PATTON BOGGS LLP

April 11, 2012

Ninth Circuit Gives a Narrow Interpretation of What Constitutes a Violation of the Computer Fraud and Abuse Act

Intellectual Property Client Alert

This Alert provides only general information and should not be relied upon as legal advice. This Alert may be considered attorney advertising under court and bar rules in certain jurisdictions.

For more information, contact your Patton Boggs LLP attorney or the authors listed below.

Scott A. Chambers, Ph.D.
schambers@pattonboggs.com

Richard Oparil
roparil@pattonboggs.com

Kevin Bell
kbell@pattonboggs.com

WWW.PATTONBOGGS.COM

On March 22, 2012, Patton Boggs LLP posted a client alert (available here) on the anti-hacking Computer Fraud and Abuse Act (CFAA), discussing that different federal courts were split on whether the CFAA imposes liability on employees who have permission to access computerized information but use the permitted access for an improper purpose. One of the cases discussed in that alert was *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), a panel decision holding that employees who properly access information but then use the information contrary to the employer's policies or against the employer's interests "exceeds authorized access" and violates the CFAA.

The full Ninth Circuit agreed to rehear the case, and in an April 11 ruling, a majority held that the CFAA is limited to violations of restrictions on *access* to information, and not restrictions on its use. The majority gave a narrow interpretation to the statutory phrase "exceeds authorized access." As a result of this decision, someone who is authorized to access only certain data or files but accesses other data or files would violate the CFAA. In his opinion for the Court, Chief Judge Kozinski gave an example of how a violation could occur: "For example, assume an employee is permitted to access only product information on the company's computer but accesses customer data: He would 'exceed[] authorized access' if he looks at the customer lists."

The Court rejected the Government's argument that the CFAA also covers someone who has unrestricted physical access to a computer, but is limited in the use to which she can put the information. Under that interpretation, which other courts had adopted, an employee authorized to access customer lists in order to do her job violates the CFAA if she sends the list to a competing company.

Chief Judge Kozinski, however, was concerned about the potential for a broadly interpreted CFAA to ensnare innocent conduct:

> Basing criminal liability on violations of private computer use polices can transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved. Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of *The New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.

The Ninth Circuit decision recognized that Courts of Appeals for the Fifth, Seventh and Eleventh Circuits have interpreted the CFAA broadly and they would find that violating a computer use restriction is a violation of the statute. Chief Judge Kozinski's opinion wrote that the other appellate courts were wrong and urged them to reconsider.

Two of the 11 judges rehearing the case dissented, with Judge Silverman opining that: “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 stated that the majority misread the CFAA.

The en banc decision in *Nosal* (available here) sets up a clear conflict among Circuit courts on the proper interpretation of the CFAA, making it possible that the U.S. Supreme Court would finally decide the issue. As discussed in our earlier alert, companies should adopt policies that clearly define employees’ access to computerized information and limit its use to proper corporate purposes.