Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.
W.D.Wash.,2000.

United States District Court, W.D. Washington,
at Seattle.
SHURGARD STORAGE CENTERS, INC., a Washington corporation, Plaintiff,
v.
SAFEGUARD SELF STORAGE, INC., a Louisiana corporation, Defendant.
No. C00-1071Z.

Oct. 30, 2000.

Employer of former employees, alleged to have appropriate trade secrets stored on employer's computers, sued competitor which allegedly received secrets, under Computer Fraud and Abuse Act (CFAA). Competitor moved to dismiss. The District Court, Zilly, J., held that: (1) for purposes of stating claim under CFAA, former employees lost access to computers when they allegedly became agents of competitor; (2) CFAA was not limited to situations in which national economy was affected; (3) fraud provision of CFAA did not require showing of common law elements; (4) provision penalizing infliction of damage on protected computers was not limited to conduct of outsiders; and (5) damage claim was stated, even though appropriation did not affect integrity of secrets within employers' computers.

Motion denied.
West Headnotes
[1] Statutes 361 188

361 Statutes
361VI Construction and Operation
361VI(A) General Rules of Construction
361k187 Meaning of Language
361k188 k. In General. Most Cited Cases
If a statute is clear and unambiguous, there is no need to look beyond its plain meaning to derive its purpose.

[2] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; Unauthorized Access or Transmission. Most Cited Cases
(Formerly 372k461.15)
Employer stated claim that former employees lacked access to its computers, as element of private action against competitor for receiving alleged trade secrets from former employees who appropriated secrets from employer's computers in violation of Computer Fraud and Abuse Act (CFAA), even though former employees claimed they had full access to computers; under principles of agency, employees lost access when they allegedly became agents of competitor and began appropriating trade secret information from computer for benefit of competitor. 18 U.S.C.A. § 1030(a)(2)(C); Restatement (Second) of Agency § 112.

[3] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; Unauthorized Access or Transmission. Most Cited Cases
(Formerly 372k461.15)

Employer engaged in self-storage business stated claim against competitor, for receipt of alleged trade secrets appropriated by former employees from employer's computers in violation of Computer Fraud and Abuse Act (CFAA), despite claim that CFAA extended protection to computers only when national economy was affected. 18 U.S.C.A. § 1030(a)(2)(C).

[4] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; Unauthorized Access or Transmission. Most Cited Cases
(Formerly 372k461.15)

Term “fraud,” as used in Computer Fraud and Abuse Act (CFAA) provision penalizing defendants who obtain access to computer with intent to defraud, meant wronging of person in his property rights by dishonest methods or schemes, rather than fraud in its common law sense. 18 U.S.C.A. § 1030(a)(4).

[5] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; Unauthorized Access or Transmission. Most Cited Cases
(Formerly 372k461.15)

Employer engaged in self-storage business stated claim against competitor, for receipt of alleged trade secrets taken by former employees from employer's computers in violation of Computer Fraud and Abuse Act (CFAA), by claiming that former employees participated in dishonest methods, even though common law elements of fraud were not satisfied. 18 U.S.C.A. § 1030(a)(4).

[6] Telecommunications 372 1342

372 Telecommunications
372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; Unauthorized Access or Transmission. Most Cited Cases
(Formerly 372k461.15)

Provision of Computer Fraud and Abuse Act (CFAA), penalizing unauthorized access to computers resulting in damage, applied to employees of employer owning computers in question as well as outsiders. 18 U.S.C.A. § 1030(a)(5)(C).

[7] Telecommunications 372 1342

372 Telecommunications

372VIII Computer Communications
372k1339 Civil Liabilities; Illegal or Improper Purposes
372k1342 k. Fraud; Unauthorized Access or Transmission. Most Cited Cases
(Formerly 372k461.15)

Employer engaged in self-storage business stated claim against competitor, for alleged damage to its computers arising from competitor's alleged receipt from former employees of trade secret information obtained in violation of Computer Fraud and Abuse Act (CFAA), despite claim that no damage occurred since information remained intact within computers; employer suffered loss in form of expenses incurred in modifying computers to preclude further data transfer. 18 U.S.C.A. § 1030(a)(5)(C).

Warren Joseph Rheaume,Roxanne L Spiegel, Foster Pepper & Shefelman, Seattle, WA, for Shurgard Storage Centers Inc, a Washington corporation, plaintiff.
Kevin Michael Paulich, Wolfstone, Panchot & Block, Seattle, WA, for Safeguard Self Storage Inc, a Louisiana corporation, defendant.

ORDER

ZILLY, District Judge.

INTRODUCTION

Shurgard Storage Centers, Inc. (plaintiff) and Safeguard Self Storage, Inc. (defendant) are competitors in the self-storage business. The plaintiff alleges that the defendant embarked on a systematic scheme to hire away key employees from the plaintiff for the purpose of obtaining the plaintiff's trade secrets. The plaintiff also alleges that some of these employees, while still working for the plaintiff, used the plaintiff's computers to send trade secrets to the defendant via e-mail. The plaintiff's complaint alleges misappropriation of trade secrets, conversion, unfair competition, violations of the Computer Fraud and Abuse Act (CFAA), tortious interference with a business expectancy, and seeks injunctive relief and damages. The defendant has moved to dismiss the CFAA claim pursuant to Fed.R.Civ.P. 12(b)(6), docket no. 7 no. 7[FN1] The Court now DENIES the defendant's motion to dismiss the CFAA claim for the reasons set forth in this order.

FN1. In a previous Minute Order, docket no. 16, the Court dismissed the unfair competition claim and denied the motion to dismiss the tortious interference claim.

MOTION TO DISMISS STANDARD

When considering a motion to dismiss under 12(b)(6), a court must accept all allegations in the complaint as true and make all reasonable inferences in favor of the plaintiff. *See Scheuer v. Rhodes,* 416 U.S. 232, 236, 94 S.Ct. 1683, 40 L.Ed.2d 90 (1974). A motion to dismiss may be granted when "it appears beyond a doubt that the plaintiff can prove no set of facts in support of his claim which would entitle him to relief." *Conley v. Gibson,* 355 U.S. 41, 45-46, 78 S.Ct. 99, 2 L.Ed.2d 80 (1957). "Nonetheless, conclusory allegations without more are insufficient to defeat a motion to dismiss for failure to state a claim." *Pillsbury, Madison & Sutro v. Lerner,* 31 F.3d 924, 928 (9th Cir.1994) (citations omitted).

FACTS

The plaintiff alleges the following facts which the Court accepts as true for the purposes of this motion. The plaintiff is the industry leader in full and self-service storage facilities in both the United States and Europe. The plaintiff's growth in the last 25 years is primarily due to the development and construction of top-quality storage centers in "high barrier to entry" ***1123** markets. Pursuant to this strategy, the plaintiff has developed a sophisticated system of

creating market plans, identifying appropriate development sites, and evaluating whether a site will provide a high return on an investment. The plaintiff invests significant resources in creating a marketing team to carry out these tasks for each potential market. These teams become familiar with the market, identify potential acquisition sites, and develop relationships with brokers and sellers in the market so that the plaintiff has the best opportunity to acquire a preferred site.

The defendant began self-storage operations in 1997. The defendant is a direct competitor of the plaintiff and develops self-storage facilities in the United States and abroad.

In late 1999, the defendant approached Eric Leland, a Regional Development Manager for the plaintiff, and offered him employment with the defendant. Because of his position with the plaintiff, Mr. Leland had full access to the plaintiff's confidential business plans, expansion plans, and other trade secrets. While still employed by the plaintiff, but acting as an agent for the defendant, Mr. Leland sent e-mails to the defendant containing various trade secrets and proprietary information belonging to the plaintiff. Mr. Leland did this without the plaintiff's knowledge or approval. Mr. Leland was later hired by the defendant in October 1999, and he has continued to give the defendant proprietary information belonging to the plaintiff. The defendant has hired away other employees of the plaintiff who have intimate knowledge of the plaintiff's business models and practices, and the defendant continues to recruit employees of the plaintiff.

DISCUSSION

The motion to dismiss raises challenging issues regarding the scope of a civil claim under a criminal statute, the Computer Fraud and Abuse Act, 18 U.S.C. § 1030.[FN2] In its complaint, the plaintiff asserts that it is entitled to relief under the CFAA. In its opposition to the motion to dismiss, the plaintiff specifies that its claim is sufficient under 18 U.S.C. §§ 1030(a)(2)(C), 1030(a)(4), and 1030(a)(5)(C).

> FN2. Though other cases have dealt with the CFAA, none have dealt with the precise issues presented by this case. *See, e.g., United States v. Czubinski,* 106 F.3d 1069, 1078-79 (1st Cir.1997) (discussing the application of the CFAA in a criminal context to a person convicted for browsing through IRS files but not sending or obtaining that information); *United States v. Sablan,* 92 F.3d 865, 867-69 (9th Cir.1996) (interpreting the mens rea requirements of the CFAA in a criminal context); *YourNetDating, Inc. v. Mitchell,* 88 F.Supp.2d 870, 872 (N.D.Ill.2000) (granting a temporary retraining order when a former employee hacked into his former employer's computers to send customers to a pornographic Internet site); *Edge v. Professional Claims Bureau, Inc.,* 64 F.Supp.2d 115, 119 (E.D.N.Y.1999) (granting summary judgment to defendant who accessed a credit report for a permissible purpose); *Shaw v. Toshiba America Information Systems, Inc.,* 91 F.Supp.2d 926, 932-37 (construing § 1030(a)(5)(A) of the CFAA); *America Online, Inc. v. LCGM, Inc.,* 46 F.Supp.2d 444, 450-51 (E.D.Va.1998) (holding that massive e-mail transmissions, or "spam," sent by customers of the plaintiff were sent without authorization because the e-mails violated the terms of service).

A. Statutory Interpretation

[1] As a preliminary matter, the Court must determine the appropriate method by which to interpret the statute. The defendant, citing *United States v. Flores-Garcia,* 198 F.3d 1119, 1121 (9th Cir.2000), asserts that a court should ascertain a statute's plain meaning by examining the statute's language as well as its object and policy. The plaintiff, however, proposes a different standard: "In interpreting a statute we must examine its language. If the statute is clear and unambiguous, that is the end of the matter. There is no need to look beyond the plain meaning in order to derive the 'purpose' of the statute." *Burton v. Stevedoring Servs. of America,* 196 F.3d 1070, 1072 (9th Cir.1999) (quotation marks omitted).

***1124** The standard articulated in *Flores-Garcia,* the case cited by the defendant, only applies when the statute is ambiguous. In *Flores-Garcia,* the court construed the meaning of a statute; in that case whether "knowingly" in the phrase "knowingly aided and assisted any alien" applied to the term "alien." *See Flores-Garcia,* 198 F.3d at 1121. The court attempted to find the meaning because the statute was unclear. *See id.* The *Burton* standard is the correct standard for statutory interpretation, and the unambiguous meaning of a statute should be the first and final inquiry unless it would lead to an absurd result. *See Burton,* 196 F.3d at 1072.

B. Does the plaintiff state a claim under 18 U.S.C. § 1030(a)(2)(C)?

Under § 1030(a)(2)(C), "[w]hoever ... intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains ... information from any protected computer if the conduct involved an interstate or foreign communication ... shall be punished" as provided in section (c) of the statute. 18 U.S.C. § 1030(a)(2)(C). Additionally, § 1030(g) 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 to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).[FN3] A "protected computer" means a computer "which is used in interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). "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." 18 U.S.C. § 1030(e)(6).

FN3. The 1994 amendments to the CFAA added this private cause of action. *See* H.R.Conf.Rep. No. 103-711, at Section 290001 (1994).

The defendant contends the plaintiff's complaint does not state a claim for relief under 18 U.S.C. § 1030(a)(2)(C) for two reasons. First, the defendant asserts that the plaintiff has not alleged that the employees in question accessed the trade secrets without authorization. Second, the defendant argues that the plaintiff has not alleged facts showing that the alleged behavior by the defendant impacts the national economy.

i. Did Plaintiff allege that its former employees were without authorization or that they exceeded authorized access?

[2] The defendant's first ground for challenging the plaintiff's claim under § 1030(a)(2)(C) is that the plaintiff has not alleged that its former employees did not have authorized access to the information in question. The defendant notes that the plaintiff alleged that Mr. Leland had full access to all the information allegedly transferred to the defendant. Accordingly, the defendant argues that the plaintiff cannot maintain an action under § 1030(a)(2)(C) because it has not alleged that anyone accessed its computers without authorization or exceeded authorized access to those computers.

The plaintiff responds by arguing that the authorization for its former employees ended when the employees began acting as agents for the defendant. The plaintiff cites to the Restatement (Second) of Agency § 112 (1958) and argues that when Mr. Leland or other former employees used the plaintiff's computers and information on those computers in an improper way they were "without authorization."

In *United States v. Galindo,* 871 F.2d 99 (9th Cir.1989), an employee of a jewelry store was authorized to pick up mail for the store. *See Galindo,* 871 F.2d at 100. The employee was convicted of stealing the mail. *See id.* In a possible attempt to conceal her actual receipt of the mail, the employee forged a signature when she received the mail. *See id.* at 101. The court held that the employee was not an agent of ***1125** the jewelry store when the employee used fraud to obtain the mail. *See id.* Relying on *Galindo,* the plaintiff argues that its former employees were not its agents when they accessed the computers to send trade secrets to the defendant.

Under the Restatement (Second) of Agency, relied upon by the *Galindo* court:

Unless otherwise agreed, the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal.

Restatement (Second) of Agency § 112 (1958). Under this rule, the authority of the plaintiff's former employees ended when they allegedly became agents of the defendant. Therefore, for the purposes of this 12(b)(6) motion, they lost their authorization and were "without authorization" when they allegedly obtained and sent the proprietary information to the defendant via e-mail. The plaintiff has stated a claim under 18 U.S.C. § 1030(a)(2)(C). FN4 *See United States v. Morris*, 928 F.2d 504, 510 (2d Cir.1991) (holding that a computer user, with authorized access to a computer and its programs, was without authorization when he used the programs in an unauthorized way).

FN4. Since the plaintiff has sufficiently alleged that the former employees were without authorization, the Court need not examine whether the employees exceeded their authorized access.

ii. Did the plaintiff have to allege that the violation of 18 U.S.C. § 1030(a)(2)(C) affected the national economy?

[3] The defendant's second argument challenging the plaintiff's claim under § 1030(a)(2)(C), as well as its other claims under the CFAA, is that the CFAA was only intended to protect information in large businesses where information, if released or stolen, could affect the public. The defendant maintains that since information from the storage business is not of the type that the CFAA was intended to protect (as opposed to the transportation or power-supply industries), the CFAA does not apply.

Nowhere in language of § 1030(a)(2)(C) is the scope limited to entities with broad privacy repercussions. The statute simply prohibits the obtaining of information from "*any* protected computer if the conduct involved an interstate or foreign communication." 18 U.S.C. § 1030(a)(2)(C) (emphasis added). According to the statute, a protected computer is a computer used in interstate or foreign commerce. *See* 18 U.S.C. § 1030(e)(2)(B). This language is unambiguous. There is no reasonable implication in any of these terms that suggests only the computers of certain industries are protected. Therefore, the defendant's argument on this issue is unpersuasive.

C. Does the plaintiff state a claim under 18 U.S.C. § 1030(a)(4)?

[4][5] A person violates 18 U.S.C. § 1030(a)(4) if he or she:
knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5, 000 in any 1-year period.

18 U.S.C. § 1030(a)(4). The only element disputed by the defendant under § 1030(a)(4) that is not present under § 1030(a)(2)(C) is the intent to defraud. The plaintiff argues for a broad definition of "defraud" in this context, stating fraud is simply "wronging one in his property rights by dishonest methods or schemes." Plaintiff's Memorandum in Opposition, docket no. 11, at 9 (citing *McNally v. United States*, 483 U.S. 350, 358, 107 S.Ct. 2875, 97 L.Ed.2d 292 (1987); *Hammerschmidt v. United States*, 265 U.S. 182, 188, 44 S.Ct. 511, 68 L.Ed. 968 (1924)). Morever, the plaintiff relies on *United* ****1126*** *States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir.1997), for the proposition that this section of the CFAA's use of "fraud" simply means wrongdoing and not proof of the common law elements of fraud. This is the proper standard for fraud in this context, and construing the complaint in the light most favorable to the plaintiff, the complaint alleges that the defendant participated in dishonest methods to obtain the plaintiff's secret information. Therefore, the plaintiff has stated a claim upon which relief can be granted under 18 U.S.C. § 1030(a)(4).

D. Does the plaintiff state a claim under 18 U.S.C. § 1030(a)(5)(C)?

Under 18 U.S.C. § 1030(a)(5)(C), "[w]hoever ... intentionally accesses a protected computer without authorization,

and as a result of such conduct, causes damage" violates the CFAA. 18 U.S.C. § 1030(a)(5)(C). The only new issue under this portion of the statute is whether the plaintiff has alleged that "damage" occurred. "The term 'damage' means any impairment to the integrity or availability of data, a program, a system, or information, that ... causes loss aggregating at least $5,000 in value during any 1-year period to one or more individuals...." 18 U.S.C. § 1030(e)(8)(A).

[6] The defendant raises two objections to this claim. First, the defendant asserts that the legislative history of this section of the CFAA shows that it is only intended to apply to "outsiders," and thus would not apply to employees. However, there is no ambiguity in the statute as to when a party is liable, ("*Whoever* ... intentionally accesses....") so this argument lacks merit. *See* 18 U.S.C. § 1030(a)(5)(C).

[7] Second, the defendant argues that the plaintiff has not pled that it incurred "damage" as defined in the statute. Specifically, the defendant argues that the alleged loss of information by the plaintiff is not "damage" under the statute. The statute says damage is "*any impairment* to the integrity ... of data ... or information." 18 U.S.C. § 1030(e)(8)(A) (emphasis added). The unambiguous meaning of "any" clearly demonstrates that the statute is meant to apply to "any" impairment to the integrity of data. However, the word "integrity" is ambiguous in this context. Webster's New International Dictionary (3d ed.1993), defines "integrity" as, "an unimpaired or unmarred condition: entire correspondence with an original condition." The word "integrity" in the context of data necessarily contemplates maintaining the data in a protected state. Because the term may be ambiguous, the Court examines the legislative history to determine if "integrity" and thus "damage" could include the alleged access and disclosure of trade secrets in this case.

The term "damage" was addressed in the Senate Report regarding the 1996 amendments to the CFAA:
The 1994 amendment required both "damage" and "loss," but it is not always clear what constitutes "damage." For example, intruders often alter existing log-on programs so that user passwords are copied to a file which the hackers can retrieve later. After retrieving the newly created password file, the intruder restores the altered log-on file to its original condition. Arguably, in such a situation, neither the computer nor its information is damaged. Nonetheless, this conduct 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.
The bill therefore defines "damage" in new subsection 1030(e)(8), with a focus on the harm that the law seeks to prevent.

S.Rep. No. 104-357, at 11 (1996). This example given in the report is analogous to ***1127** the case before the Court. The "damage" and thus violation to the "integrity" that was caused in the example is the accumulation of passwords and subsequent corrective measures the rightful computer owner must take to prevent the infiltration and gathering of confidential information. Similarly, in this case, the defendant allegedly infiltrated the plaintiff's computer network, albeit through different means than in the example, and collected and disseminated confidential information. In both cases no data was physically changed or erased, but in both cases an impairment of its integrity occurred. From the legislative history it is clear that the meaning of "integrity" and thus "damage" apply to the alleged acts of the defendant in this case and thus the plaintiff has stated a claim under 18 U.S.C. § 1030(a)(5)(C).

E. The Legislative History of the CFAA Supports the Plaintiff's Claim in This Case.

Although the Court concludes that the plaintiff has stated a claim under the CFAA, this Court is mindful of its obligation to construe statutes so as to avoid "absurd" results. *See Burton,* 196 F.3d at 1072. Though the defendant's arguments about the legislative history and intent of the CFAA go to the meaning of what this Court finds to be unambiguous language, save for "integrity," those same arguments can be construed as relevant to, for lack of a better

term, an "absurdity inquiry." Thus, considering the novelty of the legal issues presented to the Court, an in-depth analysis of the legislative history of the CFAA is appropriate.

The core of the defendant's arguments concerning legislative intent is that the CFAA was not meant to apply to the kind of factual situation presented in this case. Instead, the defendant maintains the CFAA is limited to those industries whose computers contain vast amounts of information, which if released, could significantly affect privacy interests in the public at large. The defendant also maintains the CFAA is limited to "outsiders" or "hackers," and not "insiders" (employees). Though the original scope of the CFAA was limited to the concerns addressed by the defendant, its subsequent amendments have broadened the scope sufficiently to cover the behavior alleged in this case.

The first version of the CFAA was passed in 1984. *See* S.Rep. No. 99-432, at 3 (1986). This first bill was directed at protecting classified information on government computers as well as protecting financial records and credit information on government and financial institution computers. *See id.* In 1986, the CFAA was amended to "provide additional penalties for fraud and related activities in connection with access devices and computers." *Id.* at 1. Specifically, the 1986 amendments added protection for "federal interest computers:"

Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area. It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is left uncovered. The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature.

Id. at 4. Thus, the original version of the CFAA did not intend to enact sweeping federal jurisdiction. However, the CFAA was intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature.

As for the scope of the CFAA after the 1986 amendments, there is language in the Senate Report that favors both the plaintiff's and the defendant's contentions. Examples of language helpful to the plaintiff are: "The Judiciary Committee's concern ***1128** about these problems has become more pronounced as computers proliferate in businesses and homes across the nation...." *Id.* at 2; "This technological explosion has made the computer a mainstay ... to American businesses ... it has also created a new type of criminal...." *Id.;*

Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement *or even the illegal conversion of trade secrets.*

Id. at 14 (citation omitted and emphasis added).

However, other language tends to support the defendant's contention that the CFAA has a narrow scope: "[programs should be implemented that] deflate the myth that computer crimes are glamourous, harmless pranks." *Id.* at 3; "The premise of 18 U.S.C. 1030(a)(2) will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions." *Id.* at 6; "The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers ... he could be prosecuted under [1030(a)(5)] ... By precluding liability in purely 'insider' cases such as these...." *Id.* at 7-8.

The CFAA was amended in 1996, and the phrase "protected computer" was added in place of "federal interest computer." The Senate Report on these amendments demonstrates the broad scope of this phrase. *See* S.Rep. No. 104-357, at 3 (1996) ("[The CFAA is strengthened] by closing gaps in the law to protect better the confidentiality,

integrity, and security of computer data and networks."); *Id.* at 4; ("The privacy protection coverage of the statute has two significant gaps. First, omitted from the statute's coverage is information on *any civilian* or State and local government computers, since the prohibition on unauthorized computer access to obtain non classified information extends only to the Federal Government when the perpetrator is an outsider.") (emphasis added); *Id.* at 5; ("[The CFAA] facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology. As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the [CFAA] is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime.") *Id.*

Finally, in what is dispositive of the scope of the CFAA, the report states:
The proposed subsection 1030(a)(2)(C) is intended to protect against the interstate or foreign theft of information by computer.... This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected. *In instances where the information stolen is also copyrighted, the theft may implicate certain rights under the copyright laws. The crux of the offense under subsection 1030(a)(2)(C), however, is the abuse of a computer to obtain the information.*
....
... Those who improperly use computers to obtain other types of information-such as financial records, nonclassified Government information, and information of nominal value *from private individuals or companies* -face only misdemeanor penalties, *unless the information is used for commercial advantage,* private financial gain or to commit any criminal *or tortious act.*
For example, individuals who intentionally break into, *or abuse their authority****1129*** *to use,* a computer and thereby obtain information of minimal value of $5,000 or less, would be subject to a misdemeanor penalty. The crime becomes a felony if the offense was committed for *purposes of commercial advantage* or private financial gain, for the purposes of *committing any criminal or tortious act in violation* ... of the laws of the United States or of any State, or if the value of the information obtained exceeds $5,000.

Id. at 7-8 (emphasis added). This legislative history, although in reference § 1030(a)(2), demonstrates the broad meaning and intended scope of the terms "protected computer" and "without authorization" that are also used in the other relevant sections. The report recognizes that someone could be liable under § 1030(a)(2)(C) where intellectual property rights are involved. Finally, the report states the statute is intended to punish those who illegally use computers for commercial advantage. In sum, this passage makes clear that the CFAA was intended to encompass actions such as those allegedly undertaken by the present defendant. The legislative history of the CFAA comports with the plain meaning of the statute.

CONCLUSION

For the reasons stated above, the defendant's motion to dismiss the Computer Fraud and Abuse Act claim is DENIED.

IT IS SO ORDERED.

W.D.Wash.,2000.
Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.
119 F.Supp.2d 1121, 174 A.L.R. Fed. 655

END OF DOCUMENT