EXHIBIT B

LEXSEE 2006 US DIST LEXIS 53108

LOCKHEED MARTIN CORPORATION, Plaintiff, -vs- KEVIN SPEED, STEVE FLEMING, PATRICK ST. ROMAIN, L-3 COMMUNICATIONS CORPORATION, & MEDIATECH, INC., Defendants. L-3 COMMUNICATIONS CORPORATION, Third Party Plaintiff, vs. JACK KELLY, THOMAS DORSEY, MICHAEL HOMAN, and THOMAS HULL, Third Party Defendants.

Case No. 6:05-cv-1580-Orl-31KRS

UNITED STATES DISTRICT COURT FOR THE MIDDLE DISTRICT OF FLORIDA, ORLANDO DIVISION

2006 U.S. Dist. LEXIS 53108; 81 U.S.P.Q.2D (BNA) 1669; 19 Fla. L. Weekly Fed. D 939

August 1, 2006, Decided
August 1, 2006, Filed

SUBSEQUENT HISTORY: Later proceeding at Lockheed Martin Corp. v. L-3 Communs. Corp., 2007 U.S. Dist. LEXIS 51853 (M.D. Fla., July 18, 2007)

COUNSEL: [*1] For Lockheed Martin Corporation, a Maryland Corporation, Plaintiff: Creighton R. Magid, Nathaniel H. Akerman, Dorsey & Whitney LLP, Washington, DC; Kay L. Wolf, Lori R. Benton, M. Susan Sacco, Ford & Harrison LLP, Orlando, FL.

For Kevin Speed, Steve Fleming, Defendants: William Cooper Guerrant, Jr., Hill, Ward & Henderson, P.A., Tampa, FL.

For Patrick St. Romain, Defendant: Benjamin H. Hill, III, William Cooper Guerrant, Jr., Hill, Ward & Henderson, P.A., Tampa, FL.

For L-3 Communications Corporation, Defendant: Christine M. Fitzgerald, Jason Habinsky, Jeffrey R. Coleman, Ned H. Bassen, Nicolas Swerdloff, Lisa M. Pisciotta, Hughes, Hubbard & Reed, New York, NY; David B. King, Thomas A. Zehnder, King, Blackwell, Downs & Zehnder, P.A., Orlando, FL; Juan J. Farach, Jr., Shubin & Bass, P.A., Miami, FL.

For Mediatech, Inc., a Delaware corporation, Defendant: K. Judith Lane, Smith, Hood, Perkins, Loucks, Stout, Daytona Beach, FL.

For Jack Kelly, Thomas Dorsey, Michael Homan, Thomas Hull, Third Party Defendants: Kevin K. Ross, Michael V. Elsberry, Terry C. Young, Lowndes, Drosdick, Doster, Kantor & Reed, P.A., Orlando, FL.

JUDGES: GREGORY A. PRESNELL, UNITED STATES DISTRICT [*2] JUDGE.

OPINION BY: GREGORY A. PRESNELL

OPINION

ORDER

This matter comes before the Court upon the Motion to Dismiss by Defendants Kevin Speed ("Speed") and Steve Fleming ("Fleming") (Doc. 53), to which Plaintiff Lockheed Martin Corporation ("Lockheed" or "the company") responded in opposition (Doc. 71), and the Motion to Dismiss by Patrick St. Romain ("St. Romain") (Doc. 68), to which Lockheed responded in opposition (Doc. 75). Lockheed alleges that three of its former employees accessed Lockheed computers, copied proprietary information, and delivered trade secrets to Defendant L-3 Communications Corporation ("L-3") in violation of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. For the reasons herein stated, the Court grants the Motions to Dismiss.

I. Background

Lockheed and L-3, rivals in the defense and aerospace industries, made competing bids on the United States Air Force ("USAF") contract known as the Aircrew Training and Rehearsal Support contract ("ATARS I"). USAF ultimately awarded ATARS I to Lockheed in

June 2000. ATARS I is scheduled to terminate on September 30, 2006, and the contract for ATARS II, an extension of ATARS I valued [*3] at one billion dollars, is scheduled to be awarded in the third quarter of 2006. Lockheed alleges that L-3, in an effort to gain an unfair advantage in its bid for ATARS II, conspired with three Lockheed employees -- Speed, Fleming, and St. Romain (collectively, "the Employees") -- to wrongfully obtain ATARS trade secrets. The particular allegations against the Employees are as follows:

(1) Speed, a Lockheed program manager, held ultimate responsibility for ATARS I. (Compl. PP 24-25.) Speed had "complete access to ATARS confidential and proprietary and trade secret protected information." (Compl. P 24.) Speed resigned from Lockheed on March 4, 2005 and thereafter became employed with L-3. [1] Shortly before resigning, Speed allegedly copied 200 documents (forty-four of which related to ATARS) from his Lockheed computer by burning them onto a compact disc ("CD"). (Compl. P 50(a).)

1 After resigning, Speed joined Defendant Mediatech, a Lockheed subcontractor assigned to ATARS I, which allegedly acted as a hiring front for L-3. The hiring front was designed to mask Speed's role in developing a competitive ATARS II bid for L-3. While the Complaint is unclear as to the exact relationship between Mediatech and L-3, Speed admits that he is currently employed by L-3. (Doc. 53 at 1.)

[*4] (2) Fleming, a Lockheed senior manager, "had unrestricted access to [Lockheed's] shared network drives, including data folders containing ATARS confidential and proprietary and trade secret protected information." (Compl. P 27.) Fleming resigned from Lockheed on March 18, 2005 and, like Speed, became employed with L-3. Shortly before resigning, Fleming allegedly: (a) burned 262 files onto a CD; (b) synchronized nine Lockheed data files to his BlackBerry personal digital assistant ("PDA"); and (c) on his last day of work, copied sixty-three data files onto two CDs, including "the most recent and detailed ATARS program review." (Compl. P 50(b)-(d).)

(3) St. Romain, a Lockheed site manager, "had access to the confidential and proprietary and trade secret protected financial, technical and strategic data concerning [ATARS I]." (Compl. P 28.) St. Romain resigned from Lockheed on March 25, 2005. On St. Romain's last day of employment, he allegedly "synchronized his [Lockheed] computer to a Dell PDA, thereby removing [Lockheed] documents to his PDA." (Compl. P 50(e).)

Based on these allegations relating to the Employees, Lockheed asserts that this Court has federal question subject [*5] matter jurisdiction pursuant to the CFAA.

II. Standard of Review

In ruling on a motion to dismiss, this Court must view the complaint in the light most favorable to the Plaintiff. *Scheuer v. Rhodes*, 416 U.S. 232, 236, 94 S. Ct. 1683, 40 L. Ed. 2d 90 (1974), and must limit its consideration to the pleadings and any exhibits attached thereto. FED. R. CIV. P. 10(c); *see also GSW, Inc. v. Long County, Ga.*, 999 F.2d 1508, 1510 (11th Cir. 1993). The Court will liberally construe the complaint's allegations in the Plaintiff's favor, *Jenkins v. McKeithen*, 395 U.S. 411, 421, 89 S. Ct. 1843, 23 L. Ed. 2d 404 (1969), and will not dismiss a complaint for failure to state a claim unless it appears beyond a doubt that the Plaintiff cannot prove any set of facts that support a claim for relief. *Conley v. Gibson*, 355 U.S. 41, 45-46, 78 S. Ct. 99, 2 L. Ed. 2d 80 (1957). In ruling on a motion to dismiss, "conclusory allegations, unwarranted factual deductions or legal conclusions masquerading as facts will not prevent dismissal." *Davila v. Delta Air Lines, Inc.*, 326 F.3d 1183, 1185 (11th Cir. 2003).

In reviewing a complaint on a motion to dismiss under Federal Rule of Civil Procedure ("Rule") 12(b)(6) [*6] , the rule to be applied is that, "courts must be mindful that the Federal Rules [of Civil Procedure] require only that the complaint contain a short and plain statement of the claim showing that the pleader is entitled to relief." *United States v. Baxter Int'l, Inc.*, 345 F.3d 866, 880 (11th Cir. 2003) (*citing* FED. R. CIV. P. 8(a)). This is a liberal pleading requirement, one that does not require a plaintiff to plead with particularity every element of a cause of action. *Roe v. Aware Woman Ctr. for Choice, Inc.*, 253 F.3d 678, 683 (11th Cir. 2001). Instead, the complaint need only "contain either direct or inferential allegations respecting all the material elements necessary to sustain a recovery under some viable legal theory." *Id.* (internal citation and quotation omitted). "A complaint need not specify in detail the precise theory giving rise to recovery. All that is required is that the defendant be on notice as to the claim being asserted against him and the grounds on which it rests." *Sams v. United Food and Commercial Workers Int'l Union*, 866 F.2d 1380, 1384 (11th Cir. 1989).

III. [*7] Discussion

A. Lockheed Adequately Alleges Injury Under § 1030(g)

The CFAA, primarily a criminal statute, provides a civil cause of action in § 1030(g):

> Any 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. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

18 U.S.C. § 1030(g)(2002) (emphasis added).

Thus, before reaching the merits of the alleged violations, the CFAA's private cause of action sets forth a two-part [*8] injury requirement, where a plaintiff must: (1) suffer a root injury of damage or loss; and (2) suffer one of five operatively-substantial effects in subsection (a)(5)(B)(i)-(v).

Subsection (g) first requires civil litigants to suffer "damage" [2] and/or "loss." [3] The primary injury that Lockheed alleges is the loss of its trade secrets. As this Court has held before, the alleged wrongful taking of trade secrets does not, by itself, fit within the grouping of "damage" or "loss." *Resdev, LLC v. Lot Builders Ass'n*, 2005 U.S. Dist. LEXIS 19099, No. 6:04-CV-1374, 2005 WL 1924743, at * 4 (M.D. Fla. Aug. 10, 2005) ("ResDev's position fails to acknowledge that allegedly ill-gotten revenues from a trade secret are neither a 'but-for' nor a proximate consequence of 'damage,' and nor do they fit within the grouping of 'loss.'"). Lockheed, however, also alleges that the unauthorized actions of the Employees caused Lockheed to incur costs in "responding to the . . . offenses" and in "conducting a damage assessment." (Compl. PP 70, 75, 79.) These costs are explicitly identified in the CFAA's definition of "loss." [4] Lockheed, therefore, sufficiently alleges loss pursuant to § 1030(g).

2 The CFAA defines "damage" as: "any impairment to the integrity or availability of data, a program, a system, or information[.]" 18 U.S.C. § 1030(e)(8).

[*9]

3 The CFAA defines "loss" as follows:

> 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 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).

4 *See, supra*, note 3.

Subsection (g) also requires civil litigants to allege one of the following five effects set forth in § 1030(a)(5)(B):

> (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 [*10] 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[.]

18 U.S.C. § 1030(a)(5)(B).

For each of the alleged violations of the CFAA, Lockheed invokes § 1030(a)(5)(B)(i), alleging that each violation "caused loss of $ 5,000 in value in the aggregate, including the cost of [Lockheed] responding to the . . . offense and conducting a damage assessment." (Compl. PP 70, 75, 79.) While the Complaint does not explicitly state that the only alleged losses available under the statute (responding to the offense and subsequent

damage assessment) amounted to $ 5,000, the Court finds that the liberal pleading requirements at this motion-to-dismiss stage do not require such particularity.

Thus, Lockheed sufficiently alleges a § 1030(a)(5)(B)(i) loss pursuant to § 1030(g). The Court now turns to the three alleged violations of the CFAA.

B. Lockheed Fails to Adequately Allege Violations of § 1030(a)(4)

Count I alleges that Defendants violated § 1030(a)(4) of the CFAA, which provides that whoever [*11]

> 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 Employees assert that the they did not access "without authorization" or "exceed[] authorized access" in violation of the statute because Lockheed permitted the Employees, as a function of their respective positions, to access the precise information at issue. Lockheed does not disagree that the Employees were permitted access to the information; instead, Lockheed contends that the Employees' interpretation of "authorization" is too narrow, arguing that the term is properly interpreted in light of the Second Restatement of Agency. Lockheed cites to the Restatment for the proposition that "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interest or if he is otherwise guilty of a serious breach [*12] of loyalty to the principal." Restatement (Second) of Agency § 112 (1958) (hereinafter "Restatement § 112"). Because the Employees accessed information with intent to steal and deliver to a competitor, Lockheed argues, the Employees acquired adverse interests, terminated their agency authority, and therefore accessed "without authorization." In support of this reliance on Restatement § 112, Lockheed cites two cases: *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006) and *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121, 1125 (W.D. Wash. 2000).

The Court is not persuaded by the analysis in either *Citrin* or *Shurgard*. Both cases rely heavily on extrinsic materials, particularly the Second Restatement of Agency (*Citrin* and *Shurgard*) and legislative history (*Shurgard*), to derive the meaning of "without authorization." Because the plain language of the statute is sufficient to interpret the disputed terms, this Court need not resort to extrinsic materials. In the Eleventh Circuit, there is a presumption that, in drafting a statute, [*13] "Congress said what it meant and meant what it said." *Shotz v. City of Plantation, Florida*, 344 F.3d 1161, 1167 (11th Cir. 2003). "The first rule in statutory construction is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute." *Id.* (internal quotation omitted). Words carry their ordinary meaning, unless otherwise defined. *Am. Bankers Ins. Group v. United States*, 408 F.3d 1328, 1332 (11th Cir. 2005). If Congress has used clear statutory language, a court need not consider extrinsic materials, such as legislative history, and certainly should not derive from such materials a meaning that is inconsistent with the statute's plain meaning. *Shotz*, 344 F.3d at 1167. Even where Congress has used statutory language that is not entirely transparent, courts are to resort to canons of construction to determine "the meaning of a particular statutory provision by focusing on the broader, statutory context." *Id.* at 1167 (internal quotations omitted). There is one instance where extrinsic materials are permitted to define a term: when the statutory language either [*14] produces a clearly absurd result or presents a substantial ambiguity. *Id.* at 1167.

The term, "without authorization," is not defined by the CFAA. Nonetheless, "authorization" is commonly understood as "[t]he act of conferring authority; permission." *The American Heritage Dictionary*, 89 (1976). On the other hand, the CFAA defines "exceeds authorized access" as follows: "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). The CFAA targets access "without authorization" in six separate offenses (§§ 1030(a)(1), (a)(2), (a)(3), (a)(4), (a)(5)(A)(ii), (a)(5)(A)(iii)), only three of which also reach persons "exceeding authorized access" (§§ 1030(a)(1), (a)(2), (a)(4)). Thus, it is plain from the outset that Congress singled out two groups of accessers, those "without authorization" (or those *below* authorization, meaning those having no permission to access whatsoever - typically outsiders, as well as insiders that are not permitted *any* computer access) and those exceeding authorization (or those [*15] *above* authorization, meaning those that go beyond the permitted access granted to them - typically insiders exceeding whatever access is permitted to them).

By applying the plain meaning of the statutory terms to the facts of this case, it is clear that the Employees accessed *with* authorization, did not exceed their authorization, and thus did not violate § 1030(a)(4). The analy-

sis is not a difficult one. Because Lockheed permitted the Employees to access the company computer, they were not without authorization. Further, because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access. The Employees fit within the very group that Congress chose not to reach, *i.e.*, those with access authorization. It follows that § 1030(a)(4) cannot reach them. The gist of Lockheed's complaint is aimed not so much at the Employees' improper access of the ATARS information, but rather at the Employees' actions subsequent to their accessing the information. As much as Lockheed might wish it to be so, § 1030(a)(4) does not reach the actions alleged in the Complaint. *See Int'l Ass'n of Machinists & Aero. Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 498 (D. Md. 2005) [*16] ("Thus, to the extent that Werner-Masuda may have breached the Registration Agreement by *using* the information obtained for purposes contrary to the policies established by the IAM Constitution, it does not follow, as a matter of law, that she was not authorized to access the information, or that she did so in excess of her authorization in violation of the . . . CFAA."). Where Congress targeted actions other than access, such as "communication" or "delivery" of confidential information, it explicitly provided such language. *See* 18 U.S.C. § 1030(a)(1).

1. Disagreement with Citrin and Shurgard

The Court acknowledges that the Seventh Circuit in *Citrin*, following *Shurgard*, came to a different conclusion with respect to the application of "without authorization." In *Citrin*, an employee accessed his company laptop and deleted the data in it by using a secure-erasure program, which rendered the deleted material irretrievable. *Citrin*, 440 F.3d at 419. The employee's access was "without authorization" at the point "he resolved to destroy files that incriminated himself and other files that were also the property of his employer, [*17] in violation of the duty of loyalty that agency law imposes on an employee." *Id.* at 420 (relying on *Shurgard* and Restatement § 112). To the extent *Citrin* holds that an employee accesses "without authorization" at the moment the employee acquires a subjectively adverse interest to the employer, the Court respectfully disagrees.

First, by reading Restatement § 112 legalese into the meaning of "without authorization," the term becomes equipped with a breadth that effectively shaves "exceeds authorized access" down to a mere sliver of what its plain meaning suggests. *Citrin's* use of "without authorization" appears to cover anyone without authorization to begin with (*e.g.*, outsider) or an agent that terminates his authority, including the acquiring of adverse interests. As for "exceeds authorized access" *Citrin* used the following example to illustrate the "paper thin" range that it covers on its own:

> [F]or example, the former employee of a travel agent, in violation of his confidentiality agreement with his former employer, used confidential information that he had obtained as an employee to create a program that enabled his new travel company [*18] to obtain information from his former employer's website that he could not have obtained as efficiently without the use of that confidential information. The website was open to the public, so he was authorized to use it, but he exceeded his authorization by using confidential information to obtain better access than other members of the public. [5]

Citrin, 440 F.3d at 420.

> 5 Here, *Citrin* was drawing on the circumstances in *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001).

Thus, it appears that *Citrin* relegates the work performed by "exceeds authorized access" to those outside the principal-agent relationship *(e.g.*, ex-employee) that are permitted a minimum level of access to a computer, and then exceed that access. But this effectively turns the plain reading of the statutory definition of "exceeds authorized access" on its head. The statutory definition appears purposefully aimed at the company *insider* that already has [*19] authorization - not the non-agent *outsider* with public access to a company website. [6] [7] *Citrin* agreed that the CFAA's distinguished use of "without authorization" and "exceeds authorized access" resulted in "[m]uddying the picture some." *Id.* 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.

> 6 To reiterate, the CFAA defines "exceeds authorized access" as follows: "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).
>
> 7 Even assuming that "without authorization" is to be understood in light of Restatement § 112, the reach attributed to "exceeding authorized ac-

cess," would be less than what *Citrin* gives it credit for. In *Citrin's* example, an ex-employee accessing a company website open to the public was deemed to have a threshold level of authorization that was exceeded by using confidential information to gain better access. But the term "exceeding authorized access" presumes, it would seem, a threshold level of access that is not wide-open to the public. It is odd to consider any internet passerby to the company website as having company authorization. Thus, under a *Citrin* reading, the coverage exclusively belonging to "exceeding authorized access" would be even more limited, presumably applying to those permitted some type of access above what the common public is permitted, but who are non-agents (such as, perhaps, independent contractors and clients). A more straightforward application of the statute (under either the *Citrin* reading or this Court's reading) is to identify that ex-employee for what he is: an outsider who is simply *without* authorization -- not someone who is *exceeding* authorization.

[*20] Second, *Citrin* slays all three heads of wrongful access when Congress only aimed at two heads. *Citrin* reads: (1) "without authorization" as applying to (a) persons that have no authority to begin with, and (b) agents with authority that do something to terminate that authority (including acquire adverse interests); and (2) "exceeds authorization access" as applying to non-agents exceeding a permitted threshold level of access. But this reading of the two separate terms ("without authorization" and "exceeding authorization") forces them to cover the entire spectrum of wrongful access (wrongful accessers *without* authorization, wrongful accessers *with* authorization, and wrongful accessers *exceeding* authorization). To be sure, the *Citrin* reading has its allure - it gets all of the wrongful accessers. Yet if that was the intent of Congress, why would it bother with "authorization" at all? That is, why wouldn't § 1030(a)(4) simply read as follows: "whoever knowingly and with intent to defraud, accesses a protected computer, and by means of such conduct furthers the intended fraud and obtains anything of value . . . "? Section 1030(a)(4) without any reference to [*21] "authorization" reaches the same wrongful accessers as the *Citrin* reading with "authorization" in place. Yet, when Congress aimed at an entire spectrum of wrongdoers, it did just that; it omitted any mention of "authorization." [8] In § 1030(a)(4), and others like it (§§ 1030(a)(1), (a)(2)), Congress singled out those accessing "without authorization" (or below authorization) and those "exceeding authorization" (or above authorization) while purposefully leaving those in the middle untouched (those accessing *with* authorization), regardless of their subjective intent.

8 For example, in § 1030(a)(5)(A)(i) Congress targeted all transmitters, regardless of authorization. Section 1030(a)(5)(A)(i) provides that whoever "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." 18 U.S.C. § 1030(a)(5)(A)(i). Here, even transmitters *with* authorization do not escape liability, unless the damage they cause is permitted.

[*22] Third, by reading Restatement § 112 into "without authorization," employers suddenly have a federal cause of action whenever employees access the company computer with "adverse interests" and such access causes a statutorily recognized injury. In addition to broadening the doorway to federal court, the "adverse interest" inquiry affixes remarkable reach to the statute -- a reach that is not apparent by the statute's plain language. Under *Citrin*, would checking personal email on company time without express permission and thereby causing, however unintentionally, impairment to the computer in excess of $ 5,000 give rise to CFAA liability? It might. [9]

9 *See* 18 U.S.C. § 1030(a)(5)(A)(iii) (providing that whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage. . . ."). If conducting personal activities on the job is considered an adverse interest, it would appear that § 1030(a)(5)(A)(iii) might apply to the worker checking personal email. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1634 (2003) (explaining that the apparent effect of *Shurgard* is to extend liability to "an employee's use of an employer's computer for anything other than work-related activities"); *see also* Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. Rev. 2164, 2258 (2004) (cautioning against a broad reading of "without authorization").

[*23] Fourth, the breadth of the statute given under the *Citrin* reading is especially disconcerting given that the CFAA is a *criminal* statute with a civil cause of action. To the extent "without authorization" or "exceeds authorized access" can be considered ambiguous terms, the rule of lenity, a rule of statutory construction for criminal statutes, requires a restrained, narrow interpretation. *See, e.g., Pasquantino v. United States*, 544 U.S. 349, 383, 125 S. Ct. 1766, 161 L. Ed. 2d 619 (2005) (speaking of the rule of lenity, the Court explained "[w]e

have long held that, when confronted with two rational readings of a criminal statute, one harsher than the other, we are to choose the harsher only when Congress has spoken in clear and definite language.") (internal quotations omitted). [10] The fact that this Court now addresses the CFAA in a civil context does not withdraw the necessity of applying the rule of lenity. *See, e.g., Leocal v. Ashcroft*, 543 U.S. 1, 12 n.8, 125 S. Ct. 377, 160 L. Ed. 2d 271 (U.S. 2004) (explaining in footnote dictum that, if a statute has criminal applications, "the rule of lenity applies" to the Court's interpretation of the statute even in immigration cases because of the need to "interpret [*24] the statute consistently, whether we encounter its application in a criminal or noncriminal context"); *United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18, 518 n.10, 112 S. Ct. 2102, 119 L. Ed. 2d 308 (1992) (plurality opinion) (employing the rule of lenity to interpret "a tax statute . . . in a civil setting" because the statute "has criminal applications"); *id.* at 519 (Scalia, J., concurring) (invoking the rule of lenity in a concurrence joined by Justice Thomas). Thus, the view of the CFAA adopted by this Court is one that follows the statute's plain meaning, and coincidently, has the added benefit of comporting with the rule of lenity. [11]

10 *See also United States v. Wiltberger*, 18 U.S. 76, 95, 5 L. Ed. 37 (1820) ("The rule that penal laws are to be construed strictly, is perhaps not much less old than construction itself. It is founded on the tenderness of the law for the rights of individuals; and on the plain principle that the power of punishment is vested in the legislative, not in the judicial department. It is the legislature, not the Court, which is to define a crime, and ordain its punishment.").

[*25]

11 Because the CFAA has largely been addressed in the civil context, courts may be adopting a more expansive view of "authorization" than they would have taken in the criminal context. As one commentator points out, it is one thing to say that a defendant must compensate a plaintiff for the harm it caused in a business dispute; "it is quite another to say that a defendant must go to jail for it." Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1641-42 (2003).

C. Lockheed Fails to Adequately Allege a Violation of § 1030(a)(5)(A)(i)

Count II alleges a violation of § 1030(a)(5)(A)(i), which provides whoever "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[.]" 18 U.S.C. § 1030 (a)(5)(A)(i). The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information[.]" 18 U.S.C. § 1030(e)(8) [*26] . As noted earlier in Part III(A), the loss of trade secrets does not constitute "damage" under the statute. *Resdev, LLC v. Lot Builders Ass'n*, 2005 U.S. Dist. LEXIS 19099, No. 6:04-CV-1374, 2005 WL 1924743, * 4 (M.D. Fla. Aug. 10, 2005). Likewise, while Lockheed's remedial measures (the response to the alleged conduct and subsequent damage assessment) fall under the statute's definition of "loss," such measures do not fit in the definition of "damage," which is aimed at the impairment rendered to the computer and information therein.

In its response memoranda, Lockheed requests this Court to "infer from the totality of the allegations . . . that as a result of . . . data synchronizing and the data downloading to CDs, a number of the Lockheed Martin files were permanently deleted from Lockheed Martin's computers." (Doc. 75 at 11; *see also* Doc. 71 at 12.) The Court will not infer an allegation that the Complaint does not itself allege. In the 53 pages and 165 paragraphs devoted to the Amended Complaint, the only reference to permanently deleted files is the following: "The Defendants were not authorized to damage, delete or permanently remove data files from [Lockheed] computers." (Compl. [*27] P 74.) But this statement falls short of alleging that the Employees actually *did* permanently delete or remove documents. In the paragraph of the Complaint that is devoted to providing a detailed account as to the Employees' particular actions, there is no mention of permanent deletion or removal. (Compl. P 50.) The copying of information from a computer onto a CD or PDA is a relatively common function that typically does not, by itself, cause permanent deletion of the original computer files. In the absence of an allegation of permanent deletion or removal, the Court will not create one. Count II is accordingly dismissed.

D. Lockheed Fails to Adequately Allege a Violation of § 1030(a)(5)(A)(ii)

Count III alleges that Defendants violated § 1030(a)(5)(A)(ii) of the CFAA, which provides that whoever "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage[.]" 18 U.S.C. § 1030(a)(5)(A)(ii). In light of Parts III(A), (B), it is easy to see that Count III must fail because the Employees' accessed *with authorization* and did not cause *damage*, as those terms are contemplated [*28] and defined under the CFAA. Count III is accordingly dismissed.

IV. Conclusion

Lockheed is not entitled to relief under 18 U.S.C. § 1030(a)(4) because the Employees' access was neither "without authorization" nor "exceeding authorization" as those terms are contemplated by the CFFA. Further, relief is unavailable under 18 U.S.C. § 1030(a)(5)(A)(i) because Lockheed fails to allege anything constituting "damage" as that term is defined under the statute. Finally, relief under 18 U.S.C. § 1030(a)(5)(A)(ii) is unavailable because this provision requires an allegation of "without authorization" *and* "damage" - both of which Lockheed fails to adequately allege. Accordingly, it is

ORDERED THAT the Employees' Motions to Dismiss (Docs. 53 & 68) are **GRANTED**. The dismissal of Lockheed's claims is **without prejudice** and with leave to amend. Lockheed shall have **twenty days** to replead in a manner consistent with this Order if Lockheed chooses to do so.

DONE and ORDERED in Orlando, Florida on this 1st day of August, 2006.

GREGORY A. PRESNELL

UNITED STATES DISTRICT [*29] **JUDGE**