

OPINION

Will the justices rule on the Computer Fraud and Abuse Act?

Two recent cases raise the prospect that the Court will eventually interpret its “without authorization” language.

NICK AKERMAN

THE NATIONAL LAW JOURNAL
September 23, 2009

Two cases decided in the past month — *LVRC Holdings LLC v. Brekka*, No. 07-17116, 2009 WL 2928952, (9th Cir. Sept. 15, 2009) and *U.S. v. Drew*, No. CR 08-0582, 2009 WL 2872855 (C.D. Calif. Aug. 28, 2009) — raise the prospect that the federal Computer Fraud and Abuse Act (CFAA), U.S.C. 1030, will for the first time in its 25-year history be interpreted by the U.S. Supreme Court. This article will review *Brekka* and *Drew*, their likely outcomes on appeal and what businesses should do in response to these decisions.

The CFAA, the federal computer crime statute, enumerates 12 separate violations of federal criminal law relating to computers. Eight of these violations require proof that the violator accessed the computer “without authorization” or “exceeding authorized access.” *Brekka*’s and *Drew*’s interpretation of “without authorization” in different factual and legal contexts raise significant conflicts with other federal decisions that will likely only be resolved by the Supreme Court. The meaning of “without authorization” has significant implications for the protection of competitively sensitive business data and the control and protection of public Web sites. Both criminal and civil cases are implicated since the CFAA is a criminal statute that provides a civil remedy for damages and injunctive relief for a company that “suffers damage or loss” by reason of a violation of the CFAA. 18 U.S.C. 1030(g).

EMPLOYEE THEFT OF DATA

Brekka, a civil case that affirmed summary judgment for the defendant employee, is the first circuit court opinion to hold that an employee’s authorization to access the company computer is not based on the law of agency. *Brekka* involves the classic employee theft of data whereby employees, before they leave to compete, e-mail to themselves competitively sensitive company data. The *Brekka* court refused to apply the CFAA to this theft of data, holding that employees cannot act “without authorization” because their employer gave them “permission to use” the company computer. *Brekka*, 2009 WL 2928952, at *4. The court acknowledged that its holding directly conflicts with the U.S. Court of Appeals for the 7th Circuit’s decision in *Int’l Airport Centers LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006)

In *Citrin*, the employee stole data from the company laptop and then destroyed the remaining data. Based on the Restatement (Second) of Agency § 112 (1958), the court held that an employee’s authorization to access the company computers is predicated on his agency relationship with his employer and that, when the employee violates “his duty of loyalty,” i.e., when Jacob Citrin stole data and “resolved to destroy files that incriminated himself and

other files that were also the property of his employer,” his authorization to access the company computers terminated. *Id.* at 420.

While the 9th Circuit rejected *Citrin*’s premise that “[Christopher] Brekka would have acted ‘without authorization’...once his mental state changed from loyal employee to disloyal competitor,” *Brekka* at *6, it ignored the 11th Circuit’s contrary decision in *U.S. v. Salum*, 257 Fed. App’x 225, 230-31 (11th Cir. 2007), which interpreted “without authorization” based on the defendant’s change of mental state. In *Salum*, a police officer with the Montgomery, Ala., Police Department was



Nick Akerman

charged with a criminal violation of the CFAA for providing information from the FBI’s criminal record database to a private investigator. Although *Salum*, as an employee, “had authority to access the [National Crime Information Center] database,” the court held that there was sufficient evidence for the jury to conclude that *Salum* had accessed the computer “without authorization” because at the time he accessed the computer *Salum* knew that he was accessing the information “for an improper purpose.” *Id.* at 230.

Brekka’s principle criticism of *Citrin* is 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

NICK AKERMAN, is a partner in the New York office of Dorsey & Whitney who specializes in the protection of trade secrets and computer data.

an employer.” *Brekka*, 2009 WL 2928952, at *6. The court stated that an employee “would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA.” *Id.* For that reason, the court found that *Citrin*’s interpretation of authorization “does not comport with the plain language of the CFAA.” *Id.* at *7.

Brekka’s reasoning, however, ignores the Supreme Court’s reliance in *Carpenter v. U.S.*, 484 U.S. 19 (1987) on this same state law cited by *Citrin* to interpret the plain language of “scheme to defraud” in the mail and wire fraud statutes. *Carpenter* affirmed the convictions 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.

‘WITHOUT AUTHORIZATION’

In contrast to *Brekka*, *Drew* has implications for the CFAA beyond the workplace. It is a criminal prosecution in which the federal district court overturned a jury conviction on the ground that the CFAA’s element of “without authorization” makes the statute unconstitutionally vague. The jury found 49-year-old Lori Drew guilty of violating the CFAA for using a MySpace account to harass and torment a 13-year-old girl, who, as a result, committed suicide. Drew perpetrated what has been referred to as cyberbullying by posing as a fictitious 16-year-old boy in violation of MySpace’s terms of service (TOS) that required her, among other things, to provide truthful information on MySpace and not use MySpace to harass, abuse or harm other people or solicit personal information from anyone younger than 18. Drew’s violation of MySpace’s TOS provided the proof that Drew accessed MySpace “without authorization.”

While recognizing that “most courts that have considered the issue have held that a conscious violation of a website’s terms of service/use will render the access unauthorized,” the court held that, as a matter of law, the CFAA is unconstitutionally vague. *Drew*, 2009 WL 2872855, at *10. The principle reasons it enumerated are that the CFAA “criminalizes breaches of contract” between the Web site owner and users; there is a lack of clarity as to which violation of a particular term of service

amounts to a criminal violation; the CFAA permits the Web site owner to define the “criminal conduct” through its terms of service; and “a violation of a website’s terms of service, without more” would transform the CFAA “into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanor criminals.” *Id.* at *14-16.

The court provided a number of hypothetical examples of absurd uses of the CFAA, including one that would permit the government to prosecute “the exasperated parent who sends out a group message to neighborhood friends entreating them to purchase his or her daughter’s girl scout cookies, which transgresses” MySpace’s TOS against advertising and solicitation on its site. *Id.* at *16.

THE VAGUENESS ARGUMENT

In a different context, the 7th Circuit rejected the argument that the CFAA is unconstitutionally vague and held that “[t]here is no constitutional obstacle to enforcing broad but clear statutes” and that “[t]he statute itself gives all the notice that the Constitution requires.” *U.S. v. Mitra*, 405 F.3d 492, 496 (8th Cir. 2005). Lori Drew indisputably violated the letter of the statute by intentionally accessing MySpace “without authorization” and obtaining information from the juvenile girl. Similarly, although *Mitra* did not involve cyberbullying, it did address a new computer technology, trunking communications systems, that did not exist when the CFAA was enacted. The court explained that the reason why Congress “write[s] general statutes rather than enacting a list of particular forbidden acts” is because “complexity is endemic in the modern world and that each passing year sees new developments.” *Id.* at 495.

Similarly, the *Drew* court assumed that, because the statute is worded so broadly, a simple transgression of a Web site’s term of use could constitute a violation of the CFAA because the CFAA’s element of “obtaining information” can be proved through “mere observation” of data. *Drew*, 2009 WL 2872855, at *6. That is not the correct legal standard, according to at least one other circuit. *U.S. v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997), held that there was insufficient proof to affirm a CFAA conviction when Richard Czubinski, an Internal Revenue Service employee, had exceeded his authorized access to the IRS computer but “merely” viewed restricted tax information relating to “friends, acquaintances, and political rivals.” There must be a “showing of some additional end — to which the unauthorized access is a means.” *Id.*

The *Drew* court’s view that the CFAA is

unconstitutionally vague because it criminalizes a breach of contract overlooks the well-established fact that a breach of contract can in certain instances also constitute a crime. For example, an employee who steals his employer’s trade secrets in breach of a confidentiality agreement can also be guilty of violating the Economic Espionage Act. See, e.g., *U.S. v. Chung*, 622 F. Supp. 2d 971, 975 (C.D. Calif. 2009). Moreover, that the CFAA permits Web site owners to “spell out explicitly what is forbidden” on its Web site, *EF Cultural Travel B.V. v. Zefer Corp.*, 318 F.3d 58, 63 (1st Cir. 2003), does not make it anymore unconstitutionally vague than a “No Trespass” sign that can form the predicate for criminal trespass in some jurisdictions.

Finally, because the CFAA is subject to abuse by prosecutors applying it to technical insubstantial violations does not make it unconstitutional. The wire fraud statute, for example, could equally be applied to a student who calls home interstate from college asking his parents for money for books, when he intentionally lied, planning to use the money to buy beer. No one has ever seriously argued that this potential misuse of prosecutorial discretion makes the statute unconstitutional.

Assuming *Brekka* and *Drew* are appealed, it will be a long time before both cases are resolved. In the meantime, businesses should continue to publish Web site terms of use that can be used as predicates for the CFAA by establishing the scope of authorized access with the goals of protecting their customers or users, such as MySpace does, and protecting their business data. See, e.g., *Register.com v. Verio Inc.*, 126 F. Supp. 2d 238, 245 (S.D.N.Y. 2004). To meet the risk of employee computer theft, businesses should not rely solely on the agency theory to support a CFAA civil action. “Unauthorized access” can also properly be established through written company policies delineating the scope of an employee’s authorization to access the company computers, whether through a compliance code or an employee handbook, or through employee agreements. See, e.g., *Cont’l Group Inc. v. KW Property Mgmt.*, No. 09-60202, 2009 WL 1098461, at *12 (S.D. Fla. 2009); *EF Cultural Travel B.V. v. Explorica Inc.*, 274 F.3d 577, 583-84 (1st Cir. 2001). Incorporating such policies and agreements into the workplace are now a must.