UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

Freedom Banc Mortgage Services, Inc.,

Plaintiff,

v.

Case No. 2:11-cv-01073
JUDGE GREGORY L. FROST
Magistrate Judge Mark R. Abel

Norma Lynn O'Harra et al.

Defendants.

OPINION AND ORDER

This matter is before the Court for consideration of Defendant Norma Lynn O'Harra's motion for judgment on the pleadings pursuant to Rule 12(c) (ECF No. 24), Plaintiff's memorandum in opposition (ECF No. 30), Defendant O'Harra's motion to exclude evidence outside the pleadings (ECF No. 32), and Defendant O'Harra's reply in support of its motion to dismiss (ECF No. 33). Also before this Court is Defendants Clearcreek Township and Kevin G. Knobbe's (collectively, "Clearcreek Defendants") motion for judgment on the pleadings pursuant to Rule 12(c) (ECF No. 21), Plaintiff's memorandum in opposition (ECF No. 26), and Clearcreek Defendants' motion to exclude evidence outside the pleadings and reply in support of its motion to dismiss (ECF No. 29). For the reasons that follow, the Court **GRANTS IN PART** and **DENIES IN PART** the motions to dismiss. The Court also **GRANTS** Defendant O'Harra's and Clearcreek Defendants' motions to exclude evidence outside the pleadings.

I. Background

The facts in this section are taken from Plaintiff's amended complaint and are assumed true for purposes of this Opinion and Order. Plaintiff, a corporation, hired Defendant O'Harra in

June 2008 as a contractor to perform data entry work. In June 2009, Plaintiff discovered that Defendant O'Harra was not performing the work for which she was being paid. Plaintiff filed suit against Defendant O'Harra in the Franklin County Court of Common Pleas seeking recovery of the wages it had paid to Defendant O'Harra up to that point.

In March 2010, Defendant O'Harra began remotely downloading software programs onto Plaintiff's computers. These programs provided Defendant O'Harra with unauthorized access to twenty-seven of Plaintiff's computers and five of Plaintiff's servers. Plaintiff alleges on information and belief that Defendant Knobbe and four unidentified individuals named as "John Does 2–5" assisted and/or collaborated with Defendant O'Harra in downloading these programs and accessing Plaintiff's computers.

In July 2010, Plaintiff obtained a judgment against Defendant O'Harra in the amount of $24,354.04 in the Franklin County lawsuit. Plaintiff and Defendant O'Harra discussed payment options but the parties could not reach an agreement. Later that month, Plaintiff's president Stephen Harris received a call from Defendant Knobbe. Defendant Knobbe identified himself as an officer of the Clearcreek Township Police Department and requested that Harris cease all attempts to communicate with Defendant O'Harra regarding the judgment against her.

Defendants O'Harra, Knobbe, and John Does 2–5 continued to remotely download software and monitoring programs onto Plaintiff's computers for the next several months. Through these programs, Defendants accessed Plaintiff's employees' email accounts, deleted hundreds of emails from these accounts, uninstalled Plaintiff's security camera, deleted pictures that the camera had recorded, and monitored Plaintiff's employees' Blackberry usage, among other activities. Defendants initiated contact with Plaintiff's computers approximately 125,000

times.

As a result of these unauthorized intrusions into Plaintiff's computer system, Plaintiff's computers began to operate slowly and twenty-two computers and three servers eventually became inoperable. Plaintiff lost business, productivity, and revenue as a result of the damage to its computers. In December 2010, as a result of this damage, Plaintiff ceased its business operations.

Internet Protocol ("IP") addresses assigned to Defendant O'Harra's home and work, Warren County, the Warren County Sheriff, the State of Ohio and Reading Township were used to access Plaintiff's computers. Defendant O'Harra also left behind electronic cookies indicating that she had remotely accessed Plaintiff's employees' accounts.

II. Procedural Posture

Plaintiff filed its complaint in this case on December 1, 2011 against Defendant O'Harra and John Does 1–7, with John Does 1–5 being individuals and John Does 6–7 being unidentified employers who were allegedly negligent in their supervision and oversight of the individual defendants. On March 14, 2012, Plaintiff filed an amended complaint ("Amended Complaint") substituting the names of Defendant Knobbe and Defendant Township for John Does 1 and 6, respectively. The Amended Complaint offers no new allegations against Defendant O'Harra; thus, the parties agreed that Defendant O'Harra's answer to the original complaint is deemed her answer to the Amended Complaint. Clearcreek Defendants answered the amended complaint on May 3, 2012.

The Amended Complaint asserts claims against Defendants for violations of the Computer Fraud and Abuse Act (Count One), violations of the Electronic Communication

Privacy Act (Count Two), trespass to chattels (Count Three), conversion (Count Four), and conspiracy (Count Five). The Amended Complaint includes an additional claim for negligent supervision and discipline (Count Six) against Defendant Township and John Doe 7.

Defendant O'Harra and Clearcreek Defendants now move for judgment on the pleadings pursuant to Rule 12(c). The Court will consider each of these motions in turn.

III. Analysis

Rule 12(c) provides that "[a]fter the pleadings are closed—but early enough not to delay trial—a party may move for judgment on the pleadings." Fed. R. Civ. P. 12(c). The Court reviews motions made under Rule 12(c) in the same manner it would review a motion made under Rule 12(b)(6). *Vickers v. Fairfield Med. Ctr*., 453 F.3d 757, 761 (6th Cir. 2006). Accordingly, to survive a motion for judgment on the pleadings, a complaint must provide fair notice of each claim and the grounds upon which it rests. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007) (citing *Conley v. Gibson*, 355 U.S. 41, 47 (1957)). A court, in ruling on a Rule 12(b)(6) or Rule 12(c) motion, must construe the complaint in the light most favorable to the plaintiff and treat all well-pleaded allegations contained therein as true. *Id*. at 555–56. The defendant bears the burden of demonstrating that the plaintiff failed to state a claim for relief. *Directv, Inc. v. Treesh*, 487 F.3d 471, 476 (6th Cir. 2007).

Pursuant to Rule 8(a)(2), a complaint must contain a "short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). Although Rule 8 does not require "detailed factual allegations," "it does not unlock the doors of discovery for a plaintiff armed with nothing more than conclusions." *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009). A court need not "accept as true a legal conclusion couched as a factual allegation."

Twombly, 550 U.S. at 555 (quoting *Papasan v. Allain*, 478 U.S. 265, 286 (1986)). Once the court has identified the well-pleaded allegations in the complaint, it should view each allegation in the context of the entire complaint to determine whether the plaintiff has alleged sufficient facts to support his or her claims. *See In re Polyurethane Foam Antitrust Litig.*, 799 F. Supp. 2d 777, 782 (N.D. Ohio 2011).

Considering only those well-pleaded facts, a complaint must "state a claim to relief that is plausible on its face." *Twombly*, 550 U.S. at 570. "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Iqbal*, 556 U.S. at 678 (citing *Twombly*, 550 U.S. at 556). A plaintiff's factual allegations must be enough to raise the claimed right to relief above the speculative level and to create a reasonable expectation that discovery will reveal evidence to support the claim. *Twombly*, 550 U.S. at 556. If the "well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct," the court should dismiss the complaint. *Iqbal*, 556 U.S. at 679.

A. Evidence Outside the Pleadings

The Court first addresses the issue of evidence outside the pleadings. In its memoranda in opposition to Defendant O'Harra's and Clearcreek Defendants' motions to dismiss, Plaintiff attached and referenced documents from state court proceedings and portions of a transcript from a forensic consultant's testimony that purportedly support its allegations in the Amended Complaint. (ECF No. 26-1–26-4; ECF No. 30-1.)

Because Plaintiff did not reference this evidence in the Amended Complaint, the Court will not consider it at the Rule 12(c) stage. *See Weiner v. Klais & Co.*, 108 F.3d 86, 88–89 (6th

Cir. 1997) ("Matters outside of the pleadings are not to be considered by a court in ruling on a [Rule 12(c)] motion to dismiss."). The Court also notes that both Defendant O'Harra and Clearcreek Defendants moved to exclude this evidence from the Court's consideration at this stage of the litigation and that Plaintiff did not file a memorandum in opposition, which is an additional ground on which the Court may grant the motions and exclude the evidence. S.D. Ohio Civ. R. 7.2(a)(2).

The Court **GRANTS** Defendant O'Harra's motion to exclude evidence outside the pleadings (ECF No. 32) and Clearcreek Defendants' motion to exclude evidence outside the pleadings (ECF No. 29). The Court will not consider Exhibits 26-1, 26-2, 26-3, 26-4, or 30-1 and/or any references to these exhibits for purposes of this Opinion and Order.

B. Defendant O'Harra's Motion

The Court now considers Defendant O'Harra's motion to dismiss. Defendant O'Harra first argues that Plaintiff's use of "Defendants" throughout the Amended Complaint is impermissibly vague. Defendant O'Harra asserts that the Court should disregard any allegation against "Defendants" because it is impossible to determine the role that each individual defendant played in the alleged misconduct.

This argument fails to recognize the fact that the Amended Complaint identifies Defendant O'Harra as the primary actor and alleges that Defendant Knobbe and John Does 2–5 assisted and/or collaborated with her in accessing Plaintiffs' computers. The Amended Complaint later states that electronic cookies and IP addresses assigned to Defendant O'Harra's home and work indicate that she participated in accessing Plaintiff's computers.

Necessarily regarding these allegations as true and drawing all inferences in Plaintiff's

favor, it is plausible that Defendant O'Harra, Defendant Knobbe, and John Does 2–5 all engaged in the alleged conduct and/or that Defendant O'Harra engaged in the alleged conduct with the assistance of Defendant Knobbe and John Does 2–5. *See, e.g., Hale v. Enerco Group, Inc.*, No. 1:10 CV 00867, 2011 U.S. Dist. LEXIS 781, at *12 (N.D. Ohio Jan. 5, 2011) ("While Plaintiffs have made allegations that multiple Defendants have engaged in the same conduct, those allegations are plausible and raise a reasonable expectation that discovery will reveal evidence to support their claims."). Plaintiff has sufficiently linked Defendant O'Harra to the alleged misconduct such that she has sufficient notice of the claims against her and the grounds upon which they rest. *Cf. Bondex Int'l, Inc. v. Hartford Accident & Indem. Co.*, 667 F.3d 669, 681 (6th Cir. 2011) (declining to consider one theory of liability against a certain defendant because the complaint did not link that defendant to the relevant factual allegations other than referencing the misconduct of "all Defendants"). Finally, the Amended Complaint also identifies the role of Defendant Township and John Doe 7 in the alleged misconduct (negligent supervisors). Defendant O'Harra's argument regarding the possible "permutations" of "Defendants" that could have engaged in each alleged act is without merit.

1. Computer Fraud and Abuse Act ("CFAA")

The Court next addresses the parties' arguments regarding Count One. The Amended Complaint alleges that Defendants violated §§ 1030(a)(2) and 1030(a)(5) of the CFAA, 18 U.S.C. § 1030 *et seq*. Section 1030(a)(2) applies to one who intentionally accesses a computer without authorization or exceeds authorized access and thereby obtains information from any "protected computer." Section 1030(a)(5) applies to whomever–

> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without

authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.

Defendant O'Harra first argues that Plaintiff fails to state a claim under § 1030(a)(5) because the Amended Complaint recites subsections (A) – (C) and does not identify the specific subsection that Defendant O'Harra allegedly violated. Subsections (A) – (C) are similar and vary only in the means by which the computer was accessed and/or damaged; thus, the Amended Complaint's citation to 18 U.S.C. §§ 1030(a)(2) and 1030(a)(5) is adequate. Defendant O'Harra proceeds to argue that Plaintiff's recitation of the elements of the statute is a legal conclusion that is not entitled to a presumption of truth under *Iqbal*, but ignores the factual allegations preceding this claim that set forth the grounds upon which it rests.

Defendant O'Harra next argues that Claim One is deficient because Plaintiff fails to allege facts suggesting that its computers are "protected computers" within the meaning of the CFAA. The CFAA defines the term "protected computer" as follows:

(2) the term "protected computer" means a computer–

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) *which is used in or affecting interstate or foreign commerce or communication*, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

18 U.S.C. § 1030(e)(2) (emphasis added).

Plaintiff argues that its computers are "protected" within the meaning of § 1030(e)(2) for the sole reason that they are connected to the internet. Plaintiff points to several allegations in

the Amended Complaint that involve an internet connection (*e.g.*, the allegation that Defendants accessed Plaintiff's employees' email accounts) and argues that, because its computers were connected to the internet, its computers were used in or affecting interstate commerce within the meaning of the statute. In response, Defendant O'Harra argues that Plaintiff has not alleged any facts to link its computer use to interstate commerce and that accepting Plaintiff's definition of protected computer would expand the scope of the CFAA beyond reason.

The Court begins its analysis by noting that the phrase "used in or affecting interstate or foreign commerce" evinces an intent by Congress to exercise its full power under the Commerce Clause. *See Russell v. United States*, 471 U.S. 858, 859 (1985) (holding that, in interpreting a federal arson statute, "[t]he reference to 'any building . . . used . . . in any activity affecting interstate or foreign commerce' expresses an intent by Congress to exercise its full power under the Commerce Clause" (citing 18 U.S.C. § 844(i))). Any computer that is subject to regulation under Congress' Commerce Clause power is a "protected computer" under the CFAA. *See id.*; 18 U.S.C. § 1030(e)(2); *see also United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007).

Congress may use its Commerce Clause power to regulate instrumentalities of interstate commerce. *United States v. Lopez*, 514 U.S. 549, 566 (1995). Courts have consistently held that the internet is " 'an instrumentality and channel of interstate commerce' " such that any computer that is connected to the internet is part of " 'a system that is inexorably intertwined with interstate commerce.' " *Trotter*, 478 F.3d at 921 (citing *United States v. MacEwan*, 445 F.3d 237, 245 (3d Cir. 2006)); *see also United States v. Hordaday*, 392 F.3d 1306, 1311 (11th Cir. 2004). Computers that are connected to the internet therefore are used in or affect interstate commerce such that they are protected computers under § 1030(e)(2). *See, e.g., Trotter*, 478

F.3d at 921; *Expert Janitorial, LLC v. Williams*, No. 3:09-CV-283, 2010 U.S. Dist. LEXIS 23080, at *24 (E.D. Tenn. Mar. 12, 2010); *Continental Group, Inc. v. KW Prop. Mgmt., LLC*, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009); *Patrick Patterson Custom Homes, Inc. v. Bach*, 586 F. Supp. 2d 1026, 1032 (N.D. Ill. 2008); *Paradigm Alliance, Inc. v. Celeritas Techs., LLC*, 248 F.R.D. 598, 602 and n.5 (D. Kan. 2008).

The Court notes that "[n]o additional interstate nexus is required when instrumentalities or channels of interstate commerce are regulated." *Trotter*, 478 F.3d at 920. A computer that is connected to the internet therefore satisfies § 1030(e)(2)'s interstate commerce requirement even if the plaintiff used that connection to engage in only intrastate communications. *See id.*; *see also NCMIC Fin. Corp. v. Artino*, 638 F. Supp. 2d 1042, 1060 (S.D. Iowa 2009). Allegations that a computer was used to engage in email communications is sufficient to support the inference that the computer was connected to the internet and therefore within the purview of § 1030(e)(2). *See, e.g.*, *Expert Janitorial, LLC*, 2010 U.S. Dist. LEXIS 23080, at *24.

The Court concludes that Plaintiff has sufficiently alleged facts to support the inference that its computers were connected to the internet such that they are "protected computers" under § 1030(e)(2). Defendant O'Harra's argument that accepting the above definition of a protected computer would expand the CFAA beyond reason because "modern televisions, automobiles, and even refrigerators would become protected computers," (ECF No. 33, at 6), has already been confronted and persuasively rejected. *See Trotter*, 478 F.3d at 921. *Trotter* also dispenses with Defendant O'Harra's argument that Plaintiff failed to link its internet use to interstate communications. *Id.*

Defendant O'Harra's next argument is that Plaintiff failed to properly allege that it

suffered more than $5,000 in loss as required to maintain a civil action under the CFAA. *See* 18 U.S.C. §§ 1030(g) & (c)(4)(A)(i)(I).[1] Specifically, the alleged conduct must involve "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." *Id*. § 1030 (c)(4)(A)(i)(I). Defendant O'Harra argues that damages under the CFAA must stem from a single act and that Plaintiff fails to identify an unauthorized intrusion that, itself, caused a $5,000 loss.

This argument has also been persuasively rejected. *See Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 934–35 (9th Cir. 2004). Like Defendant O'Harra, the *Creative Computing* defendant cited a quote from the Senate Report on the bill that "the Committee intends to make clear that losses caused by the same act may be aggregated for purposes of meeting the . . . threshold" in support of its argument that the CFAA requires a $5,000 loss for each unauthorized intrusion into a protected computer. *Id*. at 935. The Ninth Circuit disagreed with this interpretation and stated that "the obvious purpose of this remark was permissive, to allow aggregation to meet the $5,000 floor." *Id*. In other words, "[t]he damage floor in the Computer Fraud and Abuse Act contains no 'single act' requirement." *Id*.

Similarly unpersuasive is Defendant O'Harra's argument that the Amended Complaint fails to allege that Plaintiff sustained more than $5,000 in loss. The CFAA defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior

[1]Pursuant to 18 U.S.C. § 1030(g), a plaintiff may maintain a civil action under the CFAA if the alleged conduct involves any one of five factors set forth in § 1030(c)(4)(A)(i)(I)–(IV). Subsection (I) contains the only factor ($5,000 in loss) that is potentially relevant to this litigation.

to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). Plaintiff alleges that Defendants' conduct caused its computers to fail and that Plaintiff lost revenue as a result. *See, e.g., Crown Coal & Coke Co. v. Compass Point Res., LLC*, No. 07-1208, 2009 U.S. Dist. LEXIS 52949, at *8 (W.D. Pa. June 23, 2009) ("[I]f defendants had lost revenue because their computers were inoperable, that would be the type of lost revenue contemplated by the [CFAA]."). Plaintiff also alleges that the conduct took place within a one-year period (from March – December 2010) and that its loss exceeded $5,000. Defendant O'Harra's reliance on *Fontana v. Corry*, No. 10-1685, 2011 WL 4473285, at *9 (W.D. Pa. Aug. 30, 2011), in which the plaintiff alleged that his or her loss *and* damages—which is defined separately under the CFAA—together exceeded $5,000, is misplaced.

The Court finds that Plaintiff has sufficiently pleaded facts in support of its CFAA claim. The Court **DENIES** Defendant O'Harra's motion to dismiss Count One.

2. Stored Communications Act

Defendant O'Harra next challenges the allegations surrounding Count Two – Violation of Title II of the Electronic Communications Privacy Act (commonly referred to as the Stored Communications Act ("SCA")), 18 U.S.C. § 2701 *et seq*. The SCA makes it an offense to intentionally access without authorization (or exceed one's authorization to access) a "facility through which an electronic communication service is provided" and thereby obtain, alter, or prevent authorized access to a wire or electronic communication "while it is in electronic storage in such system." 18 U.S.C. § 2701(a). The SCA is a criminal statute that provides a civil claim for relief for any person who is aggrieved by a violation of the statute. *Id*. § 2707.

The SCA does not define "facility" but defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (incorporated by 18 U.S.C. § 2711(1)). 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." *Id*. § 2510(17) (incorporated by 18 U.S.C. § 2711(1)).

Plaintiff does not allege or argue that it provides any type of electronic communication service as defined in § 2510(15). Instead, Plaintiff alleges that its computers are "facilities" within the meaning of the statute, presumably because they enable the use of electronic communication services. Plaintiff argues that it stored information—such as data regarding employee email accounts, user-names and passwords—on its computers and that Defendants accessed that information by accessing Plaintiff's computers without authorization. Plaintiff cites *Expert Janitorial* as a case in which a court found that such allegations are sufficient to state an SCA claim. 2010 U.S. Dist. LEXIS 23080, at *15.

Defendant O'Harra argues that Plaintiff's computers are not "facilities" within the meaning of § 2701(a). In support, Defendant O'Harra cites cases in which the court questioned whether personal computers qualify as "facilities" if the computer does not, itself, provide an electronic communication service. *See, e.g.*, *Hilderman v. Enea Teksci, Inc*., 551 F. Supp. 2d 1183, 1204 (S.D. Cal. 2008). *Hilderman* highlights a more obvious problem with Plaintiff's argument: it is difficult to imagine how Plaintiff's storage of information on its computers fits within § 2510(17)'s definition of "electronic storage." Although Defendant O'Harra does not

explicitly raise this argument, it is intertwined with the question of whether Plaintiff's computers qualify as "facilities" under the statute.

"Electronic storage" as defined by § 2510(17) encompasses only that information that has been stored by an electronic communication service provider. This conclusion is evident from the plain language of subsection (B) and from the legislative history of subsection (A). *See* 18 U.S.C. § 2510(17)(B); *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511–12 (S.D.N.Y. 2001) (considering subsection (A)'s language and legislative history, which states that "[a]ny temporary, intermediate storage [in § 2510(17)(A)] describes an e-mail message that is being held by a third party Internet service provider until it is requested to be read"); *see also In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1058–59 (N.D. Cal. 2012) (adopting *Doubleclick*'s holding on this point). Information that an internet or email provider stores to its servers, information stored with a telephone company, and information maintained by an electronic bulletin board operator—if such information is stored temporarily pending delivery or for purposes of backup protection—are examples of protected electronic storage under the statute. *See United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003).

Information that an individual stores to his or her hard drive, such as images, personal information, and emails that he or she has downloaded, is not in electronic storage as defined by the statute. *See id.*; *see also Hilderman*, 551 F. Supp. 2d at 1204. In *Steiger*, for example, when a computer hacker accessed an individual's computer through an email program and retrieved personal information that the individual had saved to his hard drive, the court found that such conduct was outside the reach of the SCA. 318 F.3d at 1049. The court noted that the SCA would have applied if the hacker had also accessed information that was stored with the

individual's internet service provider. *Id*.

It follows that the relevant "facilities" that the SCA is designed to protect are not computers that enable the use of an electronic communication service, but instead are facilities that are operated by electronic communication service providers and used to store and maintain electronic storage. This interpretation of the statute is consistent with its legislative history, as

> Sen Rep. No. 99-541 (1986)'s entire discussion of [the SCA] deals only with facilities operated by electronic communications services such as 'electronic bulletin boards' and 'computer mail facilities,' and the risk that communications temporarily stored in these facilities could be accessed by hackers. It makes no mention of individual users' computers . . . .

In re Doubleclick, 154 F. Supp. 2d at 512.

Other provisions of the statute also reinforce this interpretation. For example, the conduct proscribed by § 2701(a)(1) is subject to the exceptions listed at § 2701(c). Section 2701(c)(1) exempts from the statute any conduct that has been authorized by "the person or entity providing a wire or electronic communications service." Taking this provision to its logical conclusion, if an individual's personal computer is a "facility" under the statute simply because it enables the use of an electronic communication service (as Plaintiff suggests), then the provider of that service could authorize third parties to access information that is saved to an individual's personal computer. *See Crowley v. Cybersource Corp.*, 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001); *In re iPhone Application Litig.*, 844 F. Supp. 2d at 1058. As the *Crowley* court stated, "[i]t would certainly seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of [plaintiff's] argument." 166 F. Supp. 2d at 1271.

In short, Plaintiff's allegation is too broad—its computers are not the "facilities" that the

SCA is designed to protect. Plaintiff does not allege any facts to support the inference that it maintained an electronic communication service on its computers such that Defendants accessed a protected facility within the meaning of § 2701(a). Accordingly, the Court finds that Plaintiff fails to state a claim under the SCA.

The Court **GRANTS** Defendant O'Harra's motion to dismiss Count Two.

3. Trespass to Chattels

Defendant O'Harra next argues that Plaintiff's allegations fail to state a claim for trespass to chattels. "While authority under Ohio law respecting an action for trespass to chattels is extremely meager, it appears to be an actionable tort." *Compuserve Inc. v. Cyber Promotions*, 962 F. Supp. 1015, 1021 (S.D. Ohio 1997). Ohio courts have accepted the Restatement (Second) of Torts' definition of this claim. *See id.* (collecting Ohio cases), *Dryden v. Cincinnati Bell Tel. Co.*, 135 Ohio App. 3d 394, 404, 734 N.E.2d 409 (1st Dist. 1999). Thus, to plead a claim for trespass to chattels in Ohio, a plaintiff must allege that the defendant intentionally used or intermeddled with a chattel in possession of another such that he or she (1) dispossessed the other of the chattel, or (2) the chattel is impaired as to its condition, quality, or value, or (3) the possessor is deprived of the use of the chattel for a substantial time, or (4) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest. *See Compuserve Inc.*, 962 F. Supp. at 1021 (quoting Restatement (Second) of Torts § 217); *Dryden*, 135 Ohio App. 3d at 403 (quoting Restatement (Second) of Torts § 218).

Defendant O'Harra argues that the Amended Complaint uses the term "intermeddling," which, standing alone, is insufficient to sustain a claim for trespass to chattels. This argument ignores the allegations that Defendants' conduct (which, as explained above, is properly

attributed to Defendant O'Harra) deprived Plaintiff of the use of its computers and impaired those computers as to their condition and value. *Cf. Dryden*, 135 Ohio App. 3d at 403. The Court **DENIES** Defendant O'Harra's motion to dismiss Count Three.

4. Conversion

Defendant O'Harra's next argues that Plaintiff failed to plead facts in support of its conversion claim (Count Four). This argument is also not well taken. Ohio courts define conversion as "a wrongful exercise of dominion over property in exclusion of the right of the owner, or withholding it from his possession under a claim inconsistent with his rights." *Zacchini v. Scripps-Howard Broadcasting Co.*, 47 Ohio St. 2d 224, 226, 351 N.E.2d 454 (1976). The elements of a conversion claim in Ohio are (1) the plaintiff's ownership or right of possession of the property at the time of the conversion, (2) defendant's conversion by a wrongful act or disposition of plaintiff's property rights, and (3) damages. *Dice v. White Family Cos., Inc*., 173 Ohio App. 3d 472, 878 N.E.2d 1105, 2007-Ohio-5755, ¶ 17 (2d Dist.).

Defendant O'Harra argues that Plaintiff failed to plead more than a threadbare recital of the elements and that "there is no allegation that . . . Defendant O'Harra[] was 'exercising dominion' of the computers on [the day that they allegedly failed]." (ECF No. 24, at 17.) As with her previous arguments, Defendant O'Harra fails to view Plaintiff's allegations in the context of the entire Amended Complaint. It is true that the Amended Complaint contains a section called "Fourth Cause of Action (Conversion)" and that this section includes the conclusory allegation that "Defendants exercised dominion over Plaintiff's computers in exclusion of the rights of Plaintiff." (ECF No. 8, at 8 ¶ 48.) But the Amended Complaint also states that Defendants downloaded software programs onto Plaintiff's computers that gave them

"complete access to and control over" Plaintiff's email accounts and security camera, among other things. (*Id*. at 4 ¶ 14.) The Amended Complaint then alleges that Defendants deleted hundreds of email messages from Plaintiff's email accounts, deleted photographs from Plaintiff's security camera, and continued to access and initiate contact with Plaintiff's computers until they were ultimately rendered inoperable. These allegations are sufficient to support the inference that Defendants were exercising dominion over Plaintiff's computers at the time at which they ultimately failed. The Court **DENIES** Defendant O'Harra's motion to dismiss Count Four of the Amended Complaint.

5. Conspiracy

Defendant O'Harra's final argument is that Plaintiff failed to plead facts in support of its claim for civil conspiracy. To establish a claim for civil conspiracy in Ohio, a plaintiff must allege "(1) a malicious combination, (2) two or more persons, (3) injury to person or property, and (4) the existence of an unlawful act independent from the actual conspiracy." *Aetna Cas. & Sur. Co. v. Leahey Constr. Co.*, 219 F.3d 519, 534 (6th Cir. 2000) (citing *Universal Coach, Inc. v. New York City Transit Auth., Inc*., 90 Ohio App. 3d 284, 291, 629 N.E.2d 28 (1993)). The "malicious combination" element "does not require a showing of an express agreement between defendants, but only a common understanding or design, even if tacit, to commit an unlawful act." *Knox v. Hetrick*, 8th Dist. No. 91102, 2009 WL 792357, ¶ 53 (Mar. 26, 2009).

Applying the notice pleading requirements of Rule 8, the Court finds that Plaintiff states a claim for civil conspiracy. The Amended Complaint alleges that "[f]or malicious reasons, Defendants conspired to commit unlawful acts against Plaintiff" and contains facts sufficient to support the inference that Defendants O'Harra and Knobbe both accessed Plaintiff's computer

system without authorization throughout the same time period and by the same means. The Amended Complaint also connects Defendant O'Harra to Defendant Knobbe in that Defendant Knobbe allegedly made a phone call to Stephen Harris regarding the judgment against Defendant O'Harra. Necessarily drawing all inferences in Plaintiff's favor, the Court finds that Plaintiff's allegations suggest a common understanding or design such that the "malicious combination" element for civil conspiracy claims is satisfied. *See, e.g., In re Nat'l Century Fin. Enters., Inv. Litig.*, 504 F. Supp. 2d 287, 329 (S.D. Ohio 2011) ("[A]mong the factors a fact finder may consider in inferring a conspiracy are the relationship of the parties, proximity in time and place of the acts, and the duration of the actors' joint activity." (*citing Borden, Inc. v. Spoor Behrins Campbell & Young, Inc*., 828 F. Supp. 216, 225 (S.D.N.Y. 1993))).

Plaintiff also sufficiently alleges the remaining elements of a civil conspiracy claim. The Amended Complaint identifies Defendant O'Harra and Defendant Knobbe as co-conspirators and alleges that Plaintiff suffered injury as a result of Defendants O'Harra and Knobbe's alleged misconduct. Defendant O'Harra argues that Plaintiff's reference to "Defendants" defeats its civil conspiracy claim because "[i]t is just as likely that Defendants John Does 2 through 5 and 7 conspired together as it is Defendant O'Harra conspired with another Defendant," (ECF No. 24, at 18), but the Court has already rejected this argument. Finally, the Amended Complaint states plausible claims for violations of the CFAA and trespass to chattels, both of which Plaintiff identified as unlawful acts on which its conspiracy claim is based.[2]

In arguing that Plaintiff fails to state a conspiracy claim, Defendant O'Harra incorrectly

[2]The Amended Complaint does not explicitly list conversion as an unlawful act on which its conspiracy claim is based.

cites *Blue v. Lane*, 767 F. Supp. 2d 860, 868 (S.D. Ohio 2011) as standing for the proposition that conspiracy claims are subject to heightened pleading requirements. The *Blue v. Lane* court actually addressed the issue of whether, in a claim for conspiracy to defraud, the underlying fraud claim is subject to the heightened pleading requirements of Rule 9(b). *See id*.; Fed. R. Civ. P. 9(b) (setting forth heightened pleading requirements "in alleging fraud or mistake"). Defendant O'Harra does not argue that Plaintiff's CFAA and trespass claims—the unlawful acts on which this conspiracy claim is based—are subject to the same heightened pleading requirements that apply to fraud claims. *Blue v. Lane* is therefore inapposite. Many Ohio courts have stated that conspiracy claims "must be pled with some degree of specificity and [] vague and conclusory allegations unsupported by material facts will not be sufficient to state a claim," *see, e.g., Clellan v. Wildermuth*, 10th Dist. No. 11AP-452, 2011 WL 6165004, ¶ 20 (Dec. 13, 2011) (citing *Gutierrez v. Lynch*, 826 F.2d 1534, 1538 (6th Cir. 1987)), but this language merely restates the standard for all claims post *Twombly/Iqbal*.

The Court **DENIES** Defendant O'Harra's motion to dismiss Count Five.

C. Clearcreek Defendants' Motion

Clearcreek Defendants begin their motion by arguing, like Defendant O'Harra, that Plaintiff's use of "Defendants" throughout the Amended Complaint is impermissibly vague. The Court disagrees. The Amended Complaint sufficiently identifies each Defendant's role in the alleged misconduct in that Defendant Knobbe allegedly assisted and/or collaborated with Defendant O'Harra in committing the alleged acts and Defendant Township was allegedly negligent in supervising and disciplining Defendant Knobbe. Clearcreek Defendants' argument regarding the possible "permutations" of Defendants that committed each alleged act is therefore

unavailing. Because it is plausible that Defendant O'Harra committed the alleged acts with the assistance of Defendant Knobbe, the Court declines to dismiss any of Plaintiff's claims on this ground. *See Hale*, 2011 U.S. Dist. LEXIS 781, at *12.

1. CFAA

The Court now considers Clearcreek Defendants' arguments concerning Count One. Clearcreek Defendants first argue that Plaintiff failed to allege that its computers were "protected computers" under the CFAA; the Court rejects this argument for the same reasons that it rejected Defendant O'Harra's argument on this point. Clearcreek Defendants do not offer any additional arguments regarding its alleged violation of 18 U.S.C. § 1030(a)(5).

Clearcreek Defendants' final CFAA argument is that Plaintiff failed to allege facts to support its allegation that Defendants "obtained information" from Plaintiff's computers within the meaning of 18 U.S.C. § 1030(a)(2)(C). Clearcreek Defendants argue that the focus of § 1030(a)(2)(C) is on the theft of information and that the Amended Complaint is void of any allegations that Defendants actually observed, read, or stole any of the information that it damaged and/or accessed on Plaintiff's computers. The Court again disagrees. "[T]he premise of [§ 1030(a)(2) is privacy protection" and the term " 'obtaining information' in this context includes mere observation of data." Economic Espionage Act of 1996, Pub. L. 104-294, Title II, § 201, 110 Stat. 3488, 3491-92 (1996); S. Rep. No. 104-357, at *7, 1996 WL 492169 (1996) (discussing 18 U.S.C. § 1030(a)(2)). Plaintiff alleges that Defendants accessed Plaintiff's computers without authorization, downloaded monitoring programs to those computers, and, *inter alia*, logged into personal accounts of Plaintiff's employees. These allegations are sufficient to support the inference that Defendants "observed" data within the meaning of §

1030(a)(2).

The Court **DENIES** Clearcreek Defendants' motion to dismiss Count One.

2. SCA

Clearcreek Defendants next challenge Plaintiff's SCA claim. Clearcreek Defendants offer the same arguments on this point that Defendant O'Harra offers in her motion to dismiss; namely, that Plaintiff's computers are not "facilities" within the meaning of 18 U.S.C. § 2701(a). For the reasons set forth above, the Court agrees with Clearcreek Defendants and finds that Plaintiff fails to state a claim under the SCA. The Court **GRANTS** Clearcreek Defendants' motion to dismiss Count Two.

3. State law claims (Counts Three – Six)

The Court now examines Clearcreek Defendants' arguments concerning the remaining claims. Clearcreek Defendants argue that, pursuant to Chapter 2744 of the Ohio Revised Code, they are statutorily immune from liability regarding any state law claims. Chapter 2744 addresses when political subdivisions, their departments and agencies, and their employees are immune from liability for their actions.

It is undisputed that Clearcreek Township is a political subdivision within the meaning of § 2744.01(F). The Court must therefore engage in a three-tiered analysis to determine whether Defendant Township is entitled to immunity. *See Lambert v. Clancy*, 125 Ohio St. 3d 231, 927 N.E.2d 585, 2010 Ohio 1483, ¶ 10. First, § 2744.02(A) provides a general grant of immunity in that political subdivisions "are not liable in damages in a civil action for injury, death, or loss to person or property allegedly caused by any act or omission of the political subdivision or an employee of the political subdivision in connection with a governmental or proprietary

function." Ohio Rev. Code § 2744.02(A)(1). Courts must then ask whether one of the five exceptions set forth in § 2744.02(B) strips the political subdivision of this immunity. *Lambert*, 125 Ohio St. 3d at 233. The § 2744.02(B) exceptions apply in specific cases of employee negligence (subsections (1) – (4)) or where a statute expressly imposes liability on the subdivision (subsection (5)). If none of the § 2744.02(B) exceptions apply, then the political subdivision is immune from liability pursuant to § 2744.02(A). *Lambert*, 125 Ohio St. 3d at 233. If one of the five exceptions does apply, then the court must conduct a third tier of analysis and determine whether any of the defenses set forth in § 2744.03 apply to reinstate the immunity. *Id*.

There are no statutory exceptions that would revoke political subdivision immunity where an employee commits an intentional tort such as trespass to chattels, conversion, and/or conspiracy. *See* Ohio Rev. Code § 2744.02(B). To the extent that Plaintiff is asserting Counts Three – Five against Defendant Township, Defendant Township is immune from liability for these claims.

The § 2744.02(B) exceptions also do not apply to Plaintiff's claim for negligent supervision. Plaintiff points to § 2744.02(B)(2), which states that "political subdivisions are liable for injury, death, or loss to person or property caused by the negligent performance of acts by their employees with respect to proprietary functions of the political subdivisions." But supervision of employees is not a proprietary function that would invoke the § 2744.02(B)(2) exception. *Moya v. Declemente*, 8th Dist. No. 96733, 2011 WL 5506081, at ¶ 19 (Nov. 10, 2011). Plaintiff has failed to allege facts that would strip Defendant Township of its general immunity under § 2744.02(A). The Court **GRANTS** Clearcreek Defendants' motion to dismiss

Counts Three – Six against Defendant Township.

The Court now turns to the allegations against Defendant Knobbe. Individual employees are not subject to the same three-tiered analysis that governs political subdivision immunity. *Lambert*, 125 Ohio St. 3d at 233–34. Instead, individual employee liability turns solely on the application of § 2744.03. *Id*. Under § 2744.03, an individual employee of a political subdivision is immune from liability for acts committed in connection with a governmental or proprietary function unless:

> (a) The employee's acts or omissions were manifestly outside the scope of the employee's employment or official responsibilities;
> (b) The employee's acts or omissions were with malicious purpose, in bad faith, or in a wanton or reckless manner;
> (c) Civil liability is expressly imposed upon the employee by a section of the Revised Code. . . .

Ohio Rev. Code § 2744.03(A)(6).

The parties agree that Defendant Knobbe is an individual employee of Clearcreek Township but dispute whether § 2744.03 applies. Clearcreek Defendants argue that, because the Amended Complaint does not specify whether Defendant Knobbe is being sued in his official or individual capacity, "the Court must presume that [Defendant] Knobbe is sued in his official capacity" such that any claims against him are actually claims against the Township. (ECF No. 21, at 14 (citing *Wells v. Brown*, 891 F.2d 591, 592 (6th Cir. 1989)).) Clearcreek Defendants then invoke Defendant Township's immunity under § 2744.02 and conclude that each of Plaintiff's state law claims must be dismissed.

Clearcreek Defendants' argument misrepresents the law in Ohio and in the Sixth Circuit. In *Lambert*, the Ohio Supreme Court acknowledged that the determination of whether an individual employee is sued in his official or individual capacity ultimately determines the

appropriate immunity analysis under Chapter 2744. 125 Ohio St. 3d at 234. But the court went on to examine whether the plaintiff's allegations pertained to the policies and practices of the political subdivision or to the actions taken by the defendant personally. *Id*. at 235. The allegations in *Lambert* were directed against the office of the political subdivision and not the individual that was named as the defendant; thus, the court held that the defendant was being sued in his official and not individual capacity. *Id*. The court reasoned that suing an officeholder of a political subdivision in his or her official capacity is equivalent to suing the subdivision itself and concluded that the three-tiered test for political subdivision immunity applied. *Id*. at 236.

The *Lambert* court's holding does not, as Clearcreek Defendants suggest, permit an individual employee defendant to escape liability simply because the complaint lacks certain buzzwords. Clearcreek Defendants' citation to *Wells v. Brown* on this point is misleading. First, *Wells* arose in the context of an Eleventh Amendment immunity challenge to a claim under 42 U.S.C. § 1983 and not under Ohio's political subdivision immunity statute. 891 F.2d at 592. Second, *Wells* has been substantially clarified (or, as some courts note, superceded) by *Moore v. City of Harriman*, in which the Sixth Circuit unequivocally rejected the argument that Clearcreek Defendants make here. 272 F.3d 769, 773–774 (6th Cir. 2001). The *Moore* court clarified that the Sixth Circuit adheres to a "course of proceedings" test in determining whether an individual has been sued in his or her official or individual capacity, and that listing an individual's name (and not his or her official title) on the complaint and referencing him or her as an "individual" are indications that he or she is being sued in his or her individual capacity. *Id*.

The Amended Complaint lists Kevin Knobbe as a defendant, identifies him as an

"individual," and provides an address for him that is different than the address provided for Defendant Township. Plaintiff's allegations are directed at Defendant Knobbe's conduct (*e.g.*, assisting Defendant O'Harra in accessing Plaintiff's computers) and not an official policy or practice of the Township. The only allegations that are directed against Defendant Township are those involving the negligent supervision and discipline claim. There is no basis to conclude that Defendant Knobbe is being sued in his official capacity.

The Court therefore must apply § 2744.03 to determine whether Defendant Knobbe is entitled to statutory immunity as an individual employee. Both parties assume that Defendant Knobbe's alleged acts were committed in connection with a governmental or proprietary function; the analysis therefore turns on application of the § 2744.03(A)(6) exceptions.

The Court finds that Plaintiff's allegations are sufficient to invoke the exceptions set forth in § 2744.03(A)(6)(a) and (b) such that Defendant Knobbe is stripped of any statutory immunity for purposes of this motion. The Amended Complaint alleges that Defendant Knobbe collaborated with Defendant O'Harra "for malicious reasons" and intentionally or recklessly caused damage to Plaintiff's computers, thus invoking the § 2744.03(A)(6)(a) exception. Clearcreek Defendants' argument that the phrase "malicious reasons" is distinguishable from the statutory "malicious purpose" language is without merit.

Clearcreek Defendants' final argument is that Plaintiff failed to plead its state law claims with the specificity that *Twombly* and *Iqbal* require. Clearcreek Defendants assert the same arguments on this point that Defendant O'Harra asserted in her motion to dismiss and the Court rejects these arguments for the same reasons that it espoused above. The Court **DENIES** Clearcreek Defendants' motion to dismiss Counts Three, Four, and Five against Defendant

Knobbe.

IV. Leave to Amend

As a final matter, the Court addresses Plaintiff's request for leave to amend in the alternative to its request that this Court deny Defendant O'Harra's motion. Courts in this circuit "[do] not look favorably upon bare requests for leave to amend in a response to a motion to dismiss when the requesting party could have filed a proper motion to amend and attached a proposed amended complaint for consideration by the court." *Techdisposal.com, Inc. v. CEVA Freight Mgmt*, No. 2:09-cv-356, 2009 WL 4283090, at *4 (S.D. Ohio Nov. 30, 2009). The court of appeals has explained:

> Had plaintiffs filed a motion to amend the complaint prior to th[e] Court's consideration of the motions to dismiss and accompanied that motion with a memorandum identifying the proposed amendments, the Court would have considered the motions to dismiss in light of the proposed amendments to the complaint . . . . Absent such a motion, however, Defendant was entitled to a review of the complaint as filed pursuant to Rule 12(b)(6). *Plaintiffs were not entitled to an advisory opinion from the Court informing them of the deficiencies* of the complaint and then an opportunity to cure those deficiencies.

PR Diamonds, Inc. v. Chandler, 364 F.3d 671, 699 (6th Cir. 2004) (quoting *Bengala v. PNC Bank*, 214 F.3d 776, 783–84 (6th Cir. 2000)). Plaintiff has failed to follow the proper procedure for submitting a motion to amend its Amended Complaint; thus, this Court "will not accept [Plaintiff's] alternative argument contained in a response to a motion to dismiss as a proper motion to amend." *Techdisposal.com, Inc.*, 2009 WL 4283090, at *4. The Court **DENIES** Plaintiff's request to amend its Amended Complaint.

V. Conclusion

For the foregoing reasons, the Court **GRANTS** Defendant O'Harra's motion to exclude evidence outside the pleadings (ECF No. 32) and Clearcreek Defendants' motion to exclude

evidence outside the pleadings (ECF No. 29).

Considering only those allegations in the Amended Complaint, the Court finds that Plaintiff fails to state a claim under the SCA against Defendant O'Harra. Plaintiff's claims for violations of the CFAA, trespass to chattels, conversion, and conspiracy survive Defendant O'Harra's Rule 12(c) challenge. Accordingly, the Court **GRANTS IN PART** and **DENIES IN PART** Defendant O'Harra's motion to dismiss. (ECF No. 24.)

The Court similarly finds that Plaintiff fails to state a claim under the SCA against Clearcreek Defendants. Defendant Township is immune from Plaintiff's state law claims; thus, Plaintiff also fails to state claims for trespass to chattels, conversion, conspiracy, and negligent supervision/discipline against Defendant Township. Plaintiff's remaining claims survive Clearcreek Defendants' Rule 12(c) challenge. The Court **GRANTS IN PART** and **DENIES IN PART** Clearcreek Defendants' motion to dismiss. (ECF No. 21.)

IT IS SO ORDERED.

/s/ Gregory L. Frost
GREGORY L. FROST
UNITED STATES DISTRICT JUDGE