IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TENNESSEE
EASTERN DIVISION

BLACK & DECKER (US), INC.,

Plaintiff,

v. No. 07-1201

TIMOTHY C. SMITH,

Defendant.

ORDER GRANTING IN PART AND DENYING IN PART
THE DEFENDANT'S MOTION TO DISMISS

On November 15, 2007, the Plaintiff, Black & Decker, Inc., ("B&D") filed the instant action against the Defendant, Timothy Smith, alleging that Smith shared certain confidential data with one of the Plaintiff's competitors in violation of the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030 et seq., the Tennessee Uniform Trade Secrets Act, Tenn. Code Ann. § 47-25-1701, and the Tennessee Personal and Commercial Computer Act of 2003, Tenn. Code Ann. § 39-14-602. B&D also includes claims of breach of contract, breach of duty of loyalty and/or fiduciary duty, misappropriation of confidential and proprietary information, and unfair competition and unfair trade practices against Smith. Before the Court is the Defendant's motion to dismiss two of these claims pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. The Plaintiff has responded and this motion is now ripe for disposition.

BACKGROUND

The Complaint alleges that the Defendant was hired by B&D in June 2004. (Docket Entry ("D.E.") No. 1, Compl. ¶ 6.) He began working for Michael Wilson, the Director of Engineering

for the Pressure Washer Design Group at B&D, as a project engineer in June 2006. (Id.) In July or August of 2007, B&D was informed by one of its customers that its contract to supply pressure washers would not be renewed for the year 2008. (Id. ¶ 7.) Instead, the contract was awarded to a competitor of B&D's, Techtronic Industries Co. ("TTI"). (Id.) According to the Plaintiff, TTI had not previously been engaged in large scale manufacturing of pressure washers in the United States. (Id.)

Shortly after B&D lost the contract, a recruiter began calling Wilson and many of the engineers who worked for him to ask them to interview at TTI. (Id. ¶ 8.) The Defendant was one of those contacted by the recruiter. (Id.) On October 8, 2007, Smith took a day off from work and interviewed with TTI in South Carolina. (Id.) He accepted a position with that company approximately four days later. (Id.) Wilson confronted the Defendant on October 15, 2007, about whether he intended to go work for TTI and Smith admitted that he had accepted a position there, to begin on October 22. (Id. ¶ 9.) Although the Defendant intended to leave on October 17, Wilson asked for his immediate resignation. (Id.)

B&D contends that Smith was asked to return all of its property and sign a termination agreement, in conformance with its regular practice. (Id.) In the termination agreement, the Defendant confirmed that he did not possess any confidential information or property of the Plaintiff's and that he would not disclose any trade secrets, confidential information, or proprietary data to any third party. (Id.) Smith had previously also signed a confidentiality agreement while he was working at a "related corporate entity to B&D," which encompassed both that company and its "'parents, subsidiaries, successors and assignees,' i.e. B&D." (Id. ¶ 11 (quoting the

confidentiality agreement).) This agreement required him to hold his work product in confidence and return any physical copies of such work to the company upon his termination. (See id.)

After Smith left his employment with B&D, Wilson became concerned that the Defendant might have taken confidential documents. (Id. ¶ 14.) With the assistance of an Information Technology Site Support Manager and a computer consultant, Wilson launched an investigation which revealed that on September 27, 2007, shortly after being contacted by the recruiter about TTI, the Defendant copied a large volume of confidential documents from B&D's secure servers into a file Smith had created under his own name on the company's H drive. (Id. ¶¶ 14-15.) The Plaintiff alleges that the documents Smith copied included confidential and proprietary information about B&D pressure washers and other B&D products in various stages of pre-market development. (Id. ¶ 15.) The investigation also revealed that the Defendant had again accessed certain confidential information on October 14, 2007, including material relating to pump strategies on B&D pressure washers, crankshaft issues, and the Plaintiff's Chinese engine supplier. (Id. ¶ 16.) He also accessed drawings and specifications relating to two confidential projects he was working on, as well as a suite of photographs of B&D prototypes, panel charts showing milestones and market research, test results on products, photographs of products in developments, copies of prototypes for new businesses, and pictures and files on new products. (Id.)

That same day, Smith attached a large external storage device to his B&D office desktop computer and saved many of these documents onto that device. (Id. ¶¶ 17, 20.) He also sent documents from his work email address to his personal Yahoo account, including an email he had received from a B&D co-worker that related to a B&D product. (Id. ¶ 18.) The Complaint contends that these actions violated the Computer Fraud and Abuse Act, 18 U.S.C. §§ 1030 et seq. and the

Tennessee Personal and Commercial Computer Act of 2003, Tenn. Code Ann. § 39-14-602. (Id. ¶¶ 26-32, 40-43.) In his motion to dismiss, the Defendant argues that these counts should be dismissed because the allegations in the Complaint cannot support a finding that he violated these statutes.

STANDARD OF REVIEW

Rule 12(b)(6) permits dismissal of a lawsuit for failure to state a claim upon which relief could be granted. See Fed. R. Civ. P. 12(b)(6). The Rule requires the Court to "construe the complaint in the light most favorable to the plaintiff, accept all of the complaint's factual allegations as true, and determine whether the plaintiff undoubtedly can prove no set of facts in support of the claims that would entitle relief." Grindstaff v. Green, 133 F.3d 416, 421 (6th Cir. 1998). "The Federal Rules of Civil Procedure do not require a claimant to set out in detail the facts upon which he bases his claim." Conley v. Gibson, 355 U.S. 41, 47 (1957). However, "[t]o avoid dismissal under Rule 12(b)(6), a complaint must contain either direct or inferential allegations with respect to all the material elements of the claim." Wittstock v. Mark A. Van Sile, Inc., 330 F.3d 899, 902 (6th Cir. 2003).

ANALYSIS

I. The Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) prohibits certain conduct involving unauthorized access to computers. See 18 U.S.C. § 1030(a)(1)-(a)(7). While primarily a criminal statute, it permits "[a]ny person who suffers damage or loss by reason of a violation of this section [to] maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Id. § 1030(g). The Complaint charges that the Defendant violated subsection (a)(2)(C) of 18 U.S.C. § 1030, which prohibits "intentionally access[ing] a computer

without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer if the conduct involved an interstate or foreign communication." Smith is also alleged to have violated § 1030(a)(4), which forbids "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value . . . ." Last, he is charged with a violation of § 1030(a)(5)(A), which provides that whoever

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

and, pursuant to § 1030(a)(5)(B), by such conduct caused or, in the case of an attempted offense, would have caused

> (i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $ 5,000 in value;
> (ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
> (iii) physical injury to any person;
> (iv) a threat to public health or safety; or
> (v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

is guilty of an offense punishable under § 1030(c).[1]

---

[1] In order for a civil action to be maintained pursuant to the CFAA, one of the five factors in subsection (a)(5)(B) must be involved in the alleged misconduct. 18 U.S.C. § 1030(g). The only applicable subsection to the facts of this case is (a)(5)(B)(i), which requires a loss of $5000. "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an

Thus, to state a claim under subsections (a)(2) and(a)(4), the Plaintiff must allege conduct that shows that Smith accessed a protected computer either "without authorization," or that he "exceeded authorized access," while to state a claim under subsections (a)(5)(A)(ii) or (iii), the access must be "without authorization." The statute defines the term "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). There is no definition of access "without authorization" in the statute. The term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." § 1030(e)(8). A "protected computer" is defined under the CFAA as a computer used in interstate or foreign commerce or communication. § 1030(e)(2)(B).

The Defendant argues that these charges must be dismissed because the CFAA only prohibits conduct that involves access without authorization or access that exceeds authorization. Smith, however, was granted access to B&D's network and systems, including electronic mail ("email") and internet access, by the Plaintiff per a July 18, 2007 Employee Access Agreement, which is attached to the Complaint. (D.E. No. 44, Mem. in Supp., at 1-2.) That agreement does not limit his access, but does provide that the Defendant "will maintain the confidentiality of all information of a confidential, proprietary or other legally sensitive nature . . ." and "will not send, share, or publish any such information on the internet without prior approval . . ." "in consideration for [his] request for access to [B&D]'s network . . . ." (D.E No. 1, Ex. C to Aff. of Michael Wilson.)

---

offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." § 1030(e)(11). The Plaintiff claims that the "research and development value" of the material the Defendant took with him is more than $1,000,000. (D.E. No. 1, Compl. ¶ 21.)

Both sides acknowledge that there is a split in legal authority as to whether the CFAA applies in a situation where an employee who has been granted access to his employer's computers uses that access for an improper purpose. Some courts have concluded that an employee may exceed his authorization or act without authorization when he retrieves confidential or proprietary information from his employer's computers that he has permission to access, but then uses that information in a manner that is inconsistent with the employer's interests or in a manner that violates a contractual obligation. See e.g., Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006) (reversing dismissal of CFAA claims where an employee breached his duty of loyalty after he resolved to quit; his subsequent "scrubbing" of a computer his employer lent him for his work consisted of access without authorization, because that breach of loyalty terminated his agency relationship, which was the only basis of his authority to access the laptop); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001) (concluding that where a former employee of the plaintiff provided another company with proprietary information in violation of a confidentiality agreement in order to mine his former employer's publically accessible website for certain information, he exceeded the authorization he had to navigate the website); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124-25 (W.D. Wash. 2000) (holding that the plaintiff's former employees were "without authorization" when they accessed and sent proprietary information to a competitor while still employed by the plaintiff); see also Int'l Sec. Mgmt. Group, Inc., v. Sawyer, No. 3:06cv0456, 2006 U.S. Dist. LEXIS 37059, at *58-59 (M.D. Tenn. June 6, 2006) (adopting Explorica and Shurgard Storage without analysis and finding that a plaintiff was likely to succeed on the merits of a CFAA claim where its former employee exceeded

his authorization when he emailed certain confidential information to his future business partner, in contravention of a non-disclosure agreement).

In coming to this conclusion, some of these courts have relied on the rules of agency, finding that the authority of an agent terminates when he acquires adverse interests or is otherwise guilty of a serious breach of loyalty to the principal. Citrin, 440 F.3d at 420-21 (noting that the former employee's breach of loyalty terminated his agency relationship); Shurgard, 119 F. Supp. 2d at 1125 (citing Restatement (Second) of Agency § 112 (1958)). Thus, even when an employee has unlimited authority to access his employer's computers, he oversteps that authority the minute his intentions are adverse to those of his principal.

Other courts have criticized this rationale, holding that the CFAA targets the unauthorized procurement or alteration of information, not its misuse. See e.g., Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965 (D. Ariz. 2008) (rejecting Citrin and Shurgard and holding that the plain language of the statute supports a narrower interpretation because 1) "without authorization" means without permission and 2) the CFAA's definition of "exceeds authorized access" contemplates a situation where "'access [to a computer] is improper because the defendant accesses information to which he is not entitled,'" rather than misuses information that he is authorized to access) (quoting Diamond Power Int'l v. Davidson, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007)); Brett Senior & Assocs., P.C. v. Fitzgerald, No. 06-1412, 2007 U.S. Dist. LEXIS 50833, at *12 (E.D. Pa. July 13, 2007) ("The common thread running through [cases like Explorica] is a focus on the employee's motive for accessing a computer and his or her intended use of the information obtained. As stated above, however, this interpretation reads section (a)(4) as if it said 'exceeds authorized use' instead of 'exceeds authorized access.'"); Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580, 2006 U.S.

Dist. LEXIS 53108, at *19 (M.D. Fla. Aug. 1, 2006) ("In this Court's view, the plain meaning brings clarity to the picture and illuminates the straightforward intention of Congress, *ie.*, 'without authorization' means no access authorization and 'exceeds authorized access' means to go beyond the access permitted. While Citrin attempts to stretch 'without authorization' to cover those *with* access authorization (albeit those with adverse interests), Congress did not so stipulate."); see also Am. Family Mut. Ins. Co. v. Rickman, No. 3:08-cv-583, 2008 U.S. Dist. LEXIS 32480, at *13 (N.D. Ohio Apr. 18, 2008) (dismissing CFAA claims on other grounds, but noting in dicta that "[t]he statute was not meant to cover the disloyal employee who walks off with confidential information. Rather the statutory purpose is to punish trespassers and hackers.").

After reviewing the language of the statute and its legislative history, the Court concludes that the latter line of cases is the more correct interpretation and that Congress did not intend to criminalize the Defendant's conduct. "As with any question of statutory interpretation, [the Court] must first look to the language of the statute itself." Brilliance Audio, Inc. v. Haights Cross Commc'ns, Inc., 474 F.3d 365, 371 (6th Cir. 2007) (citations omitted). If the language of the statute is unambiguous, courts need look no further. Id. (citations omitted). "Only if the statute is 'inescapably ambiguous' should a court look to other persuasive authority in an attempt to discern legislative meaning." Id. (quoting Garcia v. United States, 469 U.S. 70, 76 n.3 (1984)). Persuasive authority includes legislative history, policy rationales, other court decisions, the context in which the statute was passed, and other statutes. Id. Because this is a criminal statute, even though it is being applied in a civil context, the Court must apply the rule of lenity, so that the statute is interpreted consistently. Leocal v. Ashcroft, 543 U.S. 1, 12 n.8 (2004); Crandon v. United States, 494 U.S. 152, 158 (1990) (noting that where the governing standard in a civil action is set forth in

a criminal statute, the rule of lenity applies). The rule of lenity requires that ambiguities are resolved in favor of the party accused of violating the law. United States v. One TRW, Model M14, 7.62 Caliber Rifle, 441 F.3d 416, 420 n.3 (6th Cir. 2006).

As stated above, the statute defines the term "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." § 1030(e)(6). The Court agrees with Lockheed Martin that the plain meaning of "exceeds authorized access" is "to go beyond the access permitted." 2006 U.S. Dist. LEXIS 53108, at *19. Likewise, while there is no definition for access "without authorization," the Court finds that its plain meaning is "no access authorization." Id. The Defendant's alleged conduct clearly does not fall under these definitions, however, as he was permitted access to B&D's network and any information on that network. The fact that he did not have permission to subsequently misuse the data he accessed by sharing it with any of his former employer's competitors is another matter that may be circumscribed by a different statute. Even if the statute were ambiguous on the subject of whether it applies to an insider who breaches his contractual obligations to his employer to keep certain information confidential, the rule of lenity would require that this ambiguity be resolved in favor of the Defendant.

Furthermore, the legislative history supports the conclusion that Congress intended the CFAA to do "for computers what trespass and burglary laws did for real property." Orin S. Kerr, Cybercrimes' Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1617 (2003). Prior to the passage of the CFAA, Congress relied on wire and mail fraud statutes to prosecute computer crimes, but these laws were only applicable when defendants used a means of interstate commerce to execute the crime, such as making telephone

calls across state lines. H.R. Rep. No. 98-894, at 6 (1984). A 1984 House Report states that the proposed legislation was necessary because "[i]t is obvious that traditional theft/larceny statutes are not the proper vehicles to control the spate of computer abuse and computer-assisted crimes," given that they generally do not define property to include electronically processed or stored data, a problem compounded by the threat posed by "hackers who have been able to access (trespass into) both private and public computer systems." Id. at 9-10. Congress noted that modern computer networking capabilities "enabled the recent flurry of electronic trespassing incidents." Id. at 10.[2]

In one Senate Report that discusses the 1986 amendments to the statute, "unauthorized access," i.e. accessing a computer without authorization, is referred to as a "mere trespass offense." S. Rep. No. 99-432, at 7 (1986) (discussing 18 U.S.C. § 1030(a)(3), which only prohibits access of federal government computers "without authorization," rather than in excess of authorization, in order to prevent having federal employees, who have authorization to use a particular computer in one department, from being held criminally liable anytime they exceed their authorized access by perusing data they are not authorized to look at.) Another Senate Report states that the purpose of § 1030(a)(2), which prohibits both access without authorization and in excess of authorization, is

[2] The scope of the statute has been broadened several times. Deborah F. Buckman, Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030), 174 A.L.R. Fed. 101 §2(a) (2001). In 1986, the CFAA was amended to "provide additional penalties for fraud and related activities in connection with access devices and computers, and additional protection for federal interest computers." Id. In 1994, the Act was further altered to include the civil remedy at issue in this case. Id. In addition, §1030(a)(5) was modified "'to further protect computers and computer systems covered by the statute from damage both by outsiders, who gain access to a computer without authorization, and by insiders, who intentionally damage a computer.'" Id. (quoting S. Rep. No. 104-357, at 9 (1996)). It did so by prohibiting not just the unauthorized access of computers, but the transmission of programs, information, codes or commands that intentionally cause damage without authorization. Id. (citing §1030(a)(5)(A)).

to "protect against the interstate or foreign theft of information by computer." S. Rep. No. 104-357, at 7 (1996).[3]

Because Smith had permission to access the information in question and doing so was within the scope of his duties, it cannot be successfully argued that his access constituted a trespass. Clearly, the Plaintiff objects not to Smith's accessing of the information, but to his later misuse thereof. Thus, while the Complaint includes claims that the Defendant breached both the Employee Access Agreement and the confidentiality agreements by allegedly disclosing B&D's trade secrets and proprietary information, the Court finds that no facts alleged indicate that Smith exceeded the access he was granted by the Plaintiff or that he accessed the data without authorization. Accordingly, the Defendant's contentions brought pursuant to subsections (a)(2), (a)(4), and (a)(5)(A)(ii)- (iii) of 18 U.S.C. § 1030 are dismissed.[4]

---

[3] The court in Shurgard Storage relied heavily on legislative history in coming to the opposite conclusion. 119 F. Supp. 2d at 1127-29. However, the defendant in that case argued that the CFAA was only meant to apply to "outsiders," not "insiders" such as present and former employees. Id. at 1127. The Court agrees with Shurgard Storage's conclusion that the statute was intended to apply to anyone who accessed a protected computer without authorization or who exceeded their authorization in doing so, regardless of their relationship with the victim. See 18 U.S.C. § 1030 (criminalizing certain conduct committed by "whoever," and not providing any affirmative defenses relating to "insider" status). Obviously, those who exceed their authorization are more likely to be "insiders" than those who have no authorization to begin with, although the Court can envision scenarios where staff with no computer privileges hacks into a company computer. Shurgard Storage also noted that Congress hoped that computer fraud crimes that did not fit within the definition of "illegal conversion of trade secret'" might be prosecuted under the CFAA. 119 F. Supp. 2d at 1128 (citation omitted). However, this statement by Congress has nothing to do with how authorization is defined and does not imply that Congress intended to criminalize the breach of private confidentiality agreements in situations where the confidential information is accessed via a computer.

[4] The Plaintiff argues that dismissing the Complaint would be premature because it has discovered evidence that the Defendant accessed certain data that he would not have had permission to access as a pressure washer engineer. (D.E. No. 52, Resp., at 17.) However, B&D has not moved to amend its Complaint and the Court will not consider allegations outside the

Smith also contends that the Plaintiff's claim under § 1030(a)(5)(A)(i) must fail because B&D has not alleged that he caused damage. Section 1030(a)(5)(A)(i) applies to "anyone who intentionally damages a computer, regardless of whether they were an outsider or an insider otherwise authorized to access the computer." S. Rep. No. 104-357, at 10 (1996). The term "damage" means "any impairment to the integrity or availability of data, a program, a system, or information." § 1030(e)(8). The Complaint claims that the Defendant copied certain documents to a separate drive and later emailed some to his private email account and saved others onto an external storage device. (D.E. No. 1, Compl. ¶¶ 17-18.)

At least one court has held that the unauthorized copying and emailing of confidential or proprietary information does not constitute damage under the CFAA, because it does not impair any data, system or information. See Garelli Wong & Assocs. v. Nichols, – F. Supp. 2d –, 2008 U.S. Dist. LEXIS 3288, at *16-17 (N.D. Ill. Jan. 16, 2008) ("Though [the plaintiff] would like us to believe that recent amendments to the CFAA are intended to expand the use of the CFAA to cases where a trade secret has been misappropriated through the use of a computer, we do not believe that such conduct alone can show 'impairment to the integrity or availability of data, a program, a system, or information.'"); see also Lockheed Martin, 2006 U.S. Dist. LEXIS 53108, at *26 (holding that copying confidential information is not "damage" under the CFAA). This case is distinguishable from Nichols, and Lockheed Martin however, because the Complaint alleges that, in addition to copying certain information, Smith transferred certain confidential documents from a secure server to a non-secure shared company drive. (D.E. No. 1, Compl. ¶ 15.)

The legislative history of the Act supports the conclusion that intentionally rendering a

---

Complaint in evaluating a motion to dismiss.

computer system less secure should be considered "damage" under §1030(a)(5)(A), even when no data, program, or system, is damaged or destroyed. See S. Rep. No. 104-357, at 11 (1996) (discussing as an example of damage a situation where hackers alter existing log-on programs to gather user passwords and then restore the programs to their original condition; while neither the computer nor its data is technically damaged, such action "allows the intruder to accumulate valid user passwords to the system, requires all system users to change their passwords, and requires the system administrator to devote resources to resecuring the system. Thus, although there is arguably no 'damage,' the victim does suffer 'loss.' If the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief . . . .").[5] Because the allegations in the Complaint would support a finding that the Defendant caused "damage" to B&D's computer system when he transferred documents from a secure server to a nonsecure drive, Smith's motion to dismiss the Plaintiff's claim under § 1030(a)(5)(A)(i) is denied.

II. The Tennessee Personal and Commercial Computer Act of 2003

The Complaint also charges the Defendant with violating subsections (a)(1) and (b)(5) of section 39-14-602 of the Tennessee Annotated Code. (D.E. No. 1 Compl. ¶¶ 41-42.) Like the

[5] The example provided in the Senate Report is less than clear about what constitutes "damage," given that its author seems to indicate that the victim in that situation has suffered loss, not damage. See id. However, read in context, it is clear that Congress intended for the conduct described in the example to be considered a violation of the offense described in § 1030(a)(5)(A)(i), which then, as now, required that the defendant cause damage. The term "damage" was defined, in relevant part by the 1996 amendments, as "any impairment to the integrity or availability of data, information, program or system which (A) causes loss of more than $5,000 during any 1-year period . . ." Id. at 13. That definition has been shortened to not require anything more than "impairment to the integrity or availability of data, a program, a system, or information." § 1030(e)(8).

CFAA, the Tennessee Personal and Commercial Computer Act of 2003 is a criminal statute with a civil remedy. Tenn. Code Ann. § 39-14-604. Section 39-14-602(a)(1) provides that

> [w]hoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempts to access any telephone system, telecommunications facility, computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of . . . [o]btaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations, or promises violates this subsection (a) . . . .

Id. § 39-14-604(a)(1). Smith argues that this claim must be dismissed because no facts alleged in the Complaint support the conclusion that he acted "by means of false or fraudulent pretenses, representations, or promises." (D.E. No. 44, Mem. in Supp., at 11.) The Plaintiff insists, however, that the Defendant violated the statute because he did not tell B&D that he had considered and later accepted an offer of employment from TTI. (D.E. No. 52, Resp., at 16.)

There is no definition of the phrase " false or fraudulent pretenses" in the statute and no case interpreting it. However, the state of Tennessee has long criminalized the obtaining of property, money, or services by means of false pretenses. See Tenn. Code Ann. § 39-3-901 (repealed in 1989 and replaced by §§ 39-14-101 et seq., which consolidated various theft offenses such as embezzlement, false pretense, fraudulent conversion, and larceny, into a single statute); Rafferty v. Tennessee, 16 S.W. 728, 728 (Tenn. 1891) (noting that the obtaining of money or other personal property by false and fraudulent pretenses is a felony). In an early version of the false pretenses statute, the Tennessee legislature stated that the words "false and fraudulent pretenses" included

> all cases of pretended buying, borrowing and hireing [sic], and all other cases of bailment where the buyer or bailee intended at the time he received the goods, feloniously to steal the same. These words also include all cases where a person feloniously gets the money or goods or choses in action of another into possession by any false token or counterfeit letter, or by falsely personating [sic] another, or by

> falsely pretending to be the owner of such goods or choses in action, or by any other false and fraudulent pretense, where the party obtaining or getting the goods or choses in action into possession, intended at the time feloniously to steal the same . . . .

Sloan v. Tennessee, 79 S.W.2d 1021, 1022 (Tenn. 1935) (quoting section 3 of chapter 48 of the Acts of 1841-42, which prohibited "feloniously obtain[ing], or get[ting] into possession the personal goods or choses in action of another, by means of any false and fraudulent pretences [sic]"). More recently, the Tennessee legislature stated that "false pretenses" included "all cases of pretended buying, borrowing, or hiring, bailment or deposit, and all cases of pretended ownership, where the person obtaining possession intended, at the time he received the property, feloniously to steal the same." Tennessee v. Arnold, 719 S.W.2d 543, 546 (Tenn. Cr. App. 1986) (citing the now-repealed section 39-3-901(b), which provided a definition for "false pretenses").

The question before the Court is, thus, whether the Defendant's alleged silence about his plan to resign and go to work for B&D's competitor qualifies as a false statement that allowed him access to the Plaintiff's property. The Court finds that it was not. Although Smith's failure to tell his employer that he was planning to resign was perhaps not forthright, he did not misrepresent that he was employed by B&D as a pressure washer engineer, and as such, he had the right to view and access the Defendant's data. Moreover, his right to access that information pre-dated any contact he had with TTI and was not obtained by virtue of his omission. The Court therefore finds that the Plaintiff can prove no set of facts that would establish a violation of section 39-14-602(a)(1).

Section 39-14-602(b)(5) prohibits "intentionally and without authorization, directly or indirectly. . . . [making or causing] to be made an unauthorized copy . . . of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or

computer network commits an offense . . . ." The statute defines "authorization" as "any and all forms of consent, including both implicit and explicit consent." § 39-14-601(2). There are no cases applying this statute. As stated above, the Complaint alleges that the Defendant attached several documents to an email he sent to his personal Yahoo account and copied others to an external storage device. (D.E. No. 1, Compl. ¶¶ 17-18.) Smith argues that as an employee of B&D, he had implicit consent to copy its files. (D.E. No. 44, Mem. in Supp., at 12.) However, while the Court acknowledges that the Tennessee legislature intended for the concept of authorization to be interpreted broadly, it finds that the Complaint does state a claim upon which relief can be granted. The Plaintiff has alleged that the Defendant made a copy of confidential information for non-work related purposes without its permission. The issue of whether he had implied consent to do so is a factual question, which should not be resolved on a motion to dismiss. Thus, the Court denies the Defendant's motion as to section 39-14-602(b)(5).

CONCLUSION

For the reasons discussed above, the Court hereby GRANTS in part and DENIES in part the Defendant's motion to dismiss. Specifically, the Court dismisses all of the Plaintiff's CFAA claims, except that brought pursuant to 18 U.S.C. § 1030(a)(5)(A)(i). The Court also dismisses B&D's claim under section 39-14-602 (a)(1) of the Tennessee Code Annotated, but denies Smith's motion to dismiss that brought under section 39-14-602(b)(5).

IT IS SO ORDERED this 11th day of July, 2008.

s/ J. DANIEL BREEN
UNITED STATES DISTRICT JUDGE