Breaching Your Non-Compete May Be Breaking the Law

8/9/2011 Gregory M. Kilby

Employers around the country are increasingly relying on the Computer Fraud and Abuse Act (CFAA) to assert a claim for damages where there is evidence that a former employee has misappropriated an employer's electronic data for the benefit of the employee's new employer. While the CFAA is a criminal statute, it also provides a civil cause of action for victims of employee data theft, as well as an avenue into federal court for employers who are usually not diverse from their employees and typically rely on state law claims. An employer may use the CFAA to pursue an employee 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 any violation of the CFAA, an employer may obtain "compensatory damages and injunctive relief or other equitable relief."

The "Agency Theory"

One of the earliest decisions on the issue, and certainly one of the most significant, was handed down by the Seventh Circuit in *International Airport Centers, LLC v. Citrin*. In that case, the Seventh Circuit, in an opinion written by Judge Posner, ruled that under common law agency principles, an employee who breaches the duty of loyalty to an employer thereby becomes "unauthorized" to access the employer's data/computers, at least for the purpose of furthering an act of disloyalty to the employer. Put more simply, should the loyalties of a current employee change and the employee's interests become adverse to his current employer, the employee's authorization to access his employer's data would change as well and become unauthorized. Under this "agency theory" the authorization to access was based upon the employee's own subjective loyalties and interests and, if they changed, the employee's authorization to access the employer's computer changed with it. The First Circuit also follows this approach. *EF Cultural Travel BV v. Explorica, Inc.*

The "Intended Use Theory"

The Ninth Circuit first weighed in on the issue in 2009 in *LVRC Holdings LLC v. Brekka*, (9th Cir. 2009) and held that accessing and e-mailing company documents for use contrary to the company's interests alone did not violate the CFAA. The court found that there is no statutory language to support the contention that authorization terminates when an employee determines to act contrary to the interest of an employer.

Recently, the Ninth Circuit clarified and substantially limited the application of *Brekka*, bringing the law in the Ninth Circuit much more in line with interpretations in other circuits (although not quite as broad

as in the Seventh Circuit). Specifically, the Ninth Circuit in *United States v. Nosal*, held that the CFAA's "exceeds authorized access" provision applies where an employer has placed limitations on the employee's "permission to use" the computer and the employee has violated or "exceeded" those limitations.

The court distinguished *Brekka* in which the employee had unfettered access to the company computer and there was no employee agreement prohibiting the employee's conduct. To the contrary, the employees in *Nosal* "were subject to a computer use policy that placed clear and conspicuous restrictions on the employees' access both to the system in general and to [a proprietary] databases in particular." In other words, "an employee 'exceeds authorized access' under [the CFAA] when he or she violates the employer's computer access restrictions including use restrictions." The court went on to say that "as long as the employee has knowledge of the employer's limitations on that authorization, the employee 'exceeds authorized access' when the employee violates those limitations. It is as simple as that."

In *Nosal*, the Ninth Circuit basically adopted the "Intended Use Theory" previously articulated by both the Fifth and Eleventh Circuits. The "Intended Use Theory" provides that an employee's own subjective changing of allegiances (which is sufficient according to the *Citrin* "Agency Theory"), is not sufficient by itself to terminate authorization to access data/computers; yet an employer is not required to expressly notify the employee that his access has been terminated either. Rather, the employer can implement certain restrictions on access and use of information obtained thereby, ahead of time by policies and agreements, that are known by the employee, and if the employee still violates those limitations by accessing information and using it for improper purposes–not for its intended use–that access will be considered as having been unauthorized for purposes of the Computer Fraud and Abuse Act.

To date, the Sixth Circuit has not addressed this issue. A limited number of district courts within the Sixth Circuit (but not the E.D. or W.D. of Michigan) have addressed the issue and have rejected the Seventh and First Circuit's broad reading of the CFAA, relying instead on the more narrow interpretation advanced by the Ninth Circuit in *Brekka*. In short, it appears as if district courts in the Sixth Circuit will rely on the strict language of the employer's computer/data access policy. No court in the Sixth Circuit has addressed the issue after the Ninth Circuit decided *Nosal*.

Implications for Employers

From an employer's standpoint, the *Nosal* case is very helpful – even though it is out of the Ninth Circuit. While it was a criminal case, the same standards of "access" that apply criminally under the CFAA also apply to civil actions. That is, it allows employers to implement clear and unambiguous policies that define the scope of permissible authorization for employees to access and use their computers as well as any data from those computers. If they have such policies, then under *Nosal*

employers may have a valid CFAA claim against employees who exceed that authorization. If they do not, and their employees have "unfettered access" to the computers and data, then under *Brekka* or the district court decisions out of the Sixth Circuit, the employer will not then be allowed to assert CFAA claims against them because the limitations on access were not set at the outset.

In other words, the lesson for employers is to have comprehensive computer access and data use policies specifying not only what portions of systems employees are permitted to access, but when access is granted, specifying the permitted uses associated with such access. It is also a good idea for more sophisticated employers to have an on-screen warning for access to sensitive data that reminds employees of the employer's policy and the proper use of such sensitive data.