Nick Akerman
(212) 415-9217 ▪ akerman.nick@dorsey.com

Nick is a partner in the New York office of Dorsey & Whitney

For additional articles like this one or to watch my one hour CLE seminar video go to:
http://computerfraud.us

DORSEY
DORSEY & WHITNEY LLP

High Court May Rule on Computer Law Question

At issue is whether the Computer Fraud and Abuse Act applies to data theft by employees; the circuits are split.

By Nick Akerman

On July 26, the U.S. Court of Appeals for the Fourth Circuit became the first circuit to adopt the Ninth Circuit's holding in *U.S. v. Nosal,* 676 F.3d 854 (9th Cir. 2012), that the Computer Fraud and Abuse Act does not apply to employees who steal data from the company computers. *WEC Carolina Energy Solutions LLC v. Miller*, 2012 WL 3039213 (4th Cir. July 26, 2012). This case places the Fourth and Ninth circuits in direct conflict with the First, Third, Fifth, Seventh, Eighth and Eleventh circuits, increasing the odds that the U.S. Supreme Court will address this issue at some point.

The CFAA, the federal computer crime statute, allows individuals or companies victimized by violations of the statute to bring a civil action against the perpetrator. U.S.C. 1030(g). For a theft of data a plaintiff must prove that the defendant accessed the computer "without authorization" or exceeded his authorized access. The conflict among the circuits centers on what it means to access a computer without authorization. This article will examine the scope of this issue and the likelihood that the Supreme Court will resolve this conflict in favor of the more expansive meaning of "without authorization."

The complaint in WEC alleges the classic employee theft of data: Willie Miller, immediately prior to his resignation from WEC to join a competitor, downloaded WEC's confidential and trade-secret information from his company-issued laptop computer at the direction of his new employer and thereafter used it on behalf of his new employer to obtain business from two WEC customers. WEC's policies, while not directly restricting his "authorization to access the information," prohibited him from "using the information without authorization or downloading it to a personal computer." 2012 WL 3039213, at *1.

The Fourth Circuit in *WEC*, like the Ninth Circuit in *Nosal*, interpreted the key element of accessing the computer "without authorization" or exceeding "authorized access" narrowly to hold that the CFAA applies "primarily" to outside hackers and "that an employee is authorized to access a computer when his employer approves or sanctions his admission to that computer." *Id.* at *4. *Nosal* went even further to engraft upon "without authorization" the requirement that the defendant's access involve "the circumvention of technological barriers" to the computer. 676 F.3d. at 863.

Challenging the Seventh Circuit

Both *WEC* and *Nosa*l take direct issue with Judge Richard Posner's holding in *Int'l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006), that "when an employee accesses a computer or information on a computer to further interests that are adverse to his employer, he violates his duty of loyalty, thereby terminating his agency relationship and losing any authority he has to access the computer or any information on it." In rejecting this "cessation-of-agency theory," the court in *WEC* stated that "[s]uch a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems." 2012 WL 3039213, at *6.

The Ninth Circuit rejected *Citrin* on the basis that "[n]othing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer." *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009). However, both the Ninth and Fourth circuits ignore the Supreme Court's decision in *Carpenter v. U.S.*, 484 U.S. 19 (1987), which relied on the same state law agency principles to uphold a "scheme to defraud," the key element of the mail and wire fraud statutes.

Carpenter affirmed the conviction of a *Wall Street Journal* reporter who, prior to publication, had provided his upcoming financial columns to confederates, who bought or sold stock "based on the probable impact of the column on the market." *Id.* at 23. The court held that "an employee has a fiduciary obligation to protect confidential information obtained during the course of his employment," and intentionally exploiting that information for his own personal benefit constituted a scheme to defraud his employer of confidential information. *Id.* at 29.

WEC also incorrectly stated that only "two schools of thought exist" between *Nosal* and *Citrin*. 2012 WL 3039213, at *3. What *Nosal* and *WEC* fail to address is that the other circuits simply interpret "without authorization" unqualifiedly to mean lack of permission. Thus, the Fifth and Eleventh circuits have found lack of permission based limits on access and enhancing control by information providers." *EF Cultural Travel B.V. v. Zefer Corp*, 318 F.3d 58, 63 (1st Cir.2003). Thus, a company "can easily spell out explicitly what is forbidden" through its policies. *Id.*

The Fifth Circuit in *U.S. v. John*, 597 F.3d 263, 269, 272 (5th Cir. 2010), held that a Citigroup account manager, who accessed Citigroup's internal computer system to provide her brother with customer account information that he used to perpetrate fraudulent charges, had exceeded authorized access based on "Citigroup's official policy, that…prohibited misuse of the company's internal computer systems and confidential customer information." *Id*. at 272. Similarly, the Eleventh Circuit relied on company rules in *U.S. v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), to affirm the CFAA conviction of a Social Security Administration employee

who accessed Social Security information for personal reasons in violation of the agency's policy against "obtaining information from its databases without a business reason." *Id.*

The Third and Eighth circuits have found unauthorized access to the company computer when the access was done without a legitimate business purpose. The Third Circuit in *U.S. v. Tolliver*, 2011 WL 4090472, at *5, found unauthorized access by a bank teller who provided customer information to fraudsters who siphoned funds from customers' accounts because "she did not have a business purpose" to access those accounts. The Eighth Circuit in *U.S. v. Teague*, 646 F.3d 1119 (8th Cir. 2011), similarly found unauthorized access by an employee of a government contractor for the Department of Education who viewed President Obama's student loan records without any legitimate business purpose.

Concern Over Innocent Activities

In the final analysis, the driving force that separates *Nosal* and *WEC* from the other circuits in narrowly defining "without authorization" is a concern that "private computer use policies can transform whole categories of otherwise innocuous behavior into federal crimes," for example, that an employee "could be prosecuted" for innocent activities such as watching television on his "work computer." *Nosal,* 676 F.3d at 860; see also, *WEC*, 2012 WL 3039213, at *6.

There are two reasons why the Supreme Court is unlikely to share this concern. First, the precise same arguments could be leveled at the federal mail and wire fraud statutes because they could be used to prosecute individuals for stealing paltry sums of money through the wires or mails under circumstances that should not be criminalized, yet the court has persistently upheld both statutes. Second, based on its recent decision in *Morrison v. National Australia Bank Ltd*., 130 S.Ct. 2869, 2881 n.5 (2010), in which the court criticized "judicial lawmaking," it is highly unlikely that the Supreme Court, without any support in the plain language of the statute, will interpret "without authorization" to exclude employees.