Akin Gump
Strauss Hauer & Feld LLP

Litigation Alert

Nosal: Ninth Circuit Narrowly Interprets Computer Fraud and Abuse Act

April 12, 2012

In *United States v. Nosal*, an en banc decision reached by the U.S. Court of Appeals for the Ninth Circuit on April 10, 2012, the court narrowly-construed the Computer Fraud and Abuse Act ("CFAA")—specifically the language "exceeds authorized access" contained within the statute.

Rejecting an expansive interpretation of the CFAA that found that violation of an employer's corporate computer use policy could qualify as "exceeding authorized access," the full panel, in an opinion authored by Chief Judge Alex Kozinski, affirmed the dismissal of a number of criminal charges against David Nosal, a corporate headhunter who had relied on former employer Korn/Ferry's confidential information to further his efforts to start a competing company. Nosal convinced former colleagues at Korn/Ferry to divulge to him confidential client information obtained from a Korn/Ferry database. Although such activity violated Korn/Ferry company policy, the employees all had authorized access to the confidential database.

The 9th Circuit was particularly concerned that the broad reading of the CFAA posited by the government in *Nosal* would inadvertently criminalize many innocuous computer uses routinely engaged in by millions of Americans in the workplace daily. To this point, Judge Kozinski wrote: "Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by g-chatting with friends, playing games, shopping or watching sports highlights. Such activities are routinely prohibited by many computer-use policies, although employees are seldom disciplined for occasional use of work computers for personal purposes. Nevertheless, under the broad interpretation of the CFAA, such minor dalliances would become federal crimes. While it's unlikely that you'll be prosecuted for watching Reason.TV on your work computer, you could be. Employers wanting to rid themselves of troublesome employees without following proper procedures could threaten to report them to the FBI unless they quit. Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement."

The decision was not without its detractors. Judge Barry Silverman authored a dissenting opinion which Judge Richard Tallman joined. Therein, Judge Silverman argued: "This case has nothing to do with playing sudoku, checking email, fibbing on dating sites, or any of the other activities that the majority rightly values. It has everything to do with stealing an employer's valuable information to set up a competing business with the purloined data, siphoned away from the victim, knowing such access and use were prohibited in the defendants' employment contracts." The dissent continued: "In ridiculing scenarios not remotely presented by this case, the majority does a good job of knocking down straw men- far-fetched hypotheticals involving neither theft nor intentional fraudulent conduct, but innocuous violations of office policy." (Emphasis in original).

Judge Kozinski also acknowledged that the 9th Circuit's interpretation of the CFAA in *Nosal* is contrary to the opinions of other circuits, namely *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); and *Int'l Airport Ctrs., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006). Judge Kozinski defended the majority's holding in Nosal nonetheless by stating that "[t]hese courts looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens."

www.twitter.com/akin_gump

It remains to be seen whether the government will seek review of the decision by the U.S. Supreme Court. The immediate practical impact of this ruling at least for employers in the 9th Circuit, is that fewer options are available for redressing computer related theft of trade secrets or other related improper computer activity by employees. Clients, particularly those in the 9th Circuit, should consider this ruling carefully when considering use of the CFAA against employee activity that violates rules on use of computer systems, and revisit the scope of their employees' access to sensitive company information.

CONTACT INFORMATION

If you have any questions regarding this alert, please contact—

Anthony T. Pierce
apierce@akingump.com
202.887.4411
Washington, D.C.

Anthony C. Hill
ahill@akingump.com
202.887.4172
Washington, D.C.

Karol A. Kepchar
kkepchar@akingump.com
202.887.4104
Washington, D.C.