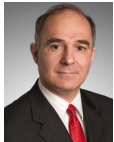


Technology Law

Computer & Internet Crimes

Where Will it End? The Ninth Circuit Decides to Revisit when a User “Exceeds Authorized Access” Under the CFAA



haynesboone
Setting precedent.

Contributed by Pierre Grosdidier, Haynes and Boone, LLP

In just a few years, the Federal Computer Fraud and Abuse Act of 1984 (the “CFAA,” 18 U.S.C. § 1030) has evolved into a broad and powerful weapon in computer-related criminal and civil litigation. Originally enacted to target hackers, the statute now reaches almost any imaginable malfeasance that involves a computer. Two recurring categories of cases arise in an employment context. First, those where disgruntled employees delete files or “wipe” hard drives in spite before they take the door. Second, cases where employees leave with copies of their employers’ proprietary information, such as client databases or electronically-stored trade secrets, with the intent of starting or joining a competing business.

In almost all employment cases, whether civil or criminal, a predicate question is whether the employee accessed his employer’s computers “without authorization,” or in a manner

that “exceed[ed] authorized access.” The CFAA does not define “without authorization.” It defines the term “exceeds authorized access” as

to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter.¹

Courts have struggled with, and split over, what constitutes unauthorized computer access under the CFAA. Some courts have construed the term broadly and held that access becomes unauthorized the instant an employee acts for personal gain and against his employer’s interests. These courts have grounded their reasoning in agency law whereby the agency stops whenever the agent acts in breach of his duty of loyalty.² Other courts have construed the term “unauthorized access” narrowly. These courts have held that an employee does not breach the CFAA if his employer authorized his access, regardless of how the employee uses the accessed information. Employees who download databases for their personal benefit using an authorized password may be guilty of trade secret theft but have not offended the CFAA.

The issue is not merely academic. A broad construction of “unauthorized access” threatens to flood federal courts with actions—especially those rooted in employment disputes—that were traditionally filed in state courts. These actions typically revolve around a CFAA claim with pendant state claims of trade secret theft, unfair competition, unjust enrichment, trespass to chattel, or breach of employment contract, just to name a few.

The Ninth Circuit published two opinions that arguably provide the most sensible construction of the CFAA’s authorization language to-date, were it not for the statute’s § 1030(a)(2)(C).³ These two cases provide a good synopsis of the issues related to what constitutes “unauthorized access” under the CFAA.

In *Brekka*, LVRC hired Brekka without a written contract and granted him unrestricted access to its computers. Brekka

Originally published by Bloomberg Finance L.P. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

sent business documents to personal email accounts during negotiations to acquire an ownership interest in LVRC. The employer discovered the communications after negotiations broke down and Brekka left his employment. It sued Brekka under the CFAA. The district court granted Brekka's motion for summary judgment, and the Ninth Circuit affirmed. The court held that *the employer* decides whether an employee is authorized to access a computer. Because LVRC gave Brekka unfettered authority to access its computers, Brekka's access was authorized even if he acted with fraudulent intent. *Brekka* stands for the proposition that in the absence of a use agreement, an employee who accesses his employer's computers with an authorized password but with fraudulent intent does not violate the CFAA. Of course, the employee's conduct may give rise to the traditional state law claims listed above. The employee breaches the CFAA when he hacks into his employer's computers, or continues to access them after the employer terminates his authorization. The *Brekka* court explicitly rejected the 7th Circuit's *Citrin* agency approach as inconsistent with its conclusion that the employer authorizes access to its computers, not the employee.

Nosal was a former Korn/Ferry International executive who allegedly attempted to start a competing business by using contact information pilfered from Korn/Ferry's executives-and-companies database. Nosal allegedly engaged three Korn/Ferry employees to exploit the database for his benefit and in breach of their use agreements. The government charged Nosal with aiding and abetting violations of § 1030(a)(4), which states that a person breaches the CFAA if the person:

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.

The district court held that the defendants had not violated § 1030(a)(4) because they were authorized to access the database for business reasons. This was true even if they acted beyond the terms of their use agreements and with the intent to defraud Korn/Ferry. The government appealed and the Ninth Circuit reversed. The court of appeals held that under the plain language of the CFAA, "an employee 'exceeds authorized access' under § 1030 when he or she violates the employer's computer access restrictions—including use restrictions." *Nosal* was different from *Brekka*, the court held, because Korn/Ferry's employees were bound by a restrictive use agreement—which they violated—and *Brekka* was not. But the two holdings were nonetheless consistent because they reflected the view that the employer decides when the employee is authorized to access a computer. A CFAA breach occurs when the employee exceeds that authorization, but cannot stand when his access is unrestricted. The court described its interpretation of the term "exceeds authorized access" as the "only logical" one possible.

The court dismissed fears that § 1030(a)(4) could criminalize "the mere violation of an employer's use restriction." A violation

of this section requires that the employee act "with intent to defraud," to obtain "anything of value" greater than "\$5,000 in any 1-year period." These conditions protect employees who use their work computers to access personal email accounts, or to check sport scores on Internet.

The *Nosal* dissent rejected the Ninth Circuit's holding that the term "exceeds authorized access" includes violations of employers' use agreements. The dissenting judge pointed out that § 1030(a)(2)(C) dispenses with the intent requirement of § 1030(a)(4) and, therefore, criminalizes innocent use of computers beyond a use agreement. A person breaches § 1030(a)(2)(C) of the CFAA if the person

intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains - . . .
(C) information from any protected computer.

The CFAA's broad definition of the term "protected computer" effectively includes any computer connected to Internet. 18 U.S.C. § 1030(e)(2). Section 1030(a)(4)'s intent requirement shields from criminal prosecution employees who check personal emails or scores on Internet in violation of their use agreement. Not so with § 1030(a)(2)(C).

The dissenting judge concluded that the court's interpretation of "exceeds authorized access" lent § 1030(a)(2)(C) to arbitrary enforcement in light of its breadth, rendering the CFAA unconstitutionally vague. This interpretation could not stand in light of the canon of statutory construction that requires "that an Act of Congress should be construed, where 'fairly possible,' in a manner that does not result in its invalidity." The correct interpretation of "exceeds authorized access" must be based on unauthorized access, such as when an employee authorized to access a computer hacks into a forbidden drive of that computer. The dissenting judge deemed this interpretation consistent with Congress's intent to criminalize computer hacking with the CFAA.

As the *Nosal* court noted, the dissent's interpretation effectively merges the meanings of "without authorization" and "exceeds authorized access." Moreover, Congress amended the CFAA nine times since 1984 and, even though it "never specifically targeted employee computer crimes," its intent may be hard to frame.⁴

Brekka seems solidly reasoned. Hacking into a computer is "unauthorized access" and violates the CFAA. In the absence of a use agreement, access that is authorized does not offend the CFAA, even when done with the intent to defraud. But uncertainty remains as to when a user "exceeds unauthorized access." Paradoxically, this last term is defined in the CFAA and "unauthorized access" is not.

The Ninth's Circuit decided to rehear *Nosal en banc* on October 27, 2011, and banned its citation as precedent. Whatever the outcome of *Nosal*, the uncertainty is unlikely to dissipate until the Supreme Court rules on the issue, or Congress clarifies its intent by amending—yet again—the CFAA. The 1st, 5th, and 11th Circuits preceded *Nosal* in holding that employees exceed authorized access when they violate use agreements.⁵ Advocates on both

sides of the *Nosal* divide can invoke solid arguments to support their positions, as the rich case law and commentary bear witness. The issue is ripe for Supreme Court review.

Meanwhile, employers who have not done so should undertake to protect their computer infrastructures. Access to servers and databases should be compartmentalized. A software developer's sales force needs access to the client database, but not to the developer's servers, for example. Employers should impose high-security password policies, and require that all employees sign comprehensive computer use agreements. One size will not fit all in this respect. Employers should work with knowledgeable employment attorneys to draft computer use agreements that match their business and operational needs.

Finally, employers with a preference for state courts should bear in mind states laws that address unauthorized computer access. Texas Penal Code Chapter 33 criminalizes the knowing access of "a computer, computer network, or computer system without the effective consent of the owner," for example.⁶ A victim of computer crimes has a statutory cause of action under Texas law.⁷ The victim may recover actual damages and reasonable attorney's fees and costs.⁸

Pierre Grosdidier is an Associate in Haynes and Boone, LLP's Business Litigation practice group in Houston, Texas. He specializes in lawsuits and arbitrations with strong engineering or software elements. Prior to practicing law, Pierre worked 18 years in the process control industry. He holds a Ph.D. from Caltech and a J.D. from the University of Texas. He is a member of the State Bar of Texas and a registered professional engineer in Texas (inactive).

¹ 18 U.S.C. § 1030(e)(6).

² See, e.g., *Int'l Airport Ctr., LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006).

³ See *LVR Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009); *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011).

⁴ See Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 Mich. L. Rev. 819, 831, 839 (2008–09) ("the legislative history provides little authority value to the current debate" over the meaning of authorization under the CFAA).

⁵ See, e.g., *United States v. John*, 597 F.3d 263 (5th Cir. 2010).

⁶ Tex. Penal Code § 33.02(a).

⁷ Tex. Civ. Prac. & Rem. Code § 143.001(a).

⁸ *Id.* § 143.002.