The Coverage Inkwell

Emerging Coverage Issues in Intellectual Property, Privacy, and Cyber Liability

White and Williams LLP

Joshua A. Mooney
mooneyj@whiteandwilliams.com

July 25, 2013

A QUESTION FOR CYBER COVERAGE: ANOTHER COURT HOLDS "WITHOUT AUTHORIZATION" UNDER CFAA MEANS HACKING

The Computer Fraud and Abuse Act (CFAA) imposes criminal and civil liability upon those who access a protected computer "without authorization" or in a manner that "exceeds authorized access." 18 U.S.C. § 1030. A split exists among federal courts over interpretation of the phrases "without authorization" and "exceeds authorized access" under the statute. In short, do these phrases only mean that a violation of the CFAA happens when a person evades technological obstacles, such as pass codes, code encryptions, or other forms of security, when accessing the network information in question? Or do they also mean that a violation happens when a person accesses network information that he or she is otherwise entitled to access, but does so for purposes that exceed his or her authorization, such as to perpetrate a crime?

Although not yet addressed by any court, this legal question will have a direct impact on the scope of coverage in cyber liability policies. Network and information security liability coverage, which covers certain loss caused by the failure to prevent an "unauthorized access" into an insured's database, is a primary component of most cyber policies. However, these policies generally do not define the meaning of "unauthorized access" or similarly used phrases. The question then becomes whether these policies provide coverage only for security breaches caused by an outside hacker, or whether they also cover wrongful acts committed by a rogue employee from within? Undoubtedly, courts will look to federal interpretation of the CFAA for guidance.

In *Power Equipment Maintenance, Inc. v. AIRCO Power Servs., Inc.*, 2013 WL 3422779 (S.D. Ga. June 28, 2013), the United States District Court for the Southern District of Georgia became the latest court to weigh in on the debate over the appropriate interpretation of "without authorization" and "exceeds authorized access" under the CFAA. Confronted with "classic allegations by an employer that former high-ranking employees misappropriated confidential information" when defecting to a direct competitor, the court held that because the defendant employees had been given access to the information in question by virtue of their executive positions, there was no CFAA violation. The salient facts of the case are as follows.

Plaintiff Power Equipment Maintenance (PEM) employed Defendants Onofry and Burrows as executive officers. By virtue of their positions, both Defendants "had access to all of [PEM's] confidential information and trade secrets." *Id.* at *1. Defendants left PEM to join with a direct competitor. Thereafter, PEM commenced a lawsuit, alleging that Defendants stole trade secrets. *Id.* PEM alleged that "between the time Defendants Onofry and Burrows decided to leave its employ and actually announced their intentions, [Defendants] surreptitiously accessed and acquired Plaintiff's confidential information and trade secrets for use during their employment with AIRCO I." *Id.*

The complaint also alleged that Defendants continued to misappropriate proprietary information after their resignation from PEM's employment. The complaint alleged:

> …after Defendant Burrow's November 21, 2012 resignation, he continued to steal confidential information despite his computer access being strictly limited. (*Id.* ¶40.) In this regard, Plaintiff alleges that Defendant Burrows solicited one of its customers by sending an email from his work account informing the customer that he was leaving for AIRCO I. (*Id.* ¶¶41–42.) In addition, Plaintiff claims that, following the revocation of his access, Defendant Burrows directed an PEM administrative assistant to print a draft contract between PEM and one of its largest clients, which contained information as to PEM's staffing, compensation policies, and profit margins. (*Id.* ¶43.)
>
> * * *
>
> Plaintiff also contends that, after leaving its employ, Defendant Burrows logged into a database of turbine industry information and upcoming business opportunities using Plaintiff's login credentials. (*Id.*, ¶49.)

Id. at *2.

PEM's lawsuit alleged violation of the CFAA, tortious interference with business relations, misappropriation of trade secrets, and conspiracy. *Id.* The lawsuit also alleged that Onofry and Burrows breached their duty of loyalty. *Id.* Defendants moved to dismiss the lawsuit, contending, among other things, that Burrow's and Onofry's actions were not violations of the CFAA because both Defendants had been authorized to access the information in question. *Id.* at *3. The court agreed.

Looking to the legislative history of the CFAA, the court concluded that the purpose of the statute was to prohibit outsiders from hacking into computers, not to govern the use of information by those who are given access to it through their employment:

> In this Court's opinion, these provisions of the CFAA were drafted to combat, what was at the time, the new and increasing phenomenon of computer hacking. According to the committee report, a major impetus behind the legislation was to "impose criminal sanctions upon 'hackers' and other criminals who access computers without authorization." H.R. Rep. 98–894, at 21 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3707.

Id. at *4.

Therefore, according to the court, "the proper inquiry is whether an employer had, at the time, both authorized the employee to access a computer and authorized that employee to access specific information on that computer." *Id.* The court concluded that such an inquiry creates an objective bright line test and makes the employer's own actions dispositive as to whether a violation of the CFAA exists:

> In this respect, the actions of the employer are more dispositive that those of the employee. That is, "[i]t 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.'" [Citation omitted.] The same is true regarding whether an employee exceeded his authorized access: it is the employer's decision as to what the employee can access that determines whether an employee exceeded his authorized access. This focus on the employer creates something more akin to a bright line rule that is easy to apply in the numerous and complex factual scenarios likely to arise when assessing whether a employee's actions violated the CFAA.

Id. at *5.

The court criticized those judicial decisions that use the agency theory and/or subjective-use analysis test to find liability where an employee uses information he or she has access to, but in a manner that violates a duty owed to the employer or otherwise is beyond the scope of his or her authorization. Citing two reasons for its criticism, the court first concluded that such an approach "is severely flawed in that it creates a nebulous area where the same action can fall on either side of the CFAA based on the highly subjective intentions of the employee." *Id.* Second, the court concluded that the "plain language" of the CFAA itself requires the more restrictive and narrow interpretation of the statute:

> Quite simply, without authorization means exactly that: the employee was not granted access by his employer. Similarly, exceeds authorized access simply means that, while an employee's initial access was permitted, the employee accessed information for which the employer had not provided permission. Resort to linguistic gymnastics and theories of agency are completely unnecessary to interpret these axioms provided by the plain language of the CFAA. In this Court's opinion, the language of the CFAA does not speak to employees who properly accessed information, but subsequently used it to the detriment of their employers: either one has been granted access or has not. Employers cannot use the CFAA to grant access to information and then sue an employee who uses that information in a manner undesired by the employer.

Id.

In the case before it, the court held that PEM's CFAA claims should be dismissed because Defendants had authorized access to the information in question:

> In this case, Plaintiff contends that Defendants Onofry and Burrows accessed sensitive information prior to announcing their intention to leave Plaintiff's employ for a competitor, taking trade secrets and other confidential information with them. . . . What is missing from the complaint, and thus fatal, is any allegation that Defendants Onofry and Burrows either lacked access or exceeded their authorized access. In its complaint, Plaintiff hangs its hat on the agency theory of authorized access, arguing that Defendants Onofry's and Burrows's access was unauthorized because it was "in violation of the fiduciary duties [ ] owed to PEM." (Id. ¶64.) As discussed above, however, this Court rejects that theory of liability under the CFAA.

Id. at *6.

What does this case mean? A review of most cases addressing the issue in the past year-and-a-half suggests that the pendulum is swinging towards the more-restrictive interpretation of the CFAA, as employed above in *Power Equipment Maintenance*. Such an interpretation scales back the scope of potential liability under the statute. For a coverage standpoint under cyber policies, whether or not this restrictive reading also applies to network and security liability coverage has not yet been addressed by courts. It is an important issue and the analysis in *Power Equipment Maintenance* is just one component to this coverage question. Questions are welcome.

The Coverage Inkwell

Joshua A. Mooney | Counsel
1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103-7395
Direct 215.864.6345 | Fax 215.399.9613
mooneyj@whiteandwilliams.com | whiteandwilliams.com
Assistant: Dana Genovese | 215.864-6331

White and Williams LLP