶ 17).

[7] Defendants dispute this statement of fact by Plaintiff, which is supported by Mr. Feehan's affidavit, by arguing that Mr. Feehan's testimony on this point has been inconsistent. In his first analysis of the June 30, 2008 email printout, during the initial stages of this suit, Mr. Feehan stated that it appeared the printout was obtained directly from Yahoo!, by Defendants' entering Plaintiff's username and password. (Doc. 6, Ex. 2). At that point, Mr. Feehan had been able to review only Plaintiff's computer, and surmised that Defendants had used SpectorPro to obtain Plaintiff's logon information, which it is capable of doing; in support of Plaintiff's effort to have the Court order a review of the Access2Go computers in question, he stated that he would need further access in order to come to a definite conclusion. After the Court granted Plaintiff's request to seize and search certain computers at Access2Go, Mr. Feehan determined that SpectorPro had been used to obtain screenshots of Plaintiff's computer activity.

Defendants' expert, Jason Gossett, upon further review, attested that the printout had been created via SpectorPro's screenshot capability, not by logging into Yahoo!'s email system. (Doc. 60, Ex. C at ¶ 17). Mr. Feehan, having reviewed Mr. Gossett's affidavit, agreed that the printout was created as Mr. Gossett had described. (Doc. 244, Ex. B at ¶ 41). With full information, both experts therefore agree on the source of the printout.

The Court finds that this point is not truly disputed. Aside from the supposed inconsistency of Mr. Feehan's testimony, Defendants offer no evidence to support their "dispute" with Plaintiff's assertion that the printout was printed from within SpectorPro, not from within the Yahoo! site. Indeed, their own expert, Mr. Gossett, was the first to attest that SpectorPro was the source of the printout. Moreover, Mr. Feehan's claimed inconsistency is of no moment: his initial affidavit was essentially an educated guess, prior to any discovery, based on his ability to review only Plaintiff's own computer, and was directed toward obtaining further evidence, which then proved that guess to have been incorrect. It was not intended, and will not be considered, as substantive evidence in this matter.

III. Blackberry text message logging and synchronization

On December 10, 2007, Plaintiff purchased a Blackberry 8703E, with service through Verizon Wireless. (Doc. 232, Ex. A at ¶ 5). He replaced it on August 29, 2008 with a Blackberry Curve. (Doc. 232, Ex. A at ¶ 6). The Blackberries automatically retained a copy of all sent and received text messages, unless they were deleted by the user. (Doc. 241, Ex. 1 at ¶ 4). Plaintiff requested that these Blackberry devices be connected to the BES server at Access2Go. (Doc. 232, Ex. A at ¶ 5, 7). All versions of BES since version 4.1, including the BES server at Access2Go, have the optional ability to capture and store text messages from Blackberry devices if those devices are connected to the BES server, but the default setting is for this capability to be disabled. (Doc. 232, Ex. D at ¶ 26, 31). Text messages do not pass through the BES server in the course of transmission from one phone to another; they are sent directly to and from the service provider, which is Verizon in this case. (Doc. 60, Ex. C at ¶ 23).

On July 14, 2008, Mr. Patton assisted Huffman, at Petrakis' direction, in enabling the BES server's capability to capture text messages from the Blackberry device. (Doc. 232, Ex. E at ¶ 15; Doc. 238, Ex. C at ¶ 6). This caused the BES server to "synchronize" with Plaintiff's Blackberry device, and resulted in the BES server obtaining thousands of Plaintiff's text messages from the Blackberry. (Doc. 232, Ex. D at ¶ 31). When synchronization occurred, the server copied the text messages that were stored on the Blackberry device and stored those copies on the BES server. (Doc. 238, Ex. B at ¶¶ 4-6). The BES server automatically synchronized with the

Blackberry device every ten minutes, though sometimes synchronization occurred at random intervals.[8] (Doc. 238, Ex. B at ¶¶ 4-7; Doc. 244, Ex. B at ¶¶ 9-13).

DISCUSSION

There are three categories of communications that Plaintiff contends Defendants "intercepted" within the meaning of the ECPA: (1) Plaintiff's email provided by Access2Go, (2) his web-based Yahoo! email account, and (3) text messages on his Blackberry device. In their Motion for Summary Judgment, Defendants assert that their monitoring of these communications constituted only "accessions" of stored communications within the meaning of the Stored Communications Act, not "interceptions" within the meaning of the ECPA.[9] Plaintiff argues that as to each of these types of communications, Defendants utilized automatic routing software, the use of which courts have found to constitute "interceptions" within the meaning of the ECPA.

As an initial matter, the Court must reject Defendants' argument that if the Court finds that Defendants "accessed" any of Plaintiff's "stored communications," it

[8] According to Mr. Grons, both of Plaintiff's Blackberry devices used operating system 4.2.1. This operating system could not be set to synchronize with the BES server at an interval other than every 10 minutes. This was the case even if the BES server was set up to synchronize constantly. (Doc. 238, Ex. B at ¶¶ 4-8). While the BES server may have been set up to synchronize on a "zero delay," Plaintiff's actual devices did not have the capability to do this, and so such constant synchronization could not occur.

Plaintiff asserts that he disputes Mr. Grons' characterization of how the synchronization worked, but offers only Mr. Feehan's finding that occasionally the BES server synchronized messages within seconds of their transmission, and that "numerous" synchronizations occurred at less than 10 minute intervals. (Doc. 244 at 6-7; Doc. 244, Ex. B at ¶¶ 9-11). Both of these issues are discussed further below.

[9] The SCA is the subject of another Order issued concurrently with this one, on the parties' Cross-Motions for Summary Judgment on the issue of whether Access2Go "ratified" Petrakis' actions and thereby authorized them under the SCA.

must automatically grant them summary judgment as to Count I, which alleges "interception." The Court agrees that the same *conduct* cannot constitute both an "interception" and an "accession." However, Plaintiff does not argue that the same conduct underlies his claims under both statutes, but rather that Defendants engaged in "interceptions" and "accessions" as to the same communications at separate times and in different ways. Defendants present no argument against this possibility, and the Court sees no reason that the same type of communication cannot be "intercepted" and "accessed" at different times and in different ways.

The Court also rejects Defendants' implication that Plaintiff has waived the argument that the two types of email were "intercepted" merely because he has also argued that they were "accessed." Defendants cite no statement of Plaintiff's that he has waived his claim that the emails were "intercepted" in violation of the ECPA, and the fact that he has presented alternative arguments in his past Motions does not operate to waive this claim. Indeed, the facts relating to the technical operation of the alleged interceptions have only now become clear.

Moreover, the Court does not appreciate Defendants' disingenuous assertion that the Court has already "found" that the communications at issue are only "electronic communications" within the meaning of the SCA, not the ECPA. On the contrary, in the Order referred to, the Court, in discussing the SCA-directed portion of Plaintiff's first Motion for Summary Judgment, noted that "[t]he parties do not dispute that the text messages and emails monitored by Petrakis are 'electronic communications' under the SCA, [or] that Petrakis intentionally accessed them." (Doc. 84 at 24). The Court certainly did not "find" that the communications were covered only by the SCA – it only noted that, as for that Motion, the parties had chosen to dispute only the issue of whether Petrakis had authorization for his actions. In those circumstances, the Court does not reach out to decide issues that are not in dispute, but resolves only those on which the parties have presented a question.[10] The Court has not yet ruled on whether any of the "monitoring" at issue in the instant Motions constituted an "interception" or an "accession,"[11] but will now do so.

Finally, the Court must reject Defendants' "ordinary course of business" argument. There is no ECPA claim if the "device" used to intercept communications is "being used by a provider of wire or electronic communication service in the ordinary course of its business."[12] 18 U.S.C. § 2510(5)(a)(ii). Defendants claim that

[10] Defendants can hardly rely on their own admission that the communications and "access" were within the definition of the SCA in order to now defeat Plaintiff's claim under the ECPA. As he is entitled, both as an alternative theory of relief and on the argument that the same communications can be "intercepted" and "accessed" at different times, Plaintiff of course maintained that both the ECPA and the SCA had been violated. Defendants cannot choose the more favorable statute (the SCA) merely by admitting to conduct under it, and automatically defeat Plaintiff's claim under the other statute.

[11] In the Court's Order on Plaintiff's second Motion for Summary Judgment, the Court held that Petrakis "accessed" Plaintiff's Access2Go email within the meaning of the SCA by directing Mr. Patton to copy it from the Access2Go server. (Doc. 210 at 7-13). Plaintiff here makes a factually distinct allegation: that an "interception" occurred when the "rule" caused his messages to be sent contemporaneously to the "dummy account." This is distinct from an after-the-fact copy of the account from the server made by Mr. Patton, which was discussed in the Court's previous Order. As noted above, the same communications – the contents of the Access2Go email account – can be both "intercepted" and "accessed."

[12] The language of § 2510(5)(a) is somewhat confusing, as it can be read to exempt only the business use of telephone-related devices, and so not to apply to email-related devices, such as the ones at issue in this case. In *Hall v. Earthlink Network, Inc.*, however, the Second Circuit convincingly analyzed the statute's

their alleged interceptions were undertaken in order to protect the company from Plaintiff's alleged sexual harassment of employees and his alleged actions against its interest, as well as to allow the company to ensure that his Access2Go emails were properly handled during his suspension.

Before determining whether Defendants may take advantage of this exemption, it is important to point out that Access2Go did not "provide" either the Yahoo! email service or the Blackberry text message service. Access2Go only "provided" its own Access2Go email. A "provider" can only be an entity whose participation is necessary to the transmission of the communication, not an entity that merely provides a terminal through which one can access a communications service provided by another company. Access2Go did not transmit Plaintiff's Yahoo! email or text messages; those were provided by Yahoo! and Verizon, respectively.[13] The "ordinary course of business" exemption applies only to the provider of the communications service, so Defendants can rely on it only to exempt the interception of Plaintiff's Access2Go email, if appropriate.

As only the "provider" can use the device in order to fall into the exception, employees of the provider who are acting without authorization may not take advantage of it. Defendants therefore claim that they were acting on Access2Go's

legislative history to conclude that Congress intended the exemption to apply to entities that provide email services, and the Court adopts that analysis. 396 F.3d 500, 504-05 (2d Cir. 2005).

[13] Though Defendants arguably "provided" storage of Plaintiff's text messages after synchronization on the company's BES server, it did not provide the text messaging service itself, as those messages passed only through Verizon's system, not Access2Go's, when being transmitted to and from the Blackberry. The evidence in this case shows, as discussed below, that Access2Go's server only acquired the text messages from storage after their transmission to the Blackberry.

behalf in intercepting Plaintiff's communications. Defendants' arguments on this point thus mirror those made in their first Motion for Summary Judgment and in response to Plaintiff's second Motion for Summary Judgment, both of which dealt with the question of whether Defendants were acting with Access2Go's authorization when they accessed Plaintiff's communications under the SCA; in both, the Court held that genuine issues of material fact precluded the entry of summary judgment on this question. Though those arguments were specifically directed toward the SCA claim, the Court finds that the analysis of whether Defendants were acting in the "ordinary course of business" follows the same contours. There is no new evidence that would resolve the dispute of fact,[14] and so the Court will not reconsider them, despite Defendants' attempts to re-argue

[14] Defendant have now put on unrebutted evidence that at the June 18, 2008 Board meeting, at which Petrakis was appointed to his "liaison" position, the Board

> discussed at length the expectation that [he] would use [his] authority as the Board's "liaison for security" to review Access2Go's electronic communications system, including the email server and the BES server, and direct the installation of the SpectorPro software as a means of detecting errors or irregularities that may lead to fraudulent activities and safeguarding company resources.

However, this new evidence does not change the Court's prior analyses of the "liaison" position, as Petrakis was empowered only to "review" the email and BES systems, and to install SpectorPro (as noted above, the alleged Yahoo! email interception is not subject to this exemption because Access2Go did not "provide" the service). "Reviewing" a communications system does not necessarily include setting up a device to intercept all emails on that system. Moreover, the Board specifically directed Petrakis to install SpectorPro, but did not specifically direct the other alleged interception activities. Finally, the language "detecting errors or irregularities that may lead to fraudulent activities and safeguarding company resources" is similar to that used in the Employee Manual to describe the "liaison" position, and, as explained in a previous Order, can reasonably be interpreted to *exclude* the types of motivations claimed by Defendants. (Doc. 209 at 30-32).

them.[15] As the evidence now stands, there is a genuine dispute of material fact as to what the powers of Petrakis' "liaison" position included, and so the Court cannot find that his decision to set up the "dummy account" was in Access2Go's ordinary course of business.

I. Access2Go email and use of "dummy account"

According to Mr. Patton, all messages received by accounts using the Access2Go server are stored on the server, and "pointers" or "links" to the messages are sent to the recipient in order to allow him to open the message, which resides on the server. On March 24, 2009, Mr. Patton, at Defendants' direction, altered the Access2Go server in order to allow them to monitor emails received by Plaintiff's email account. In order to do this, Mr. Patton set up a "dummy" email account on the server and instituted a "rule" that directed the server to send a "pointer" to Plaintiff's messages to the dummy account at the same time it sent a "pointer" to Plaintiff's account. Both accounts thus received the messages, in that they received the "pointer" to the messages, at the same time and in the same manner.

Plaintiff argues that because these "pointers" allowed the dummy account to obtain the messages at the same time as his account, the messages were "intercepted" within the meaning of the ECPA. Defendants assert two reasons for the Court to find that this was not an interception: Plaintiff has no standing to assert a right under the ECPA with regard to these messages, because only

[15] The Court rejected as a matter of law, and still rejects, Defendants' reliance on the common law "business judgment rule," and the claim that merely because Petrakis and Morgan owned a majority of Access2Go stock they had the right to make decisions on its behalf without adherence to the procedures announced in the corporate bylaws.

incoming messages were affected, and the dummy account merely "accessed" messages stored on the Access2Go server.

Defendants' standing argument is unavailing. They claim Plaintiff can only complain if they intercepted messages from him to others, but that, since they only monitored messages from others to him, he was not injured.[16] First, covered "electronic communications," as defined in § 2520, are not explicitly limited to communications *by* the victim. Defendants cite *Healix Infusion Therapy, Inc. v. Helix Health, LLC*, a Southern District of Texas case in which the district court, relying on *Ideal Aerosmith, Inc. v. Acutronic USA, Inc.*, held that a plaintiff lacked ECPA standing if he did not himself send the intercepted emails. 747 F.Supp.2d 730, 743 (S.D. Tex. 2010) (citing No. 07–1029, 2007 WL 4394447, *4 (E.D. Pa. Dec. 13, 2007)). *Ideal Aerosmith*, in turn, relied on an Eastern District of Pennsylvania case interpreting the Pennsylvania Wiretap Act, not the ECPA. *Ideal Aerosmith*, 2007 Wl 4394447, *4 (citing *Klump v. Nazareth Area Sch. Dist.*, 425 F.Supp.2d 622, 633 (E.D. Pa. 2006)). Neither *Healix* nor *Ideal Aerosmith* discuss the fact that the authority on which they both rely was dealing with a different statute, nor do they assert that the ECPA follows the interpretation of the Pennsylvania Wiretap Act. While the relevant text of the Pennsylvania statute appears to be similar to that of

[16] Plaintiff cites to *United States v. Szymuszkiewicz*, in which the Seventh Circuit found that a defendant had violated the ECPA by intercepting only email messages sent to his supervisor; he had not intercepted messages that she sent. 622 F.3d 701, 703 (7th Cir. 2010). This case is not conclusive on this question, though, as it was a criminal prosecution, so there was no issue of whether the supervisor had standing – the government can prosecute any violation of the ECPA, while only those "whose…communications" are intercepted can sue under § 2520(a). The question here is whether the communications were Plaintiff's within the meaning of the ECPA.

the ECPA, the parties have cited no authority asserting that the ECPA is governed by how Pennsylvania interprets its statute, even if Pennsylvania chooses to follow the interpretation of the ECPA.[17] Because of this discrepancy, the Court does not find these cases to be persuasive authority.

Finally, and most importantly, § 2520(a) provides that "any person whose…electronic communication is intercepted…violation of this chapter" has a civil cause of action. The Court finds that communication is ordinarily understood to be a mutual transaction, such that communications from others intended for a person are included as part of that person's communications. A recipient of a message has as much of a privacy interest in that message as does the sender. Plaintiff has as much "standing" to complain of the alleged interception of the messages as do the senders of those messages.

Defendants also argue that because the dummy account received only "pointers" directed to messages that were actually stored on the Access2Go server, the dummy account merely "accessed" "stored communications," which is outside the scope of the ECPA. While this does somewhat distinguish the case from the interceptions at issue in *United States v. Szymuszkiewicz*, in which the Seventh Circuit held that there had been an interception where an employee had set up his

[17] Indeed, as explained by the Court in its Order on Defendants' first Motion for Summary Judgment, a Pennsylvania court, applying the Pennsylvania Wiretap Act in *Commonwealth v. Proetto*, 771 A.2d 823, 829-30 (Penn. 2001), held that emails, since they are always "recorded" in some way, can never be the subject of a Pennsylvania Wiretap Act claim because the user always impliedly consents to their recording. The ECPA is certainly not interpreted in this manner. (Doc. 209 at 14 fn. 16). It would be strange indeed for a federal statute of national applicability to be governed by how one state, with its own values and considerations, chooses to interpret its similar law.

supervisor's email account to forward a copy of all of her messages to his email account, it does not defeat Plaintiff's claim.[18] 622 F.3d 701 (7th Cir. 2010). First, in *Szymuskiewicz* itself, "every message to [the supervisor] went through [the employer's] server…, and…the server *retained the message in its own files* and dispatched two copies: one for [the supervisor] and another for Szymuszkiewicz" – just as in this case, each message there was also stored by the server prior to being sent out to the recipients. *Id.* at 704 (emphasis added).[19] This "storage" by the server did not define the action as an accession in *Szymuskiewicz* (though this is what the defendant advocated), and it does not in this case. *Id.*

The pointer/copy distinction is immaterial. This "pointer" system was the way the entire Access2Go email system worked – all emails, no matter to what account they were sent, were stored on the server and obtained by the users through "pointers." Both the Shefts account and the dummy account received the "pointers" contemporaneously, and the dummy account thereby received the same ability to obtain the messages as did the Shefts account, at the same time. In *Szymuszkiewicz*, the Seventh Circuit made clear that, though the technical details are important, the key point is whether the device in question allows the

[18] If "copies" of the emails had been sent to both accounts, this case is on all fours with *Szymuskiewicz* and there was clearly an interception within the meaning of the ECPA.

[19] Moreover, the court held that even if it was the recipient's computer that received the message and copied it for forwarding, there would still be an "interception," not an "accession." *Id.* at 706.

communications to be acquired contemporaneously with transmission.[20] *Id.* at 704-05. *See also United States v. Steiger*, 318 F.3d 1039, 1050 (1th Cir. 2003) (interception of email requires use of automatic routing device). Applying the definitions found in the statute, the Seventh Circuit noted that "[e]mail messages are transfers of writings, and forwarding enabled Szymuszkiewicz to acquire those writings' contents," so technical distinctions between the way various communications systems operate are irrelevant. *Szymuszkiewicz*, 622 F.3d at 705. Here, the forwarding setup enabled Defendants to acquire Plaintiff's messages when he acquired them. The Court finds that this is sufficient to constitute an interception. The ECPA is not focused on whether a person possesses a copy of a message, but on whether the person intercepts communications to which he is not a party.[21]

[20] As the Court discusses further below, the key point appears to be that transmission of the message in question triggers the interception, that it is "automatic," not the precise amount of time between receipt by the intended recipient and the "spy." As to the Access2Go email, time lapse is not an issue, as the two accounts received the "pointers" simultaneously, but the "rule" set up by Defendants did cause the server to make a "pointer" available to both Plaintiff and the dummy account when a message was transmitted to Plaintiff's account, so this is well within the "trigger" analysis discussed below.

[21] The Court notes that Defendants' argument would appear to apply to block the application of the ECPA to spies using the internal forwarding features of web-based email services, as the end users there typically only receive links to their messages, which they then view online in web browsers, not actual copies of those messages. The Court previously rejected, as a matter of law, the argument that because emails are recorded by the service provider, users automatically consent to all surveillance under the ECPA, finding that it conflicted with the intent of Congress to protect email through the ECPA. (Doc. 209 at 17 fn. 18). Here, too, the notion that a spy using the forwarding features of a web-based email services is exempt from the ECPA because he views the messages online, rather than receiving copies, is out of line with the purpose of the statute. A person's email should not be

II. Yahoo! email and use of SpectorPro

Plaintiff also alleges that Defendants "intercepted" messages from his Yahoo! web-based email account by their use of the SpectorPro software. SpectorPro, which Defendants installed in June 2008, operates by taking images of a user's activities on his computer. As Plaintiff viewed his Yahoo! email, or composed messages within it, or engaged in any other activities on his computer, SpectorPro simultaneously captured images of his activity. Defendants claim that SpectorPro's operation did not affect interstate commerce, so its use did not affect commerce so as to put it within the terms of the ECPA.

A protected "electronic communication" protected from interception by the ECPA is defined as "any transfer of…signals,…images,…[or] data, or intelligence of any nature transmitted in whole or in part by a[n]…electromagnetic…system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12). Because SpectorPro captured information from Plaintiff's computer itself and sent that information to Defendants' "monitoring station" through Access2Go's internal network, rather

excluded from ECPA protection merely because of the mechanism by which the email system operates.

There is no caselaw that speaks directly to the question of whether a "pointer" to a message can be protected, but the Court's conclusion is bolstered by the legislative history behind the ECPA, which reveals that Congress intended for the phrase "electronic communication" to have a broad meaning:

> The term 'electronic communication' is intended to cover a broad range of communication activities . . . As a rule, a communication is an electronic communication if it is neither carried by sound waves nor can fairly be characterized as one containing the human voice (carried in part by wire). *Communications consisting solely of data, for example . . . would be electronic communications.*

H.R. Rep. No. 99-647 at 35 (1986) (emphasis added). A "pointer" to an email stored on a server is a communication that consists "solely of data." Although a "pointer" to the email and a copy of the email itself are different types of communication, both are considered electronic communications under the ECPA nonetheless.

than over the internet, Defendants claim that it does not "affect commerce" and is therefore outside the ECPA's protection. As Plaintiff notes, though, it is the communication itself that must affect commerce, not the means of interception. The Court agrees that the text of the statute clearly supports Plaintiff's interpretation: the protected "electronic communication" itself must affect commerce, not the device used to intercept the communication. 18 U.S.C. § 2510(12). "Intercept" is defined as "the…acquisition of the contents of any…electronic…communication through the use of any electronic…or other device" - this definition does not require any effect on interstate commerce. 18 U.S.C. § 2510(4). Likewise, the definition of "device" does not include a requirement that it affect commerce. 18 U.S.C. § 2510(5). If Defendants intercepted Plaintiff's Yahoo! email communications, they undoubtedly intercepted a protected electronic communication. It is thus immaterial whether SpectorPro itself used the internet to transmit images of Plaintiff's monitor to Defendants, as the statute does not require this.

Rene v. G.F. Fishers, Inc. and *United States v. Ropp*, on which Defendants rely, both deal with "keylogger" devices. *Rene*, 817 F.Supp.2d 1090 (S.D. Ind. 2011); *Ropp*, 347 F.Supp.2d 831 (C.D. Cal. 2004). Defendants, relying on these cases, assert that keylogger software does not "intercept" within the meaning of the ECPA, and claim that SpectorPro falls into the same category of device. There is an important technical distinction between the operation of keyloggers and software like SpectorPro, though: a keylogger merely, as the name suggests, only records the letters typed on a computer, while SpectorPro captured all the activity on Plaintiff's monitor, including messages he was transmitting and receiving. The "transmission" in question for a keylogger is only the transmission of signals from the keyboard to the computer, not from the computer across the internet.[22] *Rene*, 817 F.Supp.2d at 1094; *Ropp*, 347 F.Supp.2d at 837-38. A keylogger's interception, then, is merely the capturing of signals between the keyboard and the computer, not "electronic communications" that affect commerce. In neither of these cases did the keylogger's activity violate the ECPA, because the intercepted communications were not "electronic communications" that affected commerce, but were only intra-computer signals between keyboard and computer. Here, SpectorPro enabled Defendants to view Plaintiff's Yahoo! email communications as they were transmitted between his computer and others across the internet, and so is not in the same category of devices as those used in *Ropp* and *Rene*. Indeed, a key finding for the *Ropp* court was that "the network connection [was] irrelevant to the transmissions, which could have been made on a stand-alone computer that had no link at all to the internet" – here, conversely, the Yahoo! email service cannot, by definition, be used without an internet connection, as it is web-based. 347 F.Supp. at 838. Viewing and using the Yahoo! email service necessarily involves the transmission of signals over the internet.

Even if Defendants' arguments are defeated, Plaintiff still must be able to prove that Defendants' use of SpectorPro intercepted his Yahoo! email. In his Motion for Summary Judgment, Plaintiff argues that the contemporaneous "screenshots" of his Yahoo! email activity taken by SpectorPro were an "interception." In support of this argument, Plaintiff relies only on a case involving

[22] Indeed, in *Ropp*, there was a device physically attached to the cable between the keyboard and the computer. 347 F.Supp.2d at 831.

Florida's Security of Communications Act, which he claims "mirror the provisions of the ECPA pertaining to 'intercept.'" (Doc. 232 at 17 (citing *O'Brien v. O'Brien*, 899 So.2d 1133 (Fla. App. Ct. 2005)). As explained above, the fact that a state statute is similar to a federal statute, or even relies on federal interpretations of federal statutes, does not mean that the state court's decisions interpreting the state statute are controlling authority for this Court in interpreting a federal statute. The Court therefore rejects Plaintiff's reliance on *O'Brien*, and must analyze whether Defendants intercepted an electronic communication within the meaning of the ECPA.

There are not many cases analyzing the application of the ECPA to screen-capture technology. In light of the other ECPA precedent discussed in this Order, though, the Court must find that Defendants' use of SpectorPro constituted an interception under the ECPA. As discussed above, in order to "intercept" of an "electronic communication," the device in question must capture the communication "contemporaneously" with its transmission. First, it is undisputable that Plaintiff's Yahoo! email messages were "electronic communications:" they were transfers of writings transmitted by an electromagnetic system that affects interstate or foreign commerce. 18 U.S.C. § 2510(12); *Szymuszkiewicz*, 622 F.3d at 704.

Plaintiff puts on undisputed evidence that the SpectorPro software caused images of Plaintiff's computer activity, including his communications via his Yahoo! email account, to be simultaneously captured by SpectorPro. Such simultaneous capture included moments when Yahoo! was transmitting messages to or from Plaintiff's account, as shown by Plaintiff's exhibit of a Yahoo! email between himself and his attorney, which was captured by SpectorPro. Notably, any emails sent by Plaintiff on his Yahoo! account via his desktop computer would have been captured by SpectorPro *as they were transmitted* to Yahoo! via the internet. Therefore, SpectorPro contemporaneously captured Plaintiff's electronic communications within the meaning of the ECPA, and Defendants were able, if they were at the monitoring station while Plaintiff was using his Yahoo! email account, to view Plaintiff's communications as he viewed them.[23] *Szymuszkiewicz*, 622 F.3d at 706.

III. Blackberry text messages

Finally, Plaintiff argues that Defendants intercepted his Blackberry text messages by causing the Blackberry to retain all messages, and by causing the BES server to synchronize those messages with the Access2Go server. Defendants counter by arguing, *inter alia*, that the server did not acquire the text messages contemporaneously with their original transmission, so there was no "interception" of the messages.[24] The Court finds that Defendants did not intercept the text messages within the meaning of the ECPA, and that their actions constituted an accession of those messages within the terms of the SCA.

[23] In *Szymuskiewicz*, the Seventh Circuit noted that the defendant there could, *if* he were at his computer at the same time as the victim, receive the victim's messages within a moment of the victim receiving them, but did not require proof that there ever was a moment at which both were using their computers at the same time. 622 F.3d at 706. The interception by the device must take place contemporaneously; it does not matter if the "spy" actually views the intercepted communication at the same time.

[24] For the same reasons explained above, Defendants' "affecting commerce" argument is rejected. It is the messages themselves that must be transmitted via a network that affects commerce (the Verizon network); the device that intercepts those messages need not itself affect commerce in its operation.

The Court must clarify that there are two potential moments of "interception:" (1) when the Blackberry device itself retained all of the text messages sent and received by Plaintiff, and (2) when the Blackberry synchronized with the BES server. Initially, Plaintiff argued only that Defendants intercepted his text messages by causing his Blackberry device itself to capture and retain all of his messages, which were then acquired by the server when it later "synchronized" with the Blackberry device. The parties first dispute whether the Blackberry device itself, in retaining Plaintiff's messages, "intercepted" them within the meaning of the ECPA. The Seventh Circuit's precedent is clear that no additional device is needed to intercept a communication; the device sending or receiving a message can also intercept it. *Szymuskiewicz*, 622 F.3d at 707. However, Defendants point out that they did not set up the Blackberry to retain Plaintiff's messages, but that such retention was an automatic part of how the Blackberry worked. The fact that the server was set up to synchronize with the Blackberry did not cause the Blackberry to retain the messages; it would have retained them even if synchronization had not been set up. Plaintiff puts on no evidence that the Blackberry's own retention of his messages was in any way caused by Defendants' actions. None of Plaintiff's evidence contradicts this evidence from Mr. Grons. If Defendants did not cause the Blackberry to retain Plaintiff's text messages, then its retention of the messages cannot be held against them as an interception in violation of the ECPA.

Plaintiff also argues that Defendants intercepted his text messages by setting up the BES server to capture the messages from the Blackberry device through synchronization with the device. Defendants respond by arguing that such synchronization was merely an "accession" of data stored on the Blackberry, and not an "interception" contemporaneous with the messages' transmission. Plaintiff relies heavily on the finding that some of the synchronizations occurred within a few seconds of the messages' transmission, and argues that they were thus "contemporaneous." He also notes that in some instances, the BES server's synchronizations with the Blackberry occurred at irregular intervals of less than 10 minutes.

In *Szymuskiewicz*, as also discussed above, the Seventh Circuit noted that "several circuits have said that, to violate § 2511, an interception must be 'contemporaneous' with the communication," and held that the interception at issue, which was caused by the automatic forwarding of the victim's email messages to the "spy's" email account, was contemporaneous. 622 F.3d at 706 (citing *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir. 2003); *Steve Jackson Games, Inc. v. Secret Service*, 36 F.3d 457 (5th Cir. 1994); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002); *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003)). The Court agrees with Defendants that the messages were not contemporaneously acquired by the server, and that this defeats the claim that they were "intercepted." It is plain that the server acquired the messages from storage on the Blackberry, and as Defendants point out, the shortest time between transmission and synchronization of any message was two seconds, which, while a short period, is not necessarily contemporaneously. *See id.* at 706 ("within a second" contemporaneous).

More importantly, though, the Court believes that the key distinction in a situation where the intercepting device operates only intermittently is whether the transmission of the messages triggered synchronization with the server, which is not the case here. While the *Szymuskiewicz* court did note that receipt by the "spy" "within a second" was "contemporaneous by any standard," the Court does not believe that this was meant to imply that any communication that is accessed within an "eyeblink" is intercepted, rather than accessed. *Id.* In *Szymuskiewicz*, the "rule" set up by the defendant caused the server to send copies of the message to both the intended recipient and the defendant when they were transmitted – the forwarding was triggered by the transmission. As explained in *Szymuskiewicz*, even when a message *is* intercepted, there may be slight delays between when the intended recipient and the "spy" receive the message; these delays do not put the conduct outside the ECPA's prohibition. *Id.* at 705. Neither can the absence of a long delay necessarily put conduct within the ECPA.

It is this Court's understanding of *Szymuskiewicz* that in situations such as this, where the allegedly intercepting device operates only intermittently (rather than continuously, as in the SpectorPro instance), the amount of time between transmission and interception by the spy is not the primary determining factor, but rather the fact that interception was automatically triggered by transmission or reception.[25] Here, the BES server did not acquire the text messages as they were

[25] This interpretation does not mean that all "interceptions" must be triggered by the transmission of a communication. As with the screen-capture technology discussed above, some intercepting devices are "always on" and therefore capture all communications simultaneously with their transmission. However, for devices that

transmitted to or from Plaintiff, but acquired them from the Blackberry at predetermined intervals. Even if Plaintiff can show that occasionally those intervals were irregular, and shorter than the pre-set 10 minute interval, he has no evidence showing that the synchronization was ever actually triggered by the receipt or transmission of a message. Therefore, the server did not "intercept" the messages, and Plaintiff's ECPA claim as to the text messages must fail.

CONCLUSION

For the foregoing reasons, the Court finds that Defendants did intercept Plaintiff's Access2Go email and his Yahoo! email within the meaning of the ECPA, and grants Defendants summary judgment Plaintiff's claim in Count I that they violated the ECPA by intercepting his Blackberry text messages. Therefore, Plaintiff's Motion for Summary Judgment on a Major Issue (Intercept) (Doc. 231) is GRANTED IN PART AND DENIED IN PART and Defendants' Motion for Summary Judgment on Count I of Plaintiff's Complaint (Doc. 229) is GRANTED IN PART AND DENIED IN PART. IT IS SO ORDERED. An order will follow setting this matter for Final Pretrial Conference and Jury Trial.

Entered this 12th day of September, 2012.

s/ Joe B. McDade
JOE BILLY McDADE
United States Senior District Judge

work only intermittently, as the synchronization did here, such intermittent operation must be linked with the transmission of the communication.