

Federal Appellate Court Limits the Computer Fraud and Abuse Act's Scope

Article By:

Product Liability and Mass Torts

In the Ninth Circuit, the **Computer Fraud and Abuse Act ("CFAA")** no longer provides a remedy to employers whose data is taken by disloyal employees. On April 10, 2012, the Ninth Circuit Court of Appeals held, in an en banc decision in ***United States v. Nosal***, 2012 WL 1176119 (9th Cir. Apr. 10, 2012), that the CFAA does not "cover violations of corporate computer use restrictions or violations of a duty of loyalty." This decision conflicts with decisions from the Fifth, Seventh and Eleventh Circuits.

Background

Generally speaking, the CFAA prohibits obtaining information or data by accessing a computer "without authorization" or in "excess of authorization." 18 U.S.C. § 1030(a)(1)-(4). The CFAA provides both criminal penalties and civil remedies. Although the CFAA was originally intended to protect only government computers from attacks by outside hackers, amendments have broadened its reach. Some courts read the CFAA as prohibiting computer abuse committed by private employees and other corporate "insiders." However, a split of authority has developed regarding the CFAA's application to private employees.

That split consists of three general approaches. The Seventh Circuit has ruled that insiders, such as disloyal employees, may be unauthorized computer users who fall within the statute's ambit. The Fifth and Eleventh Circuits look to the employer's contracts and policies to determine whether a disloyal employee's computer conduct is without "authorization," and therefore prohibited by the CFAA. The Ninth Circuit has now confined the CFAA to its anti-hacking roots and applies its provisions only to non-employee outsiders. Although a number of district courts had held that the CFAA does not apply to "insiders," no circuit court had taken that view - until *Nosal*.

The Ninth Circuit's Ruling

In *United States v. Nosal*, the Ninth Circuit read the CFAA as "an anti-hacking statute" rather than as "an expansive misappropriation statute," and therefore held that "the CFAA does not extend to violations of use restrictions" found in employee policies or agreements. In *Nosal*, the defendant convinced his former colleagues to violate an employment policy by downloading and disclosing their employer's confidential information to help him start a competing business. The government indicted

Nosal on 20 counts, including trade secret misappropriation and CFAA violations (aiding and abetting his former colleagues). Nosal moved to dismiss the CFAA counts, arguing that the CFAA targets hackers, not individuals who misuse information obtained through authorized computer access.

The Ninth Circuit agreed with Nosal, reading "exceeds authorized access" to mean hacking, not misusing or misappropriating computer information. Specifically, the court held that "'exceeds authorized access' in the CFAA is limited to violations of restrictions on access to information, and not restrictions on its *use*." Now, in jurisdictions governed by the Ninth Circuit (California, Nevada, Arizona, Hawaii, Washington, Alaska, Idaho, Montana and Oregon), the CFAA will not permit criminal liability under the CFAA for employees' violations of private employers' computer use policies.

What It Means

It is not yet clear whether the government will petition the Supreme Court to review the Ninth Circuit's ruling. However, in light of *Nosal*, employers - particularly those that are located in, or that employ people located in, the Ninth Circuit - may wish to rethink how they protect their electronic information from employee misuse or misappropriation. Furthermore, although employers located in the Ninth Circuit must rely on other tools to combat and respond to data theft by employees, the CFAA may be available to those in other jurisdictions - particularly if appropriate computer and email usage policies are in place. Such policies might be updated to clearly state, for example, that employees are not authorized to use the company's email and other computer systems to access, download or transmit company data for competitive purposes or for any other purpose contrary to the company's interest.

© 2025 ArentFox Schiff LLP

National Law Review, Volume II, Number 114

Source URL: <https://natlawreview.com/article/federal-appellate-court-limits-computer-fraud-and-abuse-act-s-scope>