GJORDING | FOUSER

LET'S GET DIGITAL – THE NINTH CIRCUIT DISCUSSES UNAUTHORIZED COMPUTER ACCESS UNDER THE CFAA

September 2, 2016

Author: Jennifer L. Swajkoski

In today's digital age, everyone is connected – by computers, tablets and cell phones. These computing devices have upped the pace of an already fast moving world. Where it once took days, weeks or months to hear back via letter, it now takes a matter of seconds, minutes or hours via e-mail. Where you once had to take the time to listen to your voicemail, you can now send and receive a text message immediately on your phone. A quick response to a work or home life matter is no longer appreciated but expected. In order for businesses to keep up with the pace, many employers now permit employees to gain access to work accounts on their personal computing devices, such as cell phones or tablets. For employers who permit this practice, the lines between what belongs to the employee and what belongs to the employer have blurred, especially when it comes to authority and access.

For instance, consider an employee who sets a password to sync her work email account to her personally owned cell phone. She personally owns the cell phone, but who has authority to control the work account on her device? What happens if she is terminated? Additionally, does she have the authority to share her account password for legitimate work purposes?

The Ninth Circuit Court of Appeals, in two back-to-back decisions, recently sought to provide some clarity to these types of issues as they relate to the Computer Fraud and Abuse Act (CFAA), a statute designed to prevent computer hacking that imposes liability on people who knowingly access computers without permission. First the court held in *United States v. Nosal* that the CFAA criminalizes unauthorized access to employer networks by former employees. *Nosal* involved a former employee who, after leaving his company to sign on with a competitor, used the password of his former executive assistant to gain access to proprietary and confidential information from his former employer. The court determined that, despite having permission and a password from the executive assistant, Nosal did not have authority to access the network. The court determined that Nosal's authority was revoked when he left the company and explained that his use of a third party did not shield him from liability under the CFAA.

Following *Nosal*, many questioned to what extent password sharing could be actionable. The court provided further clarification in *Facebook v. Power Ventures*, its second recent decision. In that case, Power Ventures, a site where users could access contacts from their various social networking platforms in one location, was creating events and sending out messages through its users' Facebook accounts. Upon discovering this, Facebook sent a cease and desist letter demanding Power Ventures stop soliciting over its site. In an effort to clarify "authorized access" the court explained that initially user permission gave Power Ventures implied authorization to access its users' Facebook accounts. However, Facebook affirmatively revoked that authorization through its cease and desist letter. Thus, any access following the cease and desist letter was unauthorized in violation of the CFAA.

Following both cases, one thing is clear regarding authorized access. Affirmative revocation is the best way for an employer to maintain a claim for unauthorized access under the CFAA.

INSIGHTS FOR EMPLOYERS

1. Create a bright line policy that informs employees what exactly they are authorized to access.
2. Any employer that permits its employees to sync up to a work network through a personal computing device should create a policy detailing the scope of authorized access and potential consequences for access that is unauthorized or that exceeds the employee's authorization.
3. Prepare an affirmative revocation statement for employees to read and sign upon suspension, termination or resignation.

Please contact a Gjording Fouser lawyer at 208.336.9777 if you would like any additional information about this topic or any other employment issues facing your company.