

## BUSINESS INFORMATION

### Recent CFAA cases

**E**ARLY THIS YEAR, three separate circuit courts—the 5th U.S. Circuit court of Appeals in *U.S. v. Phillips*, 477 F.3d 215 (5th Cir. 2007); the 8th Circuit in *U.S. v. Trotter*, 478 F.3d 918 (8th Cir. 2007); and the 10th Circuit in *U.S. v. Willis*, 476 F.3d 1121 (10th Cir. 2007)—affirmed criminal convictions for violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030. While the CFAA is primarily a criminal statute, it provides for a private right of action for injunctive relief and compensatory damages for anyone “who suffers damage or loss by reason of a violation of” the statute. 18 U.S.C. 1030(g).

In rejecting the defendants’ challenges to their criminal convictions, these opinions provide an expansive view of the CFAA that enhances the ability of companies to use the statute’s civil remedy to combat computer crime. Such a proactive, self-help approach of prosecuting a civil action is more likely in many instances to produce quicker and more certain relief than a criminal prosecution brought by the U.S. Department of Justice. This article will review these three circuit decisions and their impact on a company’s ability to use the CFAA to retrieve stolen data, enjoin illegal access to company data and obtain compensatory damages for the theft and destruction of company data.

**Nick Akerman** is a partner in the New York office of *Dorsey & Whitney* who specializes in the protection of trade secrets and computer data.

By Nick Akerman



#### 8th Circuit rejected narrow interpretation in ‘Trotter’

In *Trotter*, the defendant, John Trotter, was a disgruntled former Salvation Army employee who had been discharged from his position as an information technology supervisor. Shortly after his discharge, the defendant accessed the Salvation Army’s computer network and deleted files, “shut down” the “computer-operated phone system” and “inserted several files with obscenities directed towards the Salvation Army.” 478 F.3d at 919. Trotter was convicted of violating § 1030(5)(A)(i) of the CFAA for causing damage to the Salvation Army computer network. Trotter, arguing for a narrow interpretation of the CFAA, claimed that “the Salvation Army’s computer network was not a ‘protected computer,’” and that because all computers “[these] days are used somehow in interstate commerce through the [I]nternet or private networks,” the CFAA “cannot possibly be so broad as to cover the computer network of a not-for-profit organization like the Salvation Army.” Id. at 921.

The 8th Circuit rejected Trotter’s challenge to the CFAA, holding that “[t]he Salvation Army’s status as a not-for-profit entity has no bearing” on the scope of the statute but “it is the characteristics of the computer or computer network, not the entity using the network, that is the focus of the statute.” Id. Because the Salvation Army’s computer was connected to the Internet, which is an “instrumentality and channel of interstate commerce,” the court held that “Congress has the power to protect it.” Id. at 921-22. The court further held that whether the defendant’s actions in violating the CFAA were wholly intrastate was of no legal significance. “Once the computer is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire.” Id. at 922, quoting *U.S. v. Mitra*, 405 F.3d 492, 496 (7th Cir. 2005).

*Willis*, rather than addressing a constitutional challenge to the CFAA, interpreted the language of the statute to apply to the theft of company data used to perpetrate identity theft. The defendant, Todd Willis, was employed by a debt-collection agency “as a small claims supervisor” with “significant responsibility for the computers.” 476 F.3d at 1123. Willis, in exchange for drugs, had provided an associate of his drug dealer with “access to individuals’ addresses, social security numbers, dates of birth, etc” from the company’s computers. These stolen data were “used to make false identity documents, open instant store credit at various retailers, and...purchase goods that were later sold for cash.” Id. Willis was convicted of aiding and abetting a violation of § 1030(a)(C)(2) for intentionally accessing his employer’s computer network without

authorization to obtain information from the computer in which his conduct involved an interstate communication.

Willis argued on appeal that for him to aid and abet a violation of this specific CFAA section, the government must prove that he had an “intent to defraud,” and because he did not know that the information obtained from his employer’s computer would be used “to commit identity theft,” there was insufficient proof that he had an intent to defraud. *Id.* at 1125. The 10th Circuit rejected Willis’ argument that the “intent to defraud” element of § 1030(a)(4) of the CFAA should be imputed to § 1030(a)(2)(C), the section of the CFAA for which he had been convicted. The court explained that “[a] plain reading of the statute reveals that the requisite intent to prove a violation of § 1030(a)(2)(C) is not an intent to defraud (as it is under (a)(4)), it is the intent to obtain unauthorized access of a protected computer.” *Id.* Thus, the court concluded that “[t]he government need not also prove...the information was used to any particular ends.” *Id.* The court emphasized “that each subsection of § 1030 [of the CFAA] addresses a different type of harm” requiring proof of different elements. *Id.* at 1126.

Also interpreting the language of the statute, the 5th Circuit in *Phillips* provided the most expansive meaning to date of the statutory term “without authorization,” a critical element of five of the seven violations in the CFAA that can form the basis for a civil suit.

Christopher Phillips was a student in the Department of Computer Sciences at the University of Texas and as such, signed U.T.’s acceptable-use computer policy, in which he agreed not to perform certain scans on his university computer account that would permit him to search for vulnerabilities to hack into and attack the network. The principal action for which Phillips was prosecuted was his hacking into a U.T. secure server that only allowed access to an authorized user through a password which was the user’s Social Security number. Phillips hacked into the network through what is known as a “brute-force attack” program, which automatically transmitted to the website as many as six Social Security numbers per second, at least some of which would correspond to those of authorized... users.” 477 F.3d at 218. This program allowed Phillips “[o]ver a fourteen-month period” to gain “access to a mother lode of data about more than 45,000 current and prospective students, donors, and alumni.” *Id.*

Phillips was convicted of violating

§ 1030(a)(5)(A)(ii) of the CFAA for knowingly accessing the U.T. network without authorization and recklessly causing damage to the network. On appeal, Phillips claimed that the government had failed to prove his access to the computer network was “without authorization.” The court summarized the recent law that “authorized access typically arises only out of contractual or agency relationship.” *Id.* at 221. In doing so, the court cited with approval two CFAA civil cases—the 7th Circuit’s opinion in *Int’l Airport Ctrs. LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), which held that an employee’s authorization to the company computers is governed by the law of agency, and the 1st Circuit’s opinion in *EF Cultural Travel B.V. v. Explorica Inc.*, 274 F.3d 577 (1st Cir. 2001), where the “confidentiality agreement defined authorized access to [the plaintiff] travel company’s computerized pricing information.” 477 F.3d at 221 n.5.

## Three criminal cases provide an expansive view of the Computer Fraud and Abuse Act—a boon to companies bringing civil cases.

The court, however, expanded the definition of “without authorization” beyond the rulings of the 1st and 7th circuits and held that “the scope of a user’s authorization to access a protected computer” under the CFAA may be determined based “on...the expected norms of intended use” of the computer. *Id.* at 219. The court not only found that Phillips’ activities were not authorized by U.T.’s acceptable-use computer policy that he had signed, but that “Phillips’s brute-force attack program was not an intended use of the UT network within the understanding of any reasonable computer user and constitutes a method of obtaining unauthorized access to computerized data that he was not permitted to view or use.” *Id.* at 220.

The court’s intended-use test was based

on the 2d Circuit’s opinion in *U.S. v. Morris*, 928 F.2d 504, 510 (2d Cir. 1991), where the court “determined that conduct, like ‘password guessing’ or finding ‘holes in... programs,’ that uses computer systems not ‘in any way related to their intended function’ amounts to obtaining unauthorized access.” 477 F.3d at 220.

The *Phillips* court also relied on dicta in *Explorica*, mentioning “the district court’s observation of a ‘default rule’ that conduct is unauthorized for § 1030 purposes ‘if it is not in line with reasonable expectations of the website owner and its users.’” *Id.* The court, however, overlooked a subsequent and related 1st Circuit case that expressly rejected the “reasonable expectations” test, labeling it as a “highly imprecise, litigation-spawning standard.” *EF Cultural Travel B.V. v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003).

## Principles set in these cases will apply to civil cases, too

In sum, the following principles established in these three criminal appellate decisions directly affect the civil arena for a company choosing to use the CFAA to remedy criminal acts directed at its computer data: First, the CFAA applies to all companies, whether for profit or not for profit and all computers as long as they are connected to the Internet. Second, the CFAA contains seven separate violations with distinct and separate elements that can predicate a civil suit that can reach a wide variety of computer crime. Third, depending on which circuit governs the jurisdiction where the case is filed, the lack of authorization can be alleged and proven based on a breach of the agency relationship; a breach of an employment contract such as a violation of company rules; or a use of the computer that exceeds expected norms of intended use.