SANDS ANDERSON

Virginia Workplace Law

Computer Abuse and Use: How Protected Are You?

By: Faith Alejandro. *Tuesday, September 4th, 2012*

If your company policies don't adequately define employee parameters of computer access as well as usage, then your company may find itself losing to disgruntled employees who take or misuse company data.

Several cases this year exemplify how important it is for employers to continually update and monitor their computer policies.

Earlier this year, the **Fourth Circuit** limited the criminal and civil protections afforded under the **Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030**. In **WEC Carolina Energy Solutions v. Miller**, Mr. Miller, the project director for WEC Carolina Energy Solutions, Inc., resigned his post. Before leaving—but while still employed by WEC—the company claims Mr. Miller downloaded WEC's proprietary information and used it to pitch a presentation and secure a potential WEC client for his new employer and competing company, Arc Energy Services, Inc. So, WEC sued Mr. Miller, his administrative assistant, and Arc under the CFAA.

But, WEC lost, with the court holding that the CFAA was intended to target system hackers, not employees who improperly accessed and used the employer's data contrary to employer policies.

The CFAA permits civil lawsuits against people who access computers without authorization. Although WEC's company policies prohibited the use of this information obtained from WEC's intranet and computer servers, the Fourth Circuit held that the CFAA merely governs hacker-type access and not use.

The Fourth Circuit held the CFAA "appl[ies] only when an individual accesses a computer without permission or obtains or alters information on a computer beyond that which he is authorized to access." Beyond the moment of access, therefore, the CFAA does not apply, even when people like Mr. Miller go on to use the information in violation of company policy. The Court justified its narrow interpretation because the CFAA also allows criminal penalties, which mandates the Court to "avoid interpretations not clearly warranted by the text."

WEC argued that by downloading WEC's data contrary to WEC's interests and company policies, Mr. Miller's status as the employer's agent instantly ceased and he lost all benefits of authorized access. The Court, however, ruled that this was a slippery slope. After all, "any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems." The Fourth Circuit reasoned that even though such a "frolic" could justify the

employer's rescission of the employee's authorization, Congress did not intend an immediate end to the employer-employee agency relationship under the CFAA.

The Court recognized "[o]ur conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers or information in bad faith, or who disregard a use policy."

The Fourth Circuit recognized that the employer still had state law claims (i.e., conversion, tortious interference with contractual relations, conspiracy, trade secret violations, breach of fiduciary duty, contract). However, as the case of **21st Century Systems, Inc. v. Perot Systems Government Services, Inc.**, shows, employers must be ready to prove their damages. Perot's former employees had copied thousands of the employer's computer files to an external hard drive, taking millions of dollars of accounts with them to establish a competing business. The employer was unable to sufficiently prove its damages under state law, and lost a $3 million jury award on appeal to the **Supreme Court of Virginia** by the employees.

Although Congress has passed several laws regarding electronic data protection, the laws stop short of providing employers with clear claims for damages against employee hackers.

For example, the **Stored Communications Act 18 U.S.C. §§ 2701–2712** permits employers who are providers of electronic services (i.e. email) to access employee's stored e-mails, but prohibits access to emails on servers hosted by third parties, such as an employee's personal Web-based email account, or text messages stored on third party sites, even though the employer paid for the phone service.

Similarly, the **Electronic Communication Privacy Act ("ECPA"), 18 U.S.C. §§ 2510–2522** protects electronic communications from unauthorized interception. But this protection applies only during transmission and ends once the message arrives.

As these recent cases and statutes show, the employer often has a difficult path to prove recovery of damages for employee data theft. As a result, employers should check their policies to be sure they clearly define not only employee limits of computer access, but also limits on usage of electronic data. Employers should also have employees authorize the employer to have access to their work computers and digital information not only on the employer's system, but also on third party systems (i.e., the "Cloud" and third party communications servers).

If you have a question regarding your company's computer access and usage policies, the **Virginia employment law attorneys** at **Sands Anderson** would be happy to assist.