CONSTANGY
BROOKS & SMITH, LLP
The Employers' Law Firm, Since 1946

CLIENT BULLETIN

Client Bulletin #466

IS COMPUTER FRAUD AND ABUSE ACT FOR HACKERS ONLY? Ninth Circuit Says Yes, and Supreme Court May Have to Make Final Call

By Nathan Johnson
Madison, WI Office

Employers looking to hold employees liable for misappropriation of trade secrets or violations of company computer policies under the Computer Fraud and Abuse Act may have to find another avenue for relief. At least that's what the U.S. Court of Appeals for the Ninth Circuit thinks.

In its highly anticipated opinion, ***United States of America v. David Nosal***, the Ninth Circuit refused to reinstate criminal charges against a man who conspired with former colleagues to steal trade secrets from his former employer. The court held that the language of the CFAA is limited to violations of restrictions on *access*, not "misuse" -- in short, applying the CFAA to "hacking" only.

The Ninth Circuit decision creates a split in the circuits, which means that the issue may be resolved once and for all by the U.S. Supreme Court. (The Ninth Circuit hears appeals from federal courts in the states of Alaska, Arizona, California, Hawaii, Idaho, Montana, Nevada, Oregon, and Washington, and the territories of Guam and the Northern Mariana Islands.) U.S. Courts of Appeal in the **Fifth** (Louisiana, Mississippi, and Texas), **Eighth** (Arkansas, Iowa, Minnesota, Missouri, Nebraska, and the Dakotas), and **Eleventh** (Alabama, Florida, and Georgia) circuits have taken a contrary position, holding that employees who knowingly violate clear company computer restrictions agreements are thereby "exceeding authorized access." The Third Circuit (Delaware, New Jersey, Pennsylvania, and the Virgin Islands) has implicitly agreed with these other circuits.

The CFAA was passed by Congress in 1984 as a means to prevent hacking and address federal computer-related offenses. The statute provides criminal penalties for, among other things, knowingly accessing a protected computer with the intent to defraud and thereby obtaining anything of value. The statute also provides civil remedies.

In taking a restrictive view of the CFAA, the Ninth Circuit said, "Basing criminal liability on violations of private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved." Accordingly, employees may continue to visit sites like YouTube, Amazon, eBay, ESPN.com, www.dailysudoku.com, and Facebook without the threat of

indictment for a federal crime. (I'm being sarcastic here.) On the other hand, the restrictive view taken by the Ninth Circuit significantly limits the remedies available to employers whose current or former employees misappropriate trade secrets and other confidential information using computer systems.

If Only Checking Facebook and ESPN Were What Had Happened in This Case…

David Nosal was a former employee of the executive search firm Korn/Ferry. After his departure from the company, Nosal persuaded several of his former colleagues, still employed with Korn/Ferry, to start a competing agency. The employees used their login credentials to download source lists, names and contact information from Korn/Ferry's confidential databases, and transmit it to Nosal. The U.S. Department of Justice indicted Nosal on 20 counts, including mail fraud, conspiracy, trade secret theft, and violations of the CFAA. The CFAA counts charged Nosal with violations of 18 U.S.C. § 1030(a)(4), for "aiding and abetting the Korn/Ferry employees in 'exceed[ing their] authorized access' with intent to defraud."

Writing for the majority, Chief Judge Alex Kozinski refused to adopt the government's broad interpretation of the statute, because Nosal's accomplices had permission to access the company database and obtain the information within. Instead, the court held that the CFAA applies only to "*outside* hackers" and "*insider* hackers." The CFAA's "without authorization" language applies to "outside hackers" who have no authorized access to the computer at all. The "exceeds authorized access" language, on the other hand, applies to "inside hackers," or individuals whose initial access to a computer is authorized but who use it to access data that they are not authorized to have.

The problem in Nosal's case, in the court's view, was that Nosal's accomplices were authorized to access the employer's computer system and were authorized to have the information that they obtained – they just weren't authorized to provide the information to Nosal.

The court spent the remainder of its opinion discussing the underlying policy pitfalls avoided by its ruling. The CFAA defines "protected computer" as any computer affected by or involved in interstate commerce (that is, any computer with Internet access). Because the scope of computers covered by the CFAA is so expansive, a broad interpretation would make any violation of a private computer use policy a federal crime.

> Minds have wandered since the beginning of time and the computer gives employees new ways to procrastinate, by 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.

Thus, a narrow interpretation, according to the court, is more in line with the general purpose of the statute, which was intended to punish hacking. Accordingly, "the CFAA is limited to violations of restrictions on access to information, and not restrictions on its *use*."

What Should Employers Make of This?

Judge Silverman's dissent in *Nosal* points out the unnecessary hype injected into the majority's opinion. Much of the discussion regarding "playing Sudoku, checking email, fibbing on dating sites, or any of the other activities the majority rightly values," had nothing to do with the case, he said. Furthermore, "[i]n 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."

The Ninth Circuit's holding is binding only in the Ninth Circuit, but there it has certainly filed the teeth of the CFAA. The statute's knowing and intentional fraud component is no longer applicable to employees who defraud their employers. This limits employers' remedies to federal trade secret statutes, like 18 U.S.C. § 1832 which carries only criminal penalties, or to comparable state statutes. More broadly, the CFAA is no long an avenue to punish unauthorized *use* of information, but only its acquisition.

As stated above, by creating a split in the circuits, the *Nosal* decision increases the odds for review by the Supreme Court.

Even in the Ninth Circuit, the *Nosal* decision is not a reason for employers to shy away from regulating computer use by their employees. All employers should continue to develop and maintain employment agreements and policies that control computer use and the acquisition, disclosure, and use of the employer's confidential and proprietary information.

If you have any questions about this or other developments, please contact any member of Constangy's **Litigation Practice Group**, or the Constangy attorney of your choice.