

Second Circuit Adopts Narrow Construction of Federal Computer Fraud Statute, Joins Circuit Split

By Clifford R. Atlas and Ravindra K. Shaw

December 10, 2015

Ruling that under the federal Computer Fraud and Abuse Act (CFAA), an individual “exceeds authorized access” *only* when he obtains or alters information on a computer that he does *not* have authorization to access for *any* purpose, the federal appeals court in New York has reversed the conviction of a former police officer. *United States v. Valle*, 2015 U.S. App. LEXIS 21028 at *4 (2d Cir. Dec. 3, 2015). The Second Circuit has jurisdiction over Connecticut, New York, and Vermont. The Second Circuit joins the Fourth and Ninth Circuits in adopting a narrow interpretation of the civil and criminal statute.

When an employee who has been granted access to an employer’s computer misuses that access, either by violating the employer’s terms of use or by breaching a duty of loyalty to the employer, employers have argued that the employee has violated the federal CFAA because the employee has “exceed[ed] authorized access” or acted “without authorization” as those terms are defined in the CFAA. Federal appellate courts are split on whether those terms should be interpreted broadly or narrowly. The First, Fifth, Seventh, and Eleventh Circuits have adopted a broad construction, allowing CFAA claims alleging an employee misused employer information that he or she was otherwise permitted to access.

With a growing split in the circuits, the likelihood of U.S. Supreme Court review increases.

Background

Gilberto Valle was an officer in the New York City Police Department (NYPD) who had access to a computer program that allowed officers to search certain restricted databases containing sensitive information about individuals, obtaining such information as home addresses and dates of birth. However, the NYPD’s policy provided that these databases could be accessed only in the course of an officer’s official duties, not for personal use.

According to the Second Circuit decision, Valle was an active member of an Internet sex fetish community in which he discussed with other Internet users committing horrific acts of sexual violence, such as kidnapping, torturing, cooking, raping, murdering, and cannibalizing women.

Valle used his database access at the NYPD to search for a woman he had known since high school and had discussed kidnapping with another Internet user. Because he had no law enforcement purpose for accessing that information, Valle was convicted by a jury of improperly accessing a government computer and obtaining information in violation of the CFAA.

Valle appealed and the Second Circuit reversed the judgment of conviction for violating the CFAA.

Not Every Policy Violation Qualifies

The CFAA imposes both criminal and civil liability on an individual who intentionally accesses a computer “without authorization” or “exceeds authorized access” and, thereby, obtains information from the computer.

“Without authorization” is not defined in the statute. “Exceeds authorized access” is defined in the statute to mean accessing a computer with authorization and using such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter.

Valle conceded that he violated NYPD policy by putting his authorized computer access to personal use. Nonetheless, he argued he did not violate the CFAA because he never used his access to obtain any information that he was not entitled to obtain, and his non-law enforcement purpose in running a

Meet the Authors



[Clifford R. Atlas](#)

Principal
New York Metro
New York City 212-545-4017
Email



[Ravindra K. Shaw](#)

Principal
New York Metro
New York City 212-545-4041
Email

search for a woman he knew from high school was irrelevant.

The Second Circuit found the intended scope of the statute was in doubt. The Court said “authorization” could refer broadly to the purposes for which one is authorized to access a computer or more narrowly to the particular files or databases in the computer to which one’s authorization extends.

The Court reviewed the legislative history and motivating policies of the statute and found support for both broad and narrow interpretations of the statute. Under a rule of lenity, the Court determined that doubts about the scope of the statute should be resolved in favor of the defendant.

The Court noted that a broad interpretation of the CFAA would allow private parties to manipulate their computer-use and personnel policies to turn their relationships into ones policed by the criminal law. Consequently, any employee who, for example, checked sports scores in violation of his employer’s use policy could be left without any authorization to access his employer’s computer systems and be subject to criminal penalties.

In effect, the Court declined to rely on prosecutors or employers to determine responsibly whether to prosecute or sue individuals for computer activities at work that may range from innocuous (*e.g.*, checking Facebook) to nefarious (*e.g.*, downloading customer lists). A narrow construction of the statute, the Court said, ensures that every violation of a private computer use policy does not become a federal crime or federal lawsuit.

In the Second, Fourth, and Ninth Circuits, employers’ claims under the CFAA are limited and must be based on the actions of employees who lack permitted *access* to information on computers, not the actions of employees who exceed a permitted *use* of employers’ information under company policies. However, employers may assert traditional state law claims against employees for breaching restrictive covenant agreements and misappropriating trade secrets.

Jackson Lewis attorneys are available to answer questions regarding this case and other workplace developments.

©2020 Jackson Lewis P.C. This material is provided for informational purposes only. It is not intended to constitute legal advice nor does it create a client-lawyer relationship between Jackson Lewis and any recipient. Recipients should consult with counsel before taking any actions based on the information contained within this material. This material may be considered attorney advertising in some jurisdictions. Prior results do not guarantee a similar outcome.

Focused on labor and employment law since 1958, Jackson Lewis P.C.’s 950+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged, stable and diverse, and share our clients’ goals to emphasize inclusivity and respect for the contribution of every employee. For more information, visit <https://www.jacksonlewis.com>.