Litigation Alert

Ninth Circuit Holds Computer Fraud and Abuse Act Criminalizes Employee's Access To Information In Violation Of Employer's Express Access Limitations

LAURENCE F. PULGRAM, TYLER G. NEWBY AND SEBASTIAN E. KAPLAN

FENWICK & WEST LLP

United States v. Nosal, No. 10-10038 (April 28, 2011) (Trott, J., O'Scannlain, J., Campbell, J.)

http://www.ca9.uscourts.gov/datastore/opinions/2011/04/28/10-10038.pdf

Summary

On Thursday, April 28, 2011, the Ninth Circuit, in a split decision, held that an employee could be criminally liable under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (the "CFAA"), for exceeding authorized access to an employer's computer system by accessing proprietary information in violation of the employer's written policies. In so holding, the Ninth Circuit joined several other circuits in interpreting the CFAA's "exceeds authorized access" prong to cover violations of an employer's clearly disclosed computer use policy to misappropriate proprietary company information. This interpretation of the CFAA also has ramifications outside the employment context, and potentially extends to enforceable terms of use policies and other contracts restricting network access.

Background of the Case

The facts of the case read like a garden-variety civil trade secret dispute. David Nosal had worked for the executive search firm Korn/Ferry International, which he left to start a competing firm. Soon after leaving the firm, Nosal engaged three Korn/Ferry employees to help set up the rival company. Those employees downloaded information about executive candidates from Korn/Ferry's password-protected leads database and provided that information to Nosal. All Korn/Ferry employees had been required to sign employment agreements prohibiting disclosure of such information.

In a federal criminal indictment, Nosal, was charged with violating § 1030(a)(4) of the CFAA, which imposes criminal liability for anyone 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." In light of the Ninth Circuit's decision in *LVRC Holdings LLC v. Brekka*, which construed the phrase "accesses . . . without authorization" to exclude the actions of individuals who had misused their otherwise authorized access to computer systems, the district court dismissed five of the eight counts against Nosal.

The Ninth Circuit's Decision

In reversing the district court, the Ninth Circuit held that "an employee 'exceeds authorized access' under § 1030 when he or she violates the employer's computer access restrictions—including use restrictions." Because the company had contractually prohibited its employees from disclosing information on its computer system to third parties, or from using the information except for legitimate business purposes, the employees exceeded their authorization when they violated that prohibition.

The Ninth Circuit distinguished *Brekka*, which addressed the CFAA's access *without* authorization prong, as opposed to the *exceeding* authorized access prong at issue in *Nosal*. Unlike the company in *Brekka*, Korn/Ferry had made its computer access and non-disclosure policies conspicuously clear to all its employees.

The Ninth Circuit addressed the concern that its interpretation of "exceeds authorized access" would make criminals out of employees who violated their employer's use policies by using work computers for personal reasons. It held that the government—and by extension, a plaintiff in a private civil action, which is also available to enforce the CFAA—would still need to satisfy the other elements of § 1030(a)(4). Those elements require proof that that (1) the defendant intended to defraud the company, (2) the computer access furthered that intent, and (3) the defendant obtained something of value through the access.

Implications

Nosal gives greater teeth to computer access and use policies, thereby improving companies' ability to deter both outsiders and insiders from stealing confidential business information. In *Nosal*, the computer use policy prohibited disclosure to outside parties and use other than for legitimate business purposes. Restrictions on disclosure create a bright line rule that puts employees on notice. Restrictions on the purpose of access—such as for legitimate business purposes—present greater vagueness problems. Although the majority did not explicitly criticize Korn/Ferry's restriction for legitimate business purposes, it effectively replaced that standard by focusing on the "intent to defraud" element. This suggests that companies may face difficulty enforcing a computer use policy where an employee's motivation falls in the gray area between a legitimate business purpose and outright fraud. Where possible, computer use policies should be drafted to prohibit actions, instead of intentions.

Employers' computer use policies, in addition to being clear, must be conspicuous. Korn/Ferry's policy was disclosed to employees at the time of hiring and each time an employee logged onto the Korn/Ferry computer system.

Nosal also has implications for restrictions on access to electronic information provided to customers or the public. A company that provides information on its website may be able to restrict the use of that information through enforceable Terms of Use. By the same token, companies who access information on an outside website should take note of what use restrictions exist. *Nosal*, however, involved the employment context, and the Ninth Circuit has not yet addressed whether the definition of access or authorization will be interpreted differently for non-employees.

For further information, please contact:

Laurence F. Pulgram, Partner, Litigation Group
lpulgram@fenwick.com, 415.875.2390

Tyler G. Newby, Of Counsel, Litigation Group and White Collar/Regulatory Group
tnewby@fenwick.com, 415.875.2495

Sebastian E. Kaplan, Associate, Litigation Group
skaplan@fenwick.com, 415.875.2477