UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

WENDI J. LEE,

Plaintiff,

v. CASE NO.: 8:10-cv-2904-T-23TBM

PMSI, INC.,

Defendant.
_____/

ORDER

The plaintiff Wendi Lee ("Lee") sued the defendant PMSI, Inc., (PMSI) her former employer, for pregnancy discrimination. (Doc. 2) PMSI answered (Doc. 5) and moved to dismiss Count II of the complaint. (Doc. 4) A previous order denied the motion to dismiss. (Doc. 7) PMSI filed an amended answer and a counterclaim (Doc. 12) asserting a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030. ("CFAA")[1] PMSI asserts that the Lee engaged in "excessive internet usage" and "visit[ed] personal websites such as Facebook and monitor[ed] and [sent] personal email through her Verizon web mail account." Lee moves (Doc. 13) to dismiss the counterclaim.

[1] PMSI also asserts a claim under 18 U.S.C. § 2707, which provides for a civil right of action for a violation of the Stored Communications Act. However, the counterclaim fails to specify the section of the Stored Communications Act that Lee violated and the response (Doc. 17) to the motion to dismiss fails to discuss the statute at all.

The CFAA is a criminal statute originally designed to target hackers who access computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possess the capacity to "access and control high technology processes vital to our everyday lives...." LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130 -1131 (9th Cir. 2009), citing 1131 H.R. Rep. 98-894, 1984 U.S.C.C.A.N. 3689, 3694 (July 24, 1984). Both the letter and the spirit of the CFAA convey that the statute is not intended to cover an employee who uses the internet instead of working. See, e.g., Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003) (rejecting a claim of trespass to chattels after an employee used the company's email system to transmit remarks disparaging the employer); Clarity Services v. Barney, 698 F.Supp.2d 1309, 1316 (M.D. Fla. 2010) (expressing skepticism that an employee violates the CFAA by checking personal email at work). A CFAA violation occurs if a defendant either (1) damages a computer system or (2) obtains information to which the employee is not entitled. See, e.g., United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (affirming the conviction of a defendant who created an internet "worm" that caused computers to crash), and Shurgard Storage Centers v. Safeguard Self Storage, 119 F.Supp.2d 1121 (W.D. Wash. 2000) (denying a motion to dismiss a CFAA claim against a defendant that hired the plaintiff's former employee, who, while still in the plaintiff's employ, sent emails to the defendant containing the plaintiff's trade secrets and proprietary information). The defendant's counterclaim fails to allege either (1) that the defendant's computer system was damaged by the plaintiff's internet usage or (2) that the plaintiff accessed any of the defendant's

information (as distinguished from her personal email and facebook pages, to which she was entitled after business hours).

The CFAA 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. . ." 18 U.S.C. § 1030(g). The statute provides a civil action only in specified circumstances. The only circumstance arguably obtaining in this action is a "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value[.]" 18 U.S.C. § 1030(c)(4)(A)(i)(I). "Loss" is defined as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior 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). "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The statute does not contemplate "lost productivity" of an employee, and with the exception of the loss of productivity, the defendant fails to allege "damage" caused by the plaintiff's internet usage. The defendant asserts (dubiously) that during her six months of employment, the plaintiff caused the defendant "financial losses in excess of $5,000, due to her lack of productivity . . ." (Doc. 12) The definition of "loss" contemplates damage to a system or data, rather than a lack of productivity.

Citing 18 U.S.C. § 1030(a)(2)(C), PMSI's counterclaim states that to recover under the CFAA, "a person must prove (1) an intentional access to a computer; (2) lack of authorization or exceeded authorization to the computer; (3) obtained information from

the computer; and (4) a loss of at least $5000.00."[2] (Doc. 12, Page 6) PMSI fails to show that the plaintiff "exceeded authorized access" or obtained information from the computer. "Exceeds authorized access" is defined as "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 counterclaim alleges that the plaintiff visited only personal websites. (Doc. 12, Pages 6 and 7) Because the only information Lee allegedly accessed was on the personal websites, not PMSI's computer system, Lee never "obtained or alter[ed] information in the computer." Lee accessed her facebook, personal email, and news websites but did not access any information that she was "not entitled so to obtain or alter."

LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009), states that "for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations. It is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'" Because PMSI fails to allege that Lee's authorization to use her work computer was terminated prior to her leaving the company, PMSI cannot show that Lee's use of the computer was "without authorization." Although Lee's internet usage may violate company policy, 18 U.S.C. § 1030 is inapplicable.

---

[2] 18 U.S.C. § 1030(a)(2)(C) also requires that the information be obtained from "a protected computer" which is defined as a computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). The defendant fails to allege that the plaintiff accessed a "protected computer."

For the proposition that an employee's personal use of a company computer in violation of a company policy constitutes a violation under the CFAA, the defendant cites only United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010), in which a worker for the Social Security Administration accessed the personal records of friends and acquaintances. The Eleventh Circuit upheld his conviction under 18 U.S.C. § 1030(a)(2)(B), which applies to government computers, because Rodriguez accessed the sensitive personal information on the government computers. In this instance, Lee did not improperly access any information on PMSI's computer, and the only information she accessed was her own information on her email and facebook accounts.

In Clarity Services v. Barney, 698 F.Supp.2d 1309 (M.D. Fla. 2010), an employee solicited and read an email from a customer on the employee's company email account after resigning from the company. The defendant also deleted information from his company laptop before returning the laptop to his former employer. The company's claim under 18 U.S.C. § 1030 was rejected because the defendant did not lack authorization to access the information or exceed his authorization. The claim was rejected despite the fact that the employee accessed customer information and deleted information on the laptop. In this instance, Lee neither accessed nor damaged any PMSI information.

Clarity Services notes that 18 U.S.C. § 1030 is a "criminal statute with a civil cause of action" and that the rule of lenity "requires a restrained, narrow interpretation." 698 F.Supp.2d at 1316. Extension of a federal criminal statute to employee misconduct in the private sector is a legislative responsibility and not a proper occasion for aggressive statutory interpretation by the judiciary. See, e.g., United States v. Rybicki, 354 F.3d 124, 135 (2d Cir. 2003).

The motion to dismiss (Doc. 13) is **GRANTED**, the defendant's counterclaim is **DISMISSED WITH PREJUDICE**, and the defendant's original answer (Doc. 5) is **REINSTATED**.

ORDERED in Tampa, Florida, on May 6, 2011.

STEVEN D. MERRYDAY
UNITED STATES DISTRICT JUDGE