E-FILED on 11/19/2010

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. SUIBIN ZHANG, Defendant.	No. CR-05-00812 RMW ORDER GRANTING MOTION TO DISMISS COUNTS ONE THROUGH THREE OF THE SUPERSEDING INDICTMENT **[Re Docket No. 171]**

Defendant Suibin Zhang moves to dismiss counts one through three of the nine count superseding indictment filed against him. The counts in question allege violations of the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(a)(4), which imposes criminal liability on an individual who "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 . . . ." For the reasons set forth below, the court grants the motion to dismiss.

/ / /

/ / /

/ / /

I. BACKGROUND[1]

From December 2001 to April 2005, Defendant Suibin Zhang was employed as a product development manager for Netgear, Inc., a company that designs and sells various networking devices. As a Netgear employee, Zhang was given a password that enabled him to gain access to a secure extranet web site maintained by Marvell Semiconductor, Inc., a company that supplies some of the switches and transceivers used in Netgear products. Marvell's extranet allows authorized customers to view and download product-related documents. Marvell regulates access to its extranet through a combination of nondisclosure agreements, registration requirements, limited licensing agreements, passwords, and permissions.

At some point shortly before March 2005, Zhang interviewed for positions at Marvell and at one of Marvell's direct competitors, Broadcom, Inc. Zhang rejected Marvell's employment offer on March 7, 2005. He accepted Broadcom's offer on March 8. On March 9, 16, and 18, before Zhang left Netgear for Broadcom, he used his password to log into Marvell's extranet and download a number of Marvell's proprietary documents.

On December 21, 2005, the grand jury returned a nine-count indictment against Zhang based on Zhang's use of Marvell's extranet while he was still employed at Netgear and some weeks before he began working at Broadcom. On January 21, 2009, the grand jury returned a superseding indictment against Zhang. Counts one through three allege that Zhang's download of documents constituted unauthorized access or conduct that exceeded his authorized access to Marvell's extranet, in violation of 18 U.S.C. § 1030(a)(4). Counts four through nine, not at issue in this motion, charge Zhang with misappropriation, unauthorized downloading, copying, transmission, and possession of stolen trade secrets, in violation of 18 U.S.C. § 1832(a)(1), (2), (3) and (4).

/ / /

/ / /

/ / /

/ / /

[1] Unless otherwise noted, background facts are taken from the superseding indictment.

II. ANALYSIS

A. Motion to Dismiss

Under Rule 12(b) of the Federal Rules of Criminal Procedure, a party may file a motion to dismiss based on "any defense, objection, or request that the court can determine without a trial of the general issue." Fed. R. Crim. P. 12(b); *United States v. Shortt Accountancy Corp.*, 785 F.2d 1448, 1452 (9th Cir. 1986). In considering a motion to dismiss, the court is limited to the face of the indictment and must accept the facts alleged in the indictment as true. *Winslow v. United States*, 216 F.2d 912, 913 (9th Cir. 1955).

B. The CFAA Charges

The provision of the CFAA in question makes it a crime if a person "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 . . . . " 18 U.S.C. § 1030(a)(4). The CFAA does not define the term authorization. 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).

The government concedes that Zhang did not access any protected computers "without authorization." They argue, however, that Zhang "exceeded authorized access" of Marvell's extranet when he downloaded proprietary and trade secret information allegedly in order to benefit Broadcom while he was still a Netgear employee with authorization to download the documents in question from Marvell. The question presented by this motion is whether an employee acts "in excess of authorized access" if he accesses confidential and proprietary information from a server that he has permission to access, but intends to use that information in a manner inconsistent with the owner's intention or in violation of contractual obligations such as nondisclosure agreements or limited license agreements.

There are two diverging lines of case law interpreting the CFAA. Courts interpreting the CFAA broadly have construed the statute to mean that an employee who uses an employer's computer to obtain business information with intent to defraud acts "without authorization" or "exceeds authorization" under the statute. *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Such courts have held that an employee loses authorization to access a computer protected by the CFAA as

soon as "the employee resolves to act contrary to the employer's interest." *LVRC Holdings, LLC v. Brekka*, 581 F.3d at 1133-34. Courts construing the CFAA narrowly, on the other hand, have concluded that the statute is violated only when initial access or access of certain information is not permitted in the first place. *Id.*; *United States v. Norsal*, 2010 WL 934257 (N.D. Cal. Jan. 6, 2010); *Lewis-Burke Associates, LLC v. Widder*, 2010 WL 2926161 (D.D.C. July 28, 2010); *Bell Aerospace Services, Inc. v. U.S. Aero Services, Inc.*, 690 F.Supp.2d 1267 (M.D. Ala. 2010); *ReMedPar, Inc. v. AllParts Medical, LLC*, 683 F.Supp.2d 605 (M.D.Tenn. 2010).

In deciding *Brekka*, the Ninth Circuit adopts the narrower interpretation of the CFAA. 581 F.3d at 1129. Brekka was employed by LVRC, a residential treatment center for addicted persons, to oversee a number of aspects of the facility. *Id.* During his employment, Brekka and LVRC began negotiations for Brekka to purchase an ownership interest in LVRC, and Brekka emailed a number of sensitive LVRC documents to his personal email account and to his wife's personal email account, which he downloaded to his personal computer. The negotiations broke down, and Brekka left LVRC. *Id.* at 1129-30. LVRC brought an action in federal court alleging that Brekka had violated the CFAA when he emailed LVRC documents to himself while he was still employed by LVRC. *Id.*

The Ninth Circuit held that to bring a successful action under section 1030(a)(4), a plaintiff "must show that [defendant]: (1) accessed a 'protected computer,' (2) without authorization or exceeding such authorization that was granted, (3) 'knowingly' and with 'intent to defraud,' and thereby (4) 'further[ed] the intended fraud and obtain[ed] anything of value.' . . . . ." *Id.* at 1131. "[A] person uses a computer 'without authorization' under [section 1030(a)(4) only] when the person has not received the permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.' *Id.* at 1135.

In so holding, the court explicitly rejected the broader interpretation of the CFAA articulated in *Citrin*. The Ninth Circuit held that the rule of lenity, which counsels against interpreting criminal statutes "in surprising and novel ways that impose unexpected burdens on defendants," required the court to interpret section 1030(a)(4) narrowly. *Id.* at 1134. Thus, the court explained that authorization

hinges not on the employee's state of mind or intentions when accessing information on the protected computer, but on "actions taken by the employer." *Id.* at 1135.

The government concedes that Zhang's downloading activity was not "without authorization" within the meaning of 18 U.S.C. § 1030(a)(4), as interpreted by *Brekka*. They argue, however, that Zhang's conduct "exceeded authorized access" because he violated the terms of the nondisclosure agreement, the extranet terms of use, and a limited use license agreement when he downloaded confidential information for reasons that were not exclusively in furtherance of the business relationship between Netgear and Marvell. The government contends that an individual "exceeds authorized access" by violating the terms of a nondisclosure or license agreement that prohibit accessing confidential information for reasons other than those specified in the agreement. Attempting to distinguish *Brekka*, the government emphasizes that the parties in *Brekka* did not have a written employment agreement, and LVRC did not promulgate employee guidelines that would prohibit employees from emailing LVRC documents to personal computers.

Zhang's alleged conduct is certainly more egregious than Brekka's. However, the government's attempt to read *Brekka* as criminalizing access in violation of an employer's nondisclosure or other agreement has been recently addressed and rejected in this district. *See Nosal*, 2010 WL 934257. As that court recognized, *Brekka* does provide "some indication, in dicta, that an employer might be able to define the scope of an employee's access in terms of how the employee uses the information obtained from the computer system." *Id.* at *6 (citing *Brekka*, 581 F.3d at 1133 ("An individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has 'exceed[ed] authorized access.'")). Nonetheless, a plain reading of section 1030(e)(6)'s definition in light of *Brekka* compels a different conclusion. An individual "exceeds authorized access" if he or she has permission to access a portion of the computer system but uses that access to "obtain or alter information in the computer that [he or she] is not entitled so to obtain or alter." *Id.* at *7. As the court in *Norsal* explained, "there is simply no way to read that definition to incorporate policies governing use of information unless the word alter is interpreted to mean misappropriate." *Id.*

The government argues that the operative word in §1030(e)(6)'s definition is "entitled," and that Marvell's policies and agreements circumscribed Zhang's "entitlement" to obtain the information. But the government's proposed definition creates a distinction between "authorization" and "entitlement" where none exists. An entitlement is the direct result of a corresponding authorization, and is circumscribed by the limits of that authorization. Within the meaning of the CFAA, Zhang was entitled to download the relevant documents because Marvell authorized his access to those documents.

Furthermore, it is clear that the court in *Brekka* intended this interpretation. *See Brekka*, 581 F.3d at 1129 ("Nor did emailing the documents "exceed authorized access," because Brekka was entitled to obtain the documents."). The court explained that "[A] person who 'intentionally accesses a computer without authorization, §§ 1030(a)(2) and (4), accesses a computer without any permission at all, while a person who 'exceeds authorized access,' *id.*, has permission to access the computer, but accesses information on the computer that the person is not entitled to access." *Id.* at 1133. The court reasoned that "[i]f the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer could constitute a criminal violation of the CFAA." *Id.* The same is true with respect to the breach of a private contract. Without the employer or the owner of the information rescinding the right to obtain the information, the defendant would have no more reason to know that breaching a private contract governing use could constitute a criminal violation of the CFAA than he would that breaching a state law fiduciary duty could lead to criminal liability.

Several district courts in other circuits have similarly narrowly construed § 1030(e)(6). For example, in *Bell Aerospace* the court stated in granting summary judgment in favor of former employees accused with violating the CFAA:

> *Exceeds Authorization*: "Exceeds authorized access" should not be confused with exceeds authorized use. Therefore, at issue here is only whether the former Bell Aerospace employees exceeded their authorized access, not whether they exceeded their authorized use.
>
> There is no evidence in the record to suggest that these employees "exceed[ed] authorized access." § 1030(a)(2) and (4); indeed, the employees were "permitted access to [Bell Aero's] network and any information on that network" under their individual user accounts. Because it appears that the CFAA is concerned with access, not use, whether these employees did not have permission to copy or subsequently misuse the accessed data by sharing them is another matter that may be circumscribed by a different statute and is not at issue here.

690 F. Supp.2d at 1272-73; *see Lewis-Burke Associates, LLC*, 2010 WL 2926161; *ReMedPar, Inc. v. AllParts Medical, LLC*, 683 F.Supp.2d at 613.

III. ORDER

Counts one through three of the superseding indictment fail to allege a valid offense under the CFAA as interpreted by the Ninth Circuit in *LVRA Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009) and by persuasive district court decisions. For the foregoing reasons, the court grants defendant Zhang's motion.

DATED: 11/19/2010

Ronald M. Whyte
RONALD M. WHYTE
United States District Judge