

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

LISA M. RENE,)	
)	
Plaintiff,)	
)	
vs.)	Cause No. 1:11-cv-514-WTL-DKL
)	
G.F. FISHERS, INC., et al.,)	
)	
Defendants.)	

ENTRY ON DEFENDANTS' MOTION TO DISMISS

This cause is before the Court on the Defendants' motion to dismiss the Plaintiff's Complaint for failure to state a claim upon which relief can be granted. The motion is fully briefed, and the Court, being duly advised, **GRANTS IN PART AND DENIES IN PART** the motion for the reasons and to the extent set forth below.

I. STANDARD

In reviewing a motion to dismiss under Rule 12(b)(6), the Court must take the facts alleged in the complaint as true and draw all reasonable inferences in favor of the plaintiff. The complaint must contain only "a short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), and there is no need for detailed factual allegations. However, the statement must "give the defendant fair notice of what the . . . claim is and the grounds upon which it rests" and the "[f]actual allegations must be enough to raise a right to relief above the speculative level." *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 633 (7th Cir. 2007) (quoting *Bell Atl. Corp. v. Twombly*, 127 S.Ct. 1955, 1965 (2007)).

A plaintiff's brief may clarify lingering uncertainty about the allegations in her complaint. *Pegram v. Herdrich*, 530 U.S. 211, 230 (2000). The facts alleged in a plaintiff's

briefs may be considered so long as the brief's allegations are consistent with the complaint. *Flying J Inc. v. City of New Haven*, 549 F.3d 538, 542, n.1 (7th Cir. 2008). Finding Rene's allegations consistent with her complaint, the Court considers and accepts as true the additional facts alleged in Rene's briefs.

II. FACTUAL BACKGROUND

The facts as alleged in the plaintiff's Complaint and in her briefs in opposition to the instant motion are as follow.

Plaintiff Lisa M. Rene ("Rene") began working for Defendants G.F. Fishers, Inc. and G.F. Oregon, Inc. at their Southport store in Indianapolis, Indiana, in January 2009. The relationship of Defendants Daniel S. Austad, Rebecca Susan Austad, and Dean Austad to Defendants G.F. Fischers, Inc. and G.F. Oregon, Inc., is unclear but irrelevant to the instant motion.

Rene's employment duties included use of the store's personal computer. Before Rene's employment, the Defendants installed keylogger software on this computer. This keylogger software recorded all keystrokes made on the store's computer keyboard. It then periodically emailed that information to Dean Austad and other Defendants.

While personal use of the store's computer generally was prohibited, Defendants Rebecca and Daniel Austad authorized Rene to access her personal checking account and her personal email account from this computer.

After Rene had used the computer to access her email and personal checking accounts, the Defendants informed Rene that they had installed keylogger software on the store's computer.

Using this software, the Defendants acquired Rene's email password and her personal checking account password. The Defendants used these passwords to access and view Rene's email and personal checking accounts, and the Defendants viewed, forwarded, and discussed among themselves some of Rene's email messages. It is unclear whether these messages had been previously read by Rene. The Defendants also viewed and discussed the contents of her personal checking account.

In late May 2009, Rene discovered that the Defendants were accessing her email and personal checking accounts. Rene confronted Daniel Austad about this access on June 4, 2009. After this confrontation, Daniel Austad falsely documented poor performance by Rene for the purpose of terminating her employment.

As a result of Rene's discovery, the Defendants terminated Rene's employment on June 22, 2009.

III. DISCUSSION

In her Complaint, Rene argues that the Defendants' actions violated the Federal Wiretap Act, the Indiana Wiretap Act, and the Stored Communications Act. Each count will be addressed in turn below.

A. Federal Wiretap Act

The Federal Wiretap Act ("FWA") criminalizes the interception of electronic communications, 18 U.S.C. § 2511(1)(a), and also provides for the recovery of civil damages for an interception, 18 U.S.C. § 2520(a). Rene claims that the Defendants have violated the FWA by intercepting the transmission of her keystrokes as she typed her passwords into the store's

personal computer. In reply, the Defendants argue that the capture of keystrokes does not constitute an “interception” as defined in the statute.

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.” 18 U.S.C. § 2510(4). In addition, interception must occur contemporaneously with the communication. *United States v. Szymuszkiewicz*, 622 F.3d 701, 705-06 (7th Cir. 2010) (noting the requirement in other circuits and applying the standard). Rene argues that when the keylogger software catches the transmission of a keystroke as it travels from keyboard to computer, a contemporaneous interception has been made. While capture and transmission may indeed occur simultaneously, this is not enough.

The Defendants argue that there was no interception because keystrokes do not constitute “electronic communication,” defined as “any transfer of signs, signals, writings, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a . . . system that affects interstate or foreign commerce.” 18 U.S.C. § 2510(12). The Defendants correctly point out that an electronic communication within the purview of the statute must be transmitted by a system that affects interstate or foreign commerce.

The 11th Circuit recently addressed a similar claim in *United States v. Barrington*, ___ F.3d ___, 2011 WL 3503206 (11th Cir. Aug. 11, 2011). In *Barrington*, three undergraduate students at Florida A&M University installed keylogger software on registrar computers in order to acquire employees’ passwords and then use these passwords to change student grades. *Id.* at *1. The keylogger software operated by “covertly record[ing] the keystrokes made by Registrar employees as they signed onto their computers, capturing their usernames and passwords.” *Id.*

The software then automatically transmitted the usernames and passwords to the students' email accounts. *Id.* However, there was no evidence that the software at issue had the capacity to contemporaneously capture information or signals being transmitted beyond the user's computer. *Id.* at *20. Accordingly, the court held that the keylogger software was not a device that could be used to intercept an electronic communication in violation of the FWA. *Id.*

Barrington explains the intersection of the requirements of contemporaneous interception with interstate commerce. Specifically, *Barrington* analyzed whether use of keylogger software satisfied the requirements of interception under the FWA. *Id.* at *20. The court noted that the "interception of electronic communications must occur contemporaneously with their transmission," but the court went further, explaining that "use of a keylogger will not violate the Wiretap Act if the signal or information captured from the keystrokes is not *at that time* being transmitted *beyond* the computer on which the keylogger is installed (or being otherwise transmitted by a system that affects interstate commerce)." *Id.* (emphasis added). The Court finds *Barrington* persuasive and accordingly adopts its holding.¹ In order to violate the FWA, contemporaneous interception must occur while the transmission is traveling through a system that affects interstate or foreign commerce.

The key to the *Barrington* decision lies in the fact that the transmission of keystrokes exists internally on a computer. The relevant "interception" acted on a system that operated solely between the keyboard and the local computer, and captured a transmission that required

¹ The Court notes that the rule adopted here is consistent with the recent case of *United States v. Szymuszkiewicz*, 622 F.3d 701 (7th Cir. 2010). In *Szymuszkiewicz*, the defendant set up a "rule" his supervisor's computer, which caused copies of the supervisor's email messages to be sent to the defendant. *Id.* at 703. The "rule" was logged and implemented on a regional server that routed incoming and outgoing messages. *Id.* at 704. The server dispatched the message and its copy to the intended email inboxes. *Id.* The interception, the "rule," thus operated on a transmitting system affecting interstate or foreign commerce.

no connection with interstate or foreign commerce to reach its destination. Because the keylogger software in *Barrington* had not been shown to capture transmissions occurring on a system affecting interstate commerce, the keylogger software in *Barrington* did not satisfy the requirements of the FWA. *See also United States v. Ropp*, 347 F. Supp. 2d 831, 837-38 (C.D. Cal. 2004) (explaining that, even though the computer itself was connected to a network, “the network connection is irrelevant to the transmissions [captured by the keylogger], which could have been made on a stand-alone computer that had no link at all to the internet or any other external network”).²

As in *Barrington* and *Ropp*, while the Defendants’ keylogger software may have captured transmissions in transit, the system through which these signals traveled did not affect interstate or foreign commerce. As a result, the intercepted keystrokes are not “electronic communications” under the FWA. Because the intercepted keystrokes were not electronic communications, they could not be “intercepted” as that term is defined in the FWA. For this reason the Court accordingly holds that the Defendants’ keylogger software did not intercept an electronic communication as a matter of law, and Rene’s claim for interception must fail.

Rene also alleges violations of 18 U.S.C. § 2511(c) and (d), regarding the use and disclosure of information that was obtained through interception. Because no interception has occurred, no violation of the use and disclosure provisions has occurred, and Rene’s Federal Wiretap Act claim fails in its entirety.

B. Indiana Wiretap Act

² Contrary to Rene’s assertion, the court in *Ropp* did not find that the computer in that case did not affect interstate or foreign commerce. Rather, *Ropp* held that, even if a *computer* were connected to a larger system that affected foreign or interstate commerce, the relevant scope of inquiry applied to the *system* transmitting the intercepted communication. 347 F. Supp. 2d at 837-38.

The Indiana Wiretap Act (“IWA”) provides a civil cause of action for anyone whose “communications are intercepted, disclosed, or used in violation of this article.” IND. CODE 35-33.5-5-4. Rene claims that, by accessing, viewing, and forwarding her email messages and other information obtained by the keylogger software, the Defendants have violated the IWA.

The Defendants argue that because Rene’s claim under the FWA fails, her claim under the IWA must also fail, because, they assert, the definition of interception under the IWA is “nearly identical” to the definition of interception under the FWA. Although these definitions indeed echo each other, Rene’s claim does not necessarily fail.

The IWA defines interception as “the intentional recording or acquisition of the contents of an electronic communication by a person other than a sender or receiver of that communication, without the consent of the sender or receiver, by means of any instrument, device, or equipment under this article.” IND. CODE 35-33.5-1-5. The FWA defines interception 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). While the meaning of these provisions may be quite similar, these definitions are hardly identical.

More pertinent to this case are the definitions of “electronic communication,” which are closely related. *Compare* IND. CODE 35-33.5-1-3.5 *with* 18 U.S.C. § 2510(12). Yet a critical phrase is absent from the IWA– while the FWA requires that a communication be transmitted by a system “affecting interstate or foreign commerce,” the IWA does not include this restriction. This Court’s holding that Rene’s FWA claim fails turns on this important phrase. Absent this phrase, the transmitting system at issue– the cord between keyboard and computer – may satisfy the system requirements for an “electronic communication” under the FWA. Likewise, the

system at issue may satisfy the requirements for “electronic communication” under the IWA. Thus, even if the federal requirement of “contemporaneous interception” is grafted on to the statute, the clear absence of this phrase would change the applicable standard for an “interception” under the IWA. While the FWA requires that the interception occur contemporaneously with transmission by a system affecting interstate commerce, the IWA appears to merely require that the interception occur contemporaneously with transmission by a system. For this reason, even if, as the Defendants’ claim, interpretation of the IWA follows federal case law as far as the text allows,³ Rene’s IWA claim survives.

The Defendants further argue that Rene’s claim under the IWA fails because Rene consented to the interception. In response, Rene contends that the interceptions occurred at a time when Rene was not on notice that her communications would be monitored. If the relevant interceptions occurred prior to the Defendants giving notice to Rene of the keylogger software, then it may be that Rene did not legally consent to the interception. Accordingly, Rene has satisfied her burden of giving the Defendants notice of the IWA claim brought against them.

C. Stored Communications Act

The Stored Communications Act (“SCA”) prohibits “intentionally accessing without authorization a facility through which an electronic communication service is provided,” and thereby obtaining access to an “electronic communication while it is in electronic storage.” 18 U.S.C. § 2701(a). It also provides for the recovery of civil damages by a person aggrieved by a violation of the statute. 18 U.S.C. § 2707(a). Rene alleges that the Defendants violated the SCA when they accessed her email messages. The Defendants contend that any email messages

³ The Court notes that whether interpretation of the IWA does indeed follow the FWA is far from established. *See State v. Lombardo*, 738 N.E.2d 653, 658 (Ind. 2000) (explaining that, unlike other states’ statutes that copy the language of the FWA, the Indiana Act “largely stands on its own,” but then comparing certain limited similarities).

viewed by them were not in “electronic storage,” and, as a result, do not fall within the protections of the statute.

“Electronic storage” is defined as “any temporary, intermediate storage of a[n] . . . electronic communication incidental to the electronic transmission thereof,” 18 USC § 2510(17)(A), and “any storage of such communication by an electronic communication service for purposes of backup protection of such communication,” 18 USC § 2510(17)(B).

The Defendants argue that, whether opened or unopened, email messages are not in electronic storage. It is unclear whether opened email messages are in electronic storage. *Compare Theofel v. Farey-Jones*, 359 F.3d 1066, 1071, 1075-76 (9th Cir. 2004) (explaining that “prior access is irrelevant to whether the messages at issue were in electronic storage”; rather, the inquiry under definition (B) is the purpose for which the messages are being stored), *and Jennings v. Jennings*, 697 S.E.2d 671, 678 (S.C. Ct. App. 2010) (holding that email messages stored on a server after the messages have been opened are in electronic storage because they are stored for backup protection), *with Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010) (holding that webmail messages opened and retained by the user, absent a showing that the webmail service was archiving copies for backup purposes, were not within the definition of “electronic storage”), *and United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (“Previously opened emails stored by Microsoft for Hotmail users are not in electronic storage”). However, the Court need not resolve this issue now, for, consistent with numerous other courts, the Court determines that at a minimum email messages that have reached the addressee’s inbox, but which have yet to be opened by the addressee, are in “temporary, intermediate storage.” *Crispin*, 717 F. Supp. 2d at 987(explaining that webmail messages that

have not yet been opened are in electronic storage); *United States v. Councilman*, 418 F.3d 67, 81 (1st Cir. 2005) (explaining that temporary storage refers to “when a message sits in an email user’s mailbox after transmission but before the user has retrieved the message from the mail server”); *Steve Jackson Games, Inc. v. U.S. Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994) (holding that email messages stored on a computer, but not yet read, were in electronic storage); *cf. United States v. Weaver*, 636 F.Supp.2d 769, 771 (C.D. Ill. 2009) (focusing not on an email message’s location, but rather on its status as opened and holding that opened email messages are not in temporary, intermediate storage).⁴ As a footnote in *Crispin* explains, the distinction critical to these courts’ holdings is rooted in the state of technology when the SCA was enacted. 717 F. Supp. 2d at 983, n.36. Passed in 1986, the SCA reflects a time when “multiple service providers [stored] communications briefly before forwarding them on to their next destination or while awaiting download by the recipient.” *Id.* (citing William Jeremy Robison, Note, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1995, 1206 (2010)). Insofar as an email message waiting to be downloaded had yet to travel the channel between server and local computer, it remained in temporary, intermediate storage incident to transmission. Similarly, inasmuch as an email waiting in an inbox has yet to be

⁴ Defendants contend that the majority of courts have held otherwise, arguing instead that an email is in electronic storage *until* it is delivered to the user’s inbox. Adjusting for changes in technology, the cases Defendants cite in support of their assertion indicate that the opposite is true. Some prior cases hinged on “delivery” – the point at which the recipient downloaded the message from the server. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1075 (“Several courts have held that [temporary, intermediate storage] covers email messages stored on an ISP’s server pending delivery to the recipient.”); *In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511-512 (S.D.N.Y. 2001) (explaining that the act focuses on “communications stored by electronic communication services incident to their transmission—for example, when an email service stores a message until the addressee downloads it”); *see Crispin*, 717 F. Supp. 2d at 972, n.15 (citing William Jeremy Robison, Note, *Free at What Cost? Cloud Computing Privacy Under the Stored Communications Act*, 98 Geo. L.J. 1995, 1198 (2010)) (explaining that, in the mid-1980s, “users could download or send email” after accessing the network via modem). Yet *Crispin* explains that the “modern day analogy” to the technology at issue in these prior cases is “an email in an inbox that has not yet been opened by the recipient.” 717 F. Supp. 2d at 983, n.36. This analogy recharacterizes “delivery” as the act of opening one’s email while accessing it from a remote server.

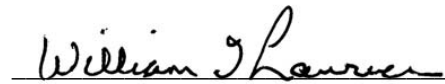
accessed by the addressee, even though it may be kept after viewing only on the regional server, it too has yet to travel to its ultimate destination.

Rene's complaint does not state whether the email messages accessed by the Defendants had already been opened by her, but Rene is not required to allege such details at this stage. By alleging that the Defendants made unauthorized access to her email, Rene has satisfied her burden of asserting a violation of the SCA.

IV. CONCLUSION

For the foregoing reasons, the Defendants' Motion to Dismiss is **GRANTED** as to Rene's Federal Wiretap Act claim, **DENIED** as to Rene's Stored Communications Act claim, and **DENIED** as to Rene's Indiana Wiretap Act claim.

SO ORDERED: 09/16/2011



Hon. William T. Lawrence, Judge
United States District Court
Southern District of Indiana

Copies to all counsel of record via electronic communication.