Legal Insight

K&L GATES

www.klgates.com

April 17, 2012

Practice Group(s):

Labor and Employment

The Ninth Circuit Weighs In on the Scope of Liability Under the CFAA

By Michael Haven

On April 10, 2012, the United States Court of Appeals for the Ninth Circuit issued its decision *en banc* in *United States of America v. David Nosal*, rejecting the notion that employees who breach their employers' computer use policies by misusing information after it has been properly acquired may be in violation of the Computer Fraud and Abuse Act ("CFAA").

In *Nosal*, the government alleged that employees of executive search firm Korn/Ferry used the company's computers to access and download confidential information to assist David Nosal ("Nosal") – a former Korn/Ferry employee – in a competing venture. The employees were authorized to access the information, but disclosure to Nosal violated Korn/Ferry company policy.

The government charged Nosal with trade secret theft, mail fraud, and conspiracy, but also with violation of the CFAA, 18 U.S.C. § 1030(a)(4), for supposedly aiding and abetting the Korn/Ferry employees in "exceeding their authorized access" to the confidential information. Nosal moved to dismiss the CFAA counts, asserting that the statute does not apply to individuals who misuse information they are authorized to access.

The district court ultimately granted Nosal's motion upon a request for reconsideration, and the Ninth Circuit affirmed following consideration *en banc*.

The result in this case hinged on interpretation of the CFAA definition of "exceeds authorized access." Nosal construed the phrase to reference only individuals authorized to access certain files but who go beyond the authorization (i.e., "hacking"). The government took a broader view, asserting that the phrase could include individuals who have unrestricted access to information but are limited in its use.

The Court found Nosal's narrower interpretation of the statute to be more plausible, refusing to interpret the CFAA as "a sweeping Internet-policing mandate." It emphasized that the CFAA was enacted in 1984 to target the emerging problem of computer hacking, and that "[t]he government's construction of the statue would expand its scope far beyond computer hacking to criminalize any unauthorized use of information obtained from a computer," making "criminals of large groups of people who would have little reason to suspect they are committing a federal crime."

Under the government's interpretation of the statute, per the Ninth Circuit every violation of a private computer use policy could be construed as a federal crime, whether or not the user had culpable intent. In other words, employees who use their employer-issued computers to play games, chat with family members, shop online, or read the news at work could be charged with a criminal offense if those activities were prohibited by company policy.

Not so according to the Ninth Circuit, which held that the phrase "exceeds authorized access" in the context of the CFAA is limited to violations of restrictions on *access* to information, and not to restrictions on *use* of information. While employees who violate computer use policies still may be disciplined by their employers and may be at risk under other statutes (such as those which impose civil and criminal liability for misappropriation of trade secrets), they should not also be subject to criminal prosecution under the CFAA. Moreover, although the Nosal case involved a *criminal*

prosecution, the statutory language it interpreted is applicable to both civil and criminal violations. As a consequence, the Ninth Circuit's decision will likely impact *civil* actions brought under the CFAA as well.

This interpretation and refusal to apply the CFAA to certain computer related activities by employees is different from the approach taken by other federal courts. More specifically, other circuits have interpreted the CFAA to encompass violations of corporate limitations on use of information and violations of the duty of loyalty. *See, e.g.*, *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). Still, the Ninth Circuit urged its sister circuits to reconsider their holdings.

As a result of these conflicts in what the CFAA means and how it should be applied, the United States Supreme Court may ultimately take up the issue. In the meantime, at least within the geographic boundaries covered by the Ninth Circuit, the CFAA cannot be used to deter or punish employees for misusing company information they were authorized to access.

Authors:

Michael Haven
mike.haven@klgates.com
+1.650.798.6772