SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
ATTORNEYS AT LAW

Labor & Employment Law BLOG
Up-to-date Information on Labor & Employment

05-18-2011

Social Media Activity In The Workplace And The Computer Fraud And Abuse Act

It should come as no surprise that employers are trying to assert a claim for violation of the Computer Fraud and Abuse Act ("CFAA") based on employees accessing social networking sites such as Facebook from work computers. While one employer was unsuccessful in stating a claim, employers should not give up on opportunities to assert the CFAA as a claim in an employment related action.

The CFAA is a criminal statute that also allows for civil action claims. To state a claim, an employer has to assert the following elements:

(1) an employee intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer (*e.g.* used in or affecting interstate commerce) [18 U.S.C. § 1030(g)]. The other essential requirement for stating a claim under this federal statute is that the employer suffers a computer related loss totaling at least $5,000 in value.

In *United States v. Nosal*, the Ninth Circuit held on April 28, 2011, that the government in a criminal action stated a CFAA claim against former employee David Nosal and his co-conspirators. Nosal is alleged to have started a competing business, and conspired with current employees of Korn/Ferry, a premier executive search firm, to have them copy Korn/Ferry's confidential database of executive candidates. The *Nosal* court held that Korn/Ferry took

considerable measures to protect its confidential database, including a screen notification that appeared with every login which stated in essence:

> "This computer system and information it stores and processes are the property of Korn/Ferry. You need specific authority to access any Korn/Ferry system or information and to do so without the relevant authority can lead to disciplinary action or criminal prosecution..."

The *Nosal* Court held that "an employee 'exceeds authorized access' under § 1030 when he or she violates the employee's computer access restrictions - including use restrictions." Further, the Court held that the majority of computer crimes prohibited by the CFAA involve taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data.

In an employment case decided on May 6, 2011, *Lee v. PMSI*, a federal district court in Florida granted a motion to dismiss a CFAA claim because the employee's alleged excessive use of the company computers to access Facebook and her personal email was not alleged to have caused damage to the company's computers. The Court held that lack of productivity due to an employee accessing Facebook does not constitute damage to a computer as required by the CFAA. Further, the Court held that since the employee was only accessing her personal information through the company's computer, PMSI could not allege that Lee accessed or damaged any PMSI information.

On the other hand, an employer may be able to state a claim under the CFAA by alleging that the employee infected the company's computer(s) with a virus that is traceable to Facebook or another social networking site. An Internet search shows a number of viruses that have been targeted to Facebook users. For example, there was a password stealing virus which urged Facebook users to open an attachment to obtain new login credentials, which once opened downloaded several types of malicious software including a program that stole

banking passwords and other sensitive information from the user's computer. McAfee, an antivirus software maker, estimated that the virus would succeed in affecting millions of computers. Another virus named the Koobface virus invited people to watch a funny video with an additional prompt to upgrade their Flash player. This upgrade was actually the means for unleashing the virus, which reportedly turned "victim machines into zombie computers to form botnets." More recently, Facebook users are warning their friends not to click on invitations "to see who has been viewing you," or to "win a free iPad," because they are suspected to be vehicles for spreading viruses and other malware.

In other words, an employer with a clear computer use policy that prohibits use of company computers to access social networking sites for personal business may be able to state a claim under the CFAA. If the facts are there, the employer may want to allege that the computer system was damaged by a computer virus which resulted in a loss of at least $5,000 in value, and that company data was compromised. The loss provision requirement can be satisfied by costs associated with a forensic assessment of how the computer was being accessed improperly, consequential damages incurred because of interruption of service, and costs to remove the virus and remedy any damage to the computer.

Application of the CFAA to social media activity is a new area of the law with few reported cases. With *Nosal*, the Ninth Circuit is now in accord with other circuits. The CFAA can be applied to employees who abuse their company's computer access rules to the detriment of the company. As a preliminary step to being able to state a claim under the CFAA, however, businesses should consult with knowledgeable legal counsel to update their computer use policies.

This article was originally posted on Sheppard Mullin's Social Media Law Update blog, which can be found at www.socialmedialawupdate.com.

For further information, please contact Michelle Sherman at (213) 617-5405. (Follow me on Twitter!)