

COMPUTER DATA

'Unauthorized Access'

UNAUTHORIZED ACCESS to a computer is a critical element to proving most violations of the federal Computer Fraud and Abuse Act (CFAA), 18 U.S.C. 1030, et seq. The CFAA is a criminal statute outlawing various acts relating to computers, including the theft of data, and it provides for civil remedies to anyone injured by a violation of the statute. 18 U.S.C. 1030(g). *Shurgard Storage Centers Inc. v. Safeguard Self Storage Inc.*, 119 F. Supp. 2d 1121, 1124-25 (W.D. Wash. 2000), decided five years ago, addressed "unauthorized access" in the context of employees who allegedly e-mailed their employer's trade secrets from the company computer to a direct competitor that was about to become their new employer.

The defendant new employer argued that the employees' use of the computers to e-mail the trade secrets could not, as a matter of law, be "unauthorized access" under the CFAA because the employees, as part of their job responsibilities, "had full access to all the information allegedly transferred." For that reason the defendant argued that the statute was "limited to 'outsiders' or 'hackers,' and not 'insiders' (employees)." Relying on the Restatement (Second) of Agency § 112 (1958), the court rejected an outside hacker limitation to the CFAA and held that the authorization of the "employees [to access the company computer] ended when they allegedly became agents of the defendant," and thus "lost their authorization and were 'without authorization' when they allegedly obtained

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

By Nick Akerman



and sent the trade secrets to the defendant via e-mail." *Id.* at 1124, 1125, 1127.

Over the past five years, other federal courts have followed the *Shurgard* ruling. See, e.g., *Charles Schwab & Co. v. Carter*, No. 04 C 7071, 2005 WL 351929, at *3 (N.D. Ill. Sept.

'Werner-Matsuda' bucking the trend, held that Computer Fraud and Abuse Act did not apply to an insider, only to outside hackers.

27, 2005); *George S. May Int'l Co. v. Hostetler*, No. 04 C 1606, 2004 WL 1197395, at *3 (N.D. Ill. May 28, 2004). As a result, one court recognized "the seemingly growing trend

utilizing the CFAA in employer-employee litigations." *Pacific Aerospace & Electronics Inc. v. Taylor*, 295 F. Supp. 2d 1188, 1197 (E.D. Wash. 2003).

'Werner-Matsuda' limited CFAA to outside hackers

The first challenge to this growing trend occurred three months ago in *Int'l Assoc. of Machinists and Aerospace Workers v. Werner-Matsuda*, 390 F. Supp. 2d 479, 494-99 (D. Md. 2005). *Werner-Matsuda* expressly rejected the holding in *Shurgard* and limited the CFAA to outside hackers. The court held that the defendant union officer who was authorized to use the union's "secure, proprietary website" did not exceed her authorization when she supplied a confidential membership list from the union's database to a rival union, which contacted members on the list to switch their membership to the rival union.

Werner-Matsuda's limited interpretation of the scope of the CFAA is significant because "inside jobs [by employees like those in *Shurgard*, who are about to leave their current company to join a competitor] occur about as often as outside jobs." 2005 CSI/FBI Computer Crime and Security Survey, at 14. See <http://gocsi.com>. This article will analyze both *Shurgard* and *Werner-Matsuda* and demonstrate why *Werner-Matsuda's* interpretation of the CFAA is unlikely to be followed, and what implications these cases have for protecting company data.

The CFAA does not define "authorized access" but does define "exceeds authorized access" to mean "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter." 18

U.S.C. 1030(e)(6). The *Matsuda-Werner* court found that “under the plain language of the statute...[the union’s officer] did not exceed her authorized access by accessing and/or obtaining Plaintiff’s membership list” because, as a union officer, she “was authorized to access” the union database “and to use such access to obtain the information on the membership list.” 390 F. Supp. 2d at 498. The court did not explain why her authorization did not terminate under the law of agency when she committed a serious breach of loyalty to the union. The court simply recognized without explanation that “*Shurgard* provides Plaintiff some support for a broader interpretation of” the CFAA. Id. at 499.

Also, at the time the union officer was hired by the union, she signed a registration agreement as “a requisite to obtaining... [a union] user identification number and password” to the database. Id. at 495. She agreed in the registration agreement “not to use the information provided through...[the union computers] for any purpose that would be contrary to the policies and procedures established by the...[union] constitution.” Id. at 483, 499. The court rejected the signed registration agreement as a basis to limit the defendant’s authorization to the computers for legitimate union business, holding that the CFAA does “not prohibit the unauthorized disclosure or use of information, but rather unauthorized access,” and its terms do not “proscribe authorized access for unauthorized or illegitimate purposes.” Id. at 499.

The court held that the defendant’s use of the membership list after she retrieved it from the union’s database may have breached her contract with the union under the registration agreement, but that breach did not equate to a lack of authorization to access the database. The court, however, solely focused on what the defendant did with the list and ignored what the defendant knew at the time she accessed the union database to obtain the list. The signed registration agreement certainly demonstrated that at the time she accessed the computer to take the list she knew she did not have the right to use that list to undermine the membership of her union.

This precise issue was addressed in *Register.com v. Verio*, 126 F. Supp. 2d 238, 253 (S.D.N.Y. 2000), where the defendant claimed

that “because it is authorized to access the...database for some purposes its access was authorized,” and that the CFAA’s definition of exceeding authorized access “does not contemplate a violation of end use restrictions placed on data as ‘exceeding authorized access.’” Id.

Commenting that “Verio’s distinctions between authorized access and an unauthorized end use of information strike the court as too fine,” the court held that “even if Verio’s means of access to the...database would otherwise be authorized, that access would be rendered unauthorized ab initio by virtue of the fact that prior to entry Verio knows that the data obtained will be later used for an unauthorized purpose.” Id.

Werner-Matsuda’s conclusion that the CFAA only applies to outside hackers and not to insiders relied primarily on the CFAA’s legislative history. The court’s pronouncement on the legislative history seems misguided in two respects. First, it cited cases interpreting not the legislative history of the CFAA, but rather a separate and unrelated statute, the Stored Wire and Electronic Communications and Transactional Records Access Act (SECA), which the plaintiff union also alleged in its complaint. 18 U.S.C. 2701, et seq. These cases hold that SECA applies only to outside hackers. 390 F. Supp. 2d at 495-99. See, e.g., *Sherman & Co. v. Salton Maxim Housewares Inc.*, 94 F. Supp. 2d 817, 820 (E.D. Mich. 2000). The court, however, cited no case that holds that the CFAA’s legislative history limits the statute to hackers.

Second, *Matsuda-Werner’s* analysis of the CFAA’s legislative history did not go beyond the 1986 and 1990 amendments and ignored the 1996 amendment to the CFAA. The *Shurgard* court reviewed the CFAA’s entire legislative history and concluded that, with the passage of the 1996 amendments, Congress intended the CFAA to cover acts by both outside hackers and insider employees. A critical amendment in 1996 replaced the term “federal interest computer” with the term “protected computer.” This change broadened the CFAA to address “in a single statute the problem of computer crime.” S. Rep. No. 104-357 at 5.

Shurgard quoted extensively from the 1996 Senate Report, including its statement that the intent of one section of the CFAA, §

1030(a)(2)(C), was “to protect against the interstate or foreign theft of information by computer,” including intellectual property, and that “[t]he crux of the offense...is the abuse of a computer to obtain the information” Id. at 7-8. While only referencing § 1030(a)(2) of the CFAA, *Shurgard* concluded that this legislative history “demonstrates the broad meaning and intended scope of the terms ‘protected computer’ and ‘without authorization’ that are also used in the other relevant [CFAA] sections” and that “the [Senate] report states that the statute is intended to punish those who illegally use computers for commercial advantage.” 119 F. Supp. 2d at 1129.

Recent cases continue to cite to ‘Shurgard’

Werner-Matsuda is unlikely to stem the growing use of the CFAA against employees and other insiders who steal computer data. Indeed, just last month the 3d U.S. Circuit Court of Appeals cited *Shurgard* in concluding that “the scope” of the “reach” of the CFAA “has been expanded over the last two decades.” *P.C. Yonkers Inc. v. Celebrations the Party and Seasonal Superstore LLC*, No. 04-4254, 2005 WL 2931940, at *5 (3d Cir. Nov. 7, 2005). See also *C.H. Robinson Worldwide Inc. v. Command Trans. LLC*, No. 05 C3401, 2005 WL 3077998, at *3-4 (N.D. Ill. Nov. 16, 2005).

Nonetheless *Werner-Matsuda* does correctly stress that what the CFAA prohibits is the “unauthorized” access to computers. As the 1st Circuit recognized in *EF Cultural Travel B.V. v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003), the “CFAA...is primarily a statute imposing limits on access and enhancing control by information providers.” Given that companies have the right to control and set limits on this access, it is critical that such authorizations clearly delineate who is permitted to access particular databases and the circumstances under which they may be accessed, whether it be in agreements, compliance rules, employee handbooks or on the computers themselves. ■■■

This article is reprinted with permission from the December 12, 2005 edition of THE NATIONAL LAW JOURNAL. © 2005 ALM Properties, Inc. All rights reserved. Further duplication without permission is prohibited. For information, contact ALM Reprint Department at 800-888-8300 x6111 or visit almreprints.com. #005-01-06-0001