THE NATIONAL LAW JOURNAL
JANUARY 4, 2016
An ALM Publication
THE PRACTICE | Commentary and advice on developments in the law

'Cannibal Cop' Decision Restrains Employers

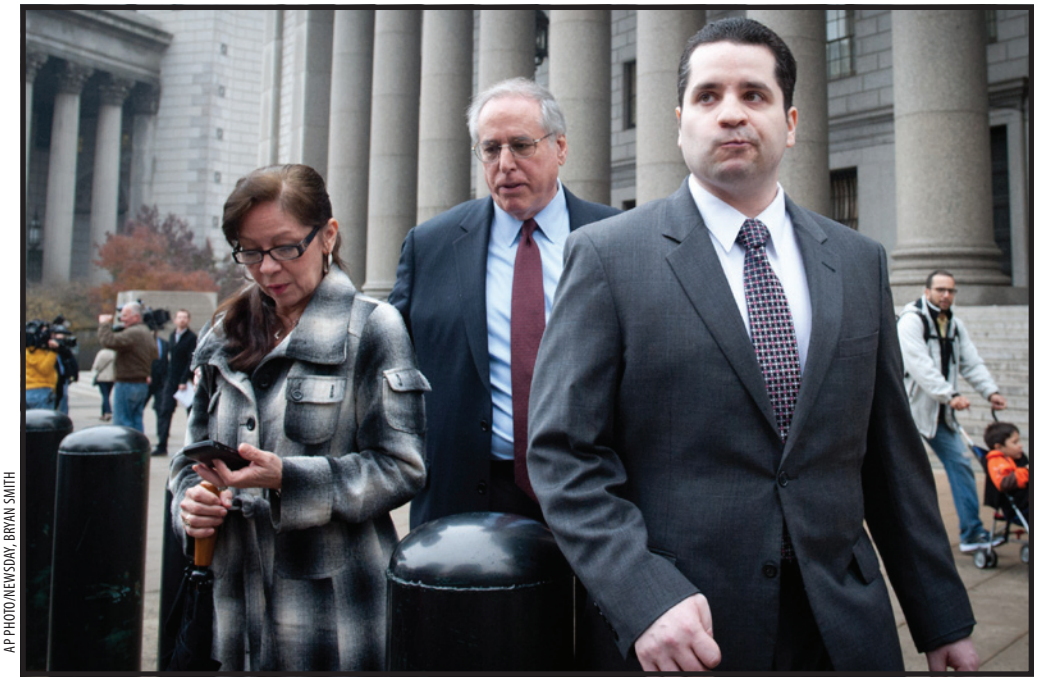
Second Circuit ruling on data theft creates more inconsistency regarding federal law's reach.

BY NICK AKERMAN

In December, a divided panel of the U.S. Court of Appeals for the Second Circuit in *U.S. v. Valle* interpreted the Computer Fraud and Abuse Act to exclude employees who access their employer's computers. The upshot is that if you are an employee in the Second Circuit and steal data from your employer to commit identity theft or to provide it to a competitor, you cannot be prosecuted by the Department of Justice or sued by your employer under the CFAA.

The CFAA, although principally a criminal statute, under Section 1030(g) permits a company to bring a civil action for damages and injunctive relief when it is the victim of computer crime.

Valle sided with the Fourth and Ninth circuits and rejected the contrary positions of the First, Fifth, Seventh and Eleventh circuits, further exacerbating a split in the circuits on the use of the CFAA against employees. *Valle* also directly implicates how employers should draft their computer policies as a predicate to take advantage of the CFAA.



AP PHOTO/NEWSDAY, BRYAN SMITH

GILBERTO VALLE: The ex-NYPD officer, right, was prosecuted for obtaining information from a database in connection with sexual fetishism.

Valle involves particularly grisly facts. Gilberto Valle, a New York City Police Department officer, according to the decision, was "an active member of an Internet sex fetish community called Dark Fetish Network." Valle engaged in "chats" consisting "of gruesome and graphic descriptions of kidnapping, torturing, cooking, raping, murdering, and cannibalizing various women."

As a member of the NYPD, Valle had access to "various restricted databases," including a federal law enforcement database "contain[ing] sensitive information about individuals such as home addresses and dates of birth." NYPD policy strictly limited Valle's access to those databases to searches relating to his "official duties" and made it a violation of "department rules" to access these databases for nonlaw enforcement "personal use" punishable by "termination and prosecution." In violation of this policy,

Valle accessed the federal database to obtain information on one of the woman he was plotting to kidnap and cannibalize. Based on this access, Valle was convicted by a jury for violating the CFAA, which makes it a crime for anyone who "intentionally … exceeds authorized access [to a government computer], and thereby obtains … information from any department or agency of the United States."

The CFAA defines "exceeds authorized access" as "access[ing] a computer with authorization" to obtain "information in the computer that the accesser is not entitled so to obtain."

The court reversed Valle's conviction, finding he did not exceed authorized access because "he was otherwise authorized to obtain the database information about" the woman. That he did so for a "non-law enforcement purpose" in violation of NYPD policy, to the court, was "irrelevant."

Relying on the "sharp division" in the circuits on the meaning of "exceeds authorized access" and the statute's mixed legislative history, the court found "that the statute is readily susceptible to different interpretations" and invoked "the rule of lenity to adopt the interpretation that favors the defendant." The court expressed concern with the "risk of criminalizing ordinary behavior inherent in its broad construction," such as "prosecut[ing] an individual for checking Facebook at work."

The dissent argued that the rule of lenity did not apply because "the statute's language is plain and unambiguous" and concluded, that "under the plain language of the statute, Valle exceeded his authorized access to a federal database in violation of the CFAA" by violating the NYPD policy that limited access only for the purpose of official police business.

MICHIGAN COURT'S RULING

Although not referenced by the dissent, a recent Michigan district court decision, *American Furukawa v. Hossain*, found that an employee's purpose in accessing the company computer is appropriate and held that "foreclosing purpose and use restrictions by employers, simply conflicts with the plain language of the statute." The court criticized the Ninth Circuit because it "never clearly explains why the CFAA's plain language does not permit computer owners to 'spell out explicitly what is forbidden' on its computers."

Furukawa also emphasized the inherent conflict in the Ninth Circuit's position allowing the CFAA to be used against an employee who "circumvents" technological "security measures" but not when the employee violates written computer policies. The court found no "difference between an employee who circumvents 'security measures,' and an employee who circumvents explicit computer limitations provided by an employer for employees regarding the employee's access, use, or purpose when accessing the employer's systems." The court said "such explicit policies are nothing but 'security measures' employers may implement to prevent individuals from doing things in an improper manner on the employer's computer systems."

Based on the current state of the law, and absent resolution by the U.S. Supreme Court or a congressional amendment, employers should take these steps:

First, establish policies proscribing the scope of permitted access to the company computers that will, as of now, at least be enforceable in all jurisdictions except the Second, Fourth and Ninth circuits.

Second, include among these policies explicit restrictions on how an employee is permitted to access the employer's data. For example, in *Furukawa* the court upheld a removable-media policy that "explicitly requires permission from a manager before accessing files with removable media." The court held that even under a narrow interpretation of "exceeds authorized use," this policy was a proper predicate for a violation of the CFAA because it "was focused on how" the employee "accessed" the employer's files.

NICK AKERMAN *is a partner in the New York office of Dorsey & Whitney, where he focuses on the Computer Fraud and Abuse Act, the Racketeer Influenced and Corrupt Organizations Act, federal trade secrets law and postemployment restrictive covenants.*