FORD & HARRISON LLP
THE RIGHT RESPONSE AT THE RIGHT TIME
LETTER
NONCOMPETE NEWS

Noncompete News: Ninth Circuit Holds Employee Data Theft is Not Punishable Under the CFAA After All

4/16/2012

Executive Summary: In its much anticipated *en banc* decision, the Ninth Circuit refused to extend the Computer Fraud and Abuse Act ("CFAA") to employee data theft in *United States v. Nosal*. The Court declined to "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." This 9-2 decision reverses an earlier 3-judge panel decision and is at odds with other circuits (including the Fifth, Seventh, and Eleventh Circuits).

Background: The case involves former employee David Nosal who worked for Korn/Ferry, an executive search firm. He was charged with 20 criminal counts including trade secret theft, mail fraud, and violations of the CFAA. In the CFAA counts, the Government alleged that Nosal aided and abetted other Korn/Ferry employees to improperly download a confidential database and wrongfully transfer the information to Nosal so he could start a competing business.

A district court dismissed the indictment and held that the CFAA was only intended for computer hackers. A 3-judge panel for the Ninth Circuit reversed and found that the CFAA applies to situations where an employee "violates the employer's [computer] access restrictions." Nosal appealed the ruling and the Ninth Circuit agreed to re-hear the case *en banc*.

The CFAA Must Be Limited to an "Anti-Hacking" Statute Because Prosecution of Harmless Misconduct Could Lead to Discriminatory and Arbitrary Enforcement

The *en banc* opinion focuses much of its analysis on a concern for the potential overreaching consequences to employees who would have "little reason to suspect they are committing a federal crime." The CFAA defines "exceeds authorized access" as "to access a computer without authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[1] Congress enacted the CFAA in 1984 primarily to address the growing problem of computer hacking.

The Court rejected the Government's broad construction of the statute to include employees who exceed authorized access on their employer's computer because it would improperly include employees who innocently engage in harmless, social past times at work. "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." The imposition of criminal liability on such employees would be improper.

The Court also rejected the Government's argument that it would not prosecute minor violations of the CFAA and noted that "we shouldn't have to live at the mercy of our local prosecutor." If the CFAA granted that much power to prosecutors, the potential negative consequence is "inviting discriminatory and arbitrary enforcement."

The Court expressly declined to follow the Fifth, Seventh, and Eleventh Circuits that interpret the CFAA to broadly cover violations of corporate computer use restrictions or violations of a duty of loyalty. The Court stated that those circuits "failed to apply the long-standing principle that we must construe ambiguous criminal statutes narrowly so as to avoid making criminal law in Congress's stead."

The Dissenting Opinion Says the Majority's Concern for Employees Who Engage in Minor Distractions at Work Is Misguided

The dissenting opinion emphasized that this case did not involve an employee who was wrongfully charged with engaging in harmless internet activity at work. Instead, Nosal was accused of defrauding his employer by stealing confidential information to set up a competing business. In the dissenters' view, the majority's opinion is driven out of a well-meaning but misguided concern because an innocent violation of an employer's computer usage policy would not qualify as a violation of the CFAA since it requires an "intent to defraud."

Employers' Bottom Line: While employers may not be able to use the CFAA to protect themselves against employee data theft in California, employers are still able to utilize the California Uniform Trade Secret Act to remedy any misappropriation of their confidential data.

If you have any questions regarding this decision or other labor and employment issues, please contact the author of this article, Michelle B. Abidoye, mabidoye@fordharrison.com, an attorney in our Los Angeles office, or the editor of Noncompete News, Jeff Mokotoff, jmokotoff@fordharrison.com, a partner in our Atlanta office.

[1]18 U.S.C. § 1030(e)(6).