IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

LOIS OWEN,	)	
	)	
Plaintiff,	)	**Case No. 1:15-cv-9880**
	)	
v.	)	
	)	**Judge John Z. Lee**
PAUL CIGNA, PROFESSIONAL CONSULTANTS, INC. & NOAH EDMEIER,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION AND ORDER

Plaintiff Lois Owen claims that Defendants Paul Cigna, Professional Consultants, Inc., and Noah Edmeier violated multiple federal laws when they accessed her private email account through her former work computer. Defendants have moved under Fed. R. Civ. P. 12(b)(6) to dismiss the complaint for failure to state a claim upon which relief may be granted. For the reasons given below, the Court grants the motion in part and denies it in part. Count I is dismissed without prejudice, Count II is dismissed with prejudice, and Count III may proceed.

DISCUSSION

In reviewing the sufficiency of a complaint, the Court views it in the light most favorable to the nonmoving party and accepts all well-pleaded facts as true. *Zahn v. N. Am. Power & Gas, LLC*, 815 F.3d 1082, 1087 (7th Cir. 2016).

According to Owen's complaint, she worked for Cigna and Professional Consultants, Inc. (PCI) until July 2013. Compl. at 1.[1] After leaving her job at PCI, Owen filed a complaint with the Illinois Human Rights Commission (IHRC), in which she accused her former employers of sexual harassment and of creating a hostile work environment. *Id.*

During discovery in the IHRC case, Owen learned that "Defendants, including PCI's technology consultant Noah Edmeier, accessed her email account without her permission after she left work." *Id.* at 2. She has attached to her complaint Cigna's affidavit from the IHRC case, where Cigna confirms that Defendants did indeed acquire Owen's personal emails through her former work computer, which was the property of PCI. *Id.*, Ex. A, Cigna Aff., ¶ 7. Neither the complaint nor the accompanying exhibits indicate precisely how Defendants used her former work computer to access her personal emails, which Owen alleges were "stored on a server at att.net," rather than on the computer. Compl. ¶ 30.

The emails in question, which Cigna attached to his affidavit, contained sexually explicit content, including photos of nude women (though not of Owen herself). Owen alleges that she has been "damaged in excess of $5,000.00 as a result of the access to her account, including publication of her confidential email correspondence." Compl. ¶ 19.

[1] Citations to the complaint are to page numbers when the allegation in question is not found in a numbered paragraph.

I. Federal Wiretap Act, 18 U.S.C. §§ 2510–22

In Count I, Owen brings a claim under 18 U.S.C. § 2520, which creates a private right of action for violations of Title I of the Electronic Communications Privacy Act, commonly known as the Federal Wiretap Act. She claims that Defendants violated the section of the Act that applies (with certain exceptions) when a person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." *Id.* § 2511(1)(a).

Defendants argue that Owen's Wiretap Act claim must be dismissed because her own allegations show that Defendants acquired her emails after she stopped working at PCI, rather than at the time the emails were sent. Mem. Supp. at 5–7. Because Defendants' acquisition of the emails was not "contemporaneous" with the emails being sent or received, Defendants argue that their acquisition does not qualify as an "interception" as required by the Wiretap Act. *Id.*

In response, Owen contends that the Seventh Circuit rejected the "contemporaneous" requirement in *United States v. Szymuszkiewicz*, 622 F.3d 701, (7th Cir. 2010). But this is a misreading of the case. In *Szymuszkiewicz*, the Seventh Circuit first acknowledged that "[s]everal circuits have said that, to violate § 2511, an interception must be 'contemporaneous' with the communication." *Id.* at 705. The court did not then go on to adopt that requirement expressly, but neither did the court reject the requirement or even criticize it. Instead, the *Szymuszkiewicz* court explained that the "contemporaneous" requirement did not mean, as the

defendant in that case argued, that an email communication had to be intercepted "in flight" to violate the Act. *Id.* at 706. The defendant in *Szymuszkiewicz* had been surreptitiously receiving his supervisor's emails within an "eye blink" of his supervisor's receipt of them, and the Seventh Circuit considered this "contemporaneous by any standard." *Id.*

The Court is persuaded that Defendants could only have violated the Wiretap Act if they accessed Owen's emails contemporaneously with the emails' transmission or receipt. The concept of interception suggests contemporaneousness, and, as the Third Circuit explained in *Fraser v. Nationwide Mutual Insurance Co.*, 352 F.3d 107, 113 (3d Cir. 2003), Congress has chosen not to overrule the cases that have read a contemporaneousness requirement into the Wiretap Act when the Act was amended. The Court's view is also supported by at least one case in this district decided after *Szymuszkiewicz*. *See Epstein v. Epstein*, No. 14 C 8431, 2015 WL 1840650, at *3 (N.D. Ill. Apr. 20, 2015) (adopting contemporaneousness requirement).

The allegations in Owen's complaint, which must be credited at this stage, establish that Defendants did not access her emails contemporaneously with the emails' transmission or receipt. Owen alleges that Defendants accessed her emails after she stopped working for PCI in July 2013, *see* Compl. at 1–2, and she has attached the emails to her complaint, the most recent of which was sent in May 2011. Transmission and access separated by more than two years cannot be said to be "contemporaneous by any standard."

Accordingly, Count I is dismissed for failure to state a claim upon which relief may be granted. Because Owen stresses in her brief that she does not actually know precisely when Defendants accessed her emails (meaning they could have done so contemporaneously with the emails' transmission), *see* Resp. Br. at 3, this dismissal is without prejudice.

II. Computer Fraud and Abuse Act, 18 U.S.C. § 1030

In Count II, Owen claims that Defendants violated the Computer Fraud and Abuse Act (CFAA). As is relevant here, the Act creates liability for a person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." 18 U.S.C. § 1030(a)(2). The "term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6). The Act provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator." *Id.* § 1030(g).

Owen alleges that Defendants exceeded their authorization to access her former work computer when they used it to retrieve her emails. Compl. ¶ 27. In return, Defendants argue that they could not exceed their authority to access the computer because the computer belonged to PCI—not to Owen—and Owen, who had left the company, was no longer using it. Mem. Supp. at 8–9.

Neither party has identified—and the Court has not found—any CFAA case involving an employee's claim that her former employer exceeded its authority to access its own computer. Owen cites *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010), but that case concerned privileged emails between an employee and her attorney and did not concern the CFAA.

The facts alleged in a complaint "must raise the claim above a mere 'speculative level,'" *Bonnstetter v. City of Chicago*, 811 F.3d 969, 973 (7th Cir. 2016) (quoting *Bell Atlantic Corp. v. Twombly,* 550 U.S. 544, 555 (2007)), and the Court agrees with Defendants that Owen's allegations are insufficient to state a CFAA claim that they exceeded their authority to access the computer in question. "Authorization" is not defined in the statute, but courts that have considered its definition have concluded that the word should be given its common meaning. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015); *CollegeSource, Inc. v. AcademyOne, Inc.*, 597 F. App'x 116, 129 (3d Cir. 2015).[2]

None of Owen's allegations suggests that she retained any authority to grant or deny anyone permission to access her former work computer after she left PCI. She may well have had the power to deny access to her web-based email account, but the CFAA is aimed at unauthorized access to computers, not unauthorized access to web-based accounts, *see* 18 U.S.C. § 1030(a)(2), and the only computer Owen alleges Defendants accessed without authority is her former work computer. These allegations do not raise her claim above the speculative level, and Count II is

[2] Black's defines authorization as "[o]fficial permission to do something; sanction or warrant." Black's Law Dictionary (10th ed. 2014).

dismissed for failure to state a claim upon which relief can be granted. This dismissal is with prejudice.

III. Stored Communications Act, 18 U.S.C. §§ 2701–12

In Count III, Owen claims that Defendants violated the Stored Communications Act (SCA), which is Title II of the Electronic Communications Privacy Act, by accessing her private emails. Those emails, she alleges, were "stored on a server at att.net." Compl. ¶ 30.

The SCA is violated when a person "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage." 18 U.S.C. § 2701(a).

In their motion, Defendants first argue that the emails were not in "electronic storage" as meant in the Act, and thus Owen has not stated an SCA claim. Mem. Supp. 12–14. "Electronic storage" is defined as

> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

18 U.S.C. § 2510(17).

The first definition, which concerns "temporary, intermediate storage," clearly does not apply to Owen's emails, but Defendants argue that the second

definition does not apply either. Owen, Defendants point out, has not alleged that she was storing "backup" copies of her emails on the att.net server, and they cite cases in which courts have observed that email stored by a web-based email service is not stored for "backup" purposes unless another copy exists somewhere. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1077 (9th Cir. 2004) ("Even as to remote computing services that are also electronic communications services, not all storage covered by sections 2702(a)(2)(B) and 2703(b)(2)(B) is also covered by section 2510(17)(B). A remote computing service might be the only place a user stores his messages; in that case, the messages are not stored for backup purposes."); *United States v. Weaver*, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) ("[U]nless a Hotmail user varies from default use, the remote computing service is the only place he or she stores messages, and Microsoft is not storing that user's opened messages for backup purposes.").

But neither *Theofel* nor *Weaver* holds that an SCA claim must be dismissed if its allegations do not explicitly track one of the definitions of electronic storage in 18 U.S.C. § 2510(17). The *Theofel* court simply explained that any copies of the plaintiffs' emails stored by an electronic communication service could be considered backup copies if the plaintiffs had previously downloaded the messages. 359 F.3d at 1075.[3] The court never suggested that, to state an SCA claim, a plaintiff must allege

[3] Nowadays, countless email users access web-based email accounts on cellular phones, tablets, and other mobile devices, and those emails remain accessible even when the individual is not connected to the web-based server. Whether messages that can be accessed in this manner are "stored" for "purposes of backup protection" under the SCA is a question for another day. *See Theofel*, 359 F.3d at 1076 ("But the mere fact that a copy *could* serve as a backup does not mean it is stored for that purpose.")

that a message was being stored for backup purposes. And *Weaver* involved the government's authority to subpoena certain communications in a criminal case and did not address federal civil pleading standards. 636 F. Supp. 2d at 769.

Defendants also rely on *Fraser v. Nationwide Mutual Insurance Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), a case holding that an electronic communication is not in electronic storage under either definition in 18 U.S.C. § 2510(17) if the email has already been received by the intended recipient. But Defendants fail to mention that, on appeal, the Third Circuit expressly declined to adopt the district court's holding. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2003) ("[T]o us it seems questionable that the transmissions were not in backup storage—a term that neither the statute nor the legislative history defines. Therefore, while we affirm the District Court, we do so through a different analytical path, assuming without deciding that the e-mail in question was in backup storage."). Moreover, as the *Theofel* court explained, the district court's holding in *Fraser* is inconsistent with the text of the 18 U.S.C. § 2510(17):

> In contrast to subsection (A), subsection (B) does not distinguish between intermediate and post-transmission storage. Indeed, *Fraser*'s interpretation renders subsection (B) essentially superfluous, since temporary backup storage pending transmission would already seem to qualify as "temporary, intermediate storage" within the meaning of subsection (A). By its plain terms, subsection (B) applies to backup storage regardless of whether it is intermediate or post-transmission.

359 F.3d at 1075–76. The Court agrees with the *Theofel* court's rejection of the district court's holding in *Fraser*.

Additionally, the Court finds persuasive cases such as *Pascal Pour Elle, Ltd. v. Jin*, 75 F. Supp. 3d 782 (N.D. Ill. 2014), and *Kaufman v. Nest Seekers, LLC*, No. 05 CV 6782 (GBD), 2006 WL 2807177 (S.D.N.Y. Sept. 26, 2006), which explicitly reject the idea that a plaintiff, to state an SCA claim, must specify that a stored electronic communication was in "temporary, intermediate storage" or was stored "for purposes of backup protection." *See Pascal*, 75 F. Supp. 3d at 788–90 (SCA claim was adequately pled despite that plaintiff had "not alleged that the data was being stored temporarily, incidental to its transmission, or that it was stored as backup"); *Kaufman*, 2006 WL 2807177, at *7 (simple allegations that electronic communications were stored on a particular server were "sufficient to make out the element of 'electronic storage'"). As the *Pascal* court explained, Federal Rule of Civil Procedure 8(a)(2) requires only "a short and plain statement of the claim showing that the pleader is entitled to relief," and whether the communications at issue in an SCA claim were "stored for back-up purposes [is] more appropriately left for summary judgment or trial." 75 F. Supp. 3d 782, 788–90 (N.D. Ill. 2014); *see also Joseph v. Carnes*, 108 F. Supp. 3d 613, 618 (N.D. Ill. 2015) (holding that emails archived in a database were in "electronic storage" as defined in 18 U.S.C. § 2510(17)(B)).

Defendants next argue that, even if they accessed the emails while the emails were in electronic storage, they were authorized to do so and thus cannot be liable under the SCA. Mem. Supp. 14–15. Indeed, the SCA "does not apply with respect to conduct authorized . . . by the person or entity providing a wire or electronic

communications service." 18 U.S.C. § 2701(c)(1). But—unlike Defendants' undeniable authority to access the PCI computer after Owen stopped working for PCI—Defendant was not authorized to access Owen's att.net email account (at least according to Owen), and the resolution of this issue too is best reserved for consideration after discovery.

For the reasons given above, Defendants' motion to dismiss is granted in part and denied in part. Count I is dismissed without prejudice, Count II is dismissed with prejudice, and Count III may proceed.

SO ORDERED

ENTER: 5/25/16

JOHN Z. LEE
United States District Judge