The Rise of the Computer Fraud and Abuse Case

BY SEBASTIAN E. KAPLAN

Fenwick
FENWICK & WEST LLP

Major changes are in the works for the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. In the past ten years, the CFAA has moved from obscurity into the limelight as Congressional amendments drastically increased its scope. The watershed began in late 2001, when Congress, as part of the USA Patriot Act, adopted a definition of "loss" in the CFAA that made it easier for private litigants to meet the $5,000 threshold for damage or loss. In 2007, Congress expanded a crucial liability provision to criminalize "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information." 18 U.S.C. § 1030(a)(2)(C). This section imposes liability on anyone who accesses a computer without authorization or who exceeds authorization, even if the person commits no further wrongdoing. Since 2002, complaints alleging a cause of action under the CFAA have increased nearly 600% percent.

2011 brought several potential developments in CFAA jurisprudence. First, the Ninth Circuit decided and then recanted *United States v. Nosal*, a case effectively resolving a raging circuit split on the meaning of "authorization." Second, Congress is considering an amendment to the CFAA that would eliminate liability under the CFAA that is predicated solely on the violation of a computer use policy or website terms of use.

Many commentators have criticized the CFAA for potentially criminalizing activity such as visiting social networking sites or checking personal email. These critiques stem largely from *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), where federal prosecutors indicted a Missouri woman for cyberbullying a minor. The legal basis for the prosecution was that the defendant, a middle aged woman, violated MySpace's terms and conditions by creating a profile claiming she was a teenage girl. Although the district court granted defendant's motion for judgment of acquittal, the court left open whether violations of a websites terms and conditions could result in criminal prosecution.

Although *Drew* was a criminal prosecution, it shows how business litigators can test the CFAA's boundaries. The CFAA is now pleaded in several contexts that go far beyond the computer hacking activities that most associate with cybercrime and that motivated the passage of the statute. Specifically, the CFAA is now a common cause of action in civil disputes between employers and employees who download or copy information from company computers before leaving their employer. These disputes mostly arise where an employee leaves to work for a competitor, but employers also now raise the CFAA as a counterclaim to employee complaints of wrongful discharge and employment discrimination. Additionally, the CFAA has begun to make its mark in consumer class actions against online service providers, especially companies who collect consumer information online.

The CFAA has several other benefits for businesses. First, it confers federal jurisdiction over commercial torts that are usually pleaded only as state law actions, such as trade secret misappropriation, breach of contract, and intentional interference with prospective economic advantage. Second, there are fewer elements to prove under the CFAA than related state law claims; it is often necessary only to show a defendant accessed a computer and that the plaintiff suffered damage or loss in excess of $5,000.

The actual scope of the CFAA will ultimately turn on the definition of "authorization." There is now raging a circuit split over whether the CFAA's authorization language should be construed broadly or narrowly. Under the broad view, anyone who knows they are acting against the interest of the computer owner is acting "without authorization." So, an employee who has accepted a job with a competitor, and accesses his current employer's computer before quitting, does so "without authorization."

The broad view has been adopted by Judge Posner and the Seventh Circuit. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit reversed the district court's order dismissing an employer's CFAA claim against a former employee who had copied confidential information from his work laptop and wiped his computer before leaving to start his own competing business. The Circuit held: "Citrin's breach of his duty of loyalty terminated his agency relationship . . . and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420–21. Commentators refer to this view as the "agency view."

Under the contrasting narrow view, the victim must grant and revoke authorization, not the defendant. So, an employee who is given authorization to access his employer's customer contact database when he is hired retains his authorization until the employer specifically revokes it, even if the employee has resolved to abscond to a competitor with valuable trade secrets.

This narrow view has been adopted by the Ninth Circuit. In *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), the Ninth Circuit affirmed the district court's grant of summary judgment for the defendant on the CFAA claim. Brekka worked for LVRC, and emailed numerous LVRC files to his personal email address during his employment before leaving to compete with LVRC. LVRC also accused Brekka of accessing its network using an unexpired password after he ceased his employment.

The Ninth Circuit held: "No language in the CFAA supports LVRC's argument that authorization to use a computer ceases when an employee resolves to use the computer contrary to the employer's interest." *Id.* at 1133. To satisfy constitutional notice, the court held: "The plain language of the statute therefore indicates that "authorization" depends on actions taken by the employer . . . . If the employer has not rescinded the defendant's right to use the computer, the defendant 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.* at 1135.

In the year or so after *Brekka*, district courts mostly aligned themselves in these two camps. This past year, however, two circuit court decisions changed the landscape in a way that expands the scope of the CFAA.

In *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), a criminal defendant and former employee at the Social Security Administration ("SAA") appealed his conviction and twelve-month sentence under the CFAA. Rodriguez used his privilege as an SSA employee to access a government database and retrieve personal information about individuals he knew, including women he pursued romantically. The question was whether Rodriguez accessed the database without authorization or exceeding authorization—he was authorized to access the database generally, but the SSA prohibited its employees from obtaining information without a legitimate purpose. The Eleventh Circuit affirmed the conviction, holding Rodriguez *exceeded* his authorization by violating the SSA policy. That Circuit distinguished *Brekka* on the grounds there was no explicit employer policy involved in that case.

In *United States v. Nosal*, 642 F.3d 781 (9th Cir. 2011), the Ninth Circuit panel reversed the district court's order dismissing an indictment against Nosal for conspiring to defraud his former employer by taking confidential information and inducing other employees to take such information. Like the Eleventh Circuit, the panel relied on the "exceeds authorized access" language in the CFAA. The panel distinguished *Brekka*—which only addressed access "without authorization"—on the grounds that the victim company had a policy it made employees sign that restricted their use and disclosure of the victim's information to legitimate company business. The panel noted but dodged the problem that this interpretation may apply to all sorts of innocuous activity an employer may prohibit—it merely claimed that § 1030(a)(4) requires the CFAA violation be part of a fraudulent scheme. The dissent, however, correctly pointed out that § 1030(a)(2)(C) contains identical "exceeds authorized access" language, without any qualification requiring additional wrongdoing such as fraud. The majority opinion provided no rationale for limiting the liability provision of § 1030(a)(2)(C) in a way that would not, for example, prohibit an employee who accessed his social networking account on a work computer from being liable if his employer prohibited

personal internet use on the job. Perhaps motivated by the dissent's critique, the Ninth Circuit has now called *Nosal* for en banc rehearing and vacated the panel's decision.

The problem, it seems, is that courts, and for that matter, the rest of us, are unsure what appropriate conventions apply when it comes to computers and the internet. We have had centuries to iron-out the social and legal norms regarding physical trespass—the closest, but still imperfect analogy to the cause of action created by the CFAA. And while physical trespass may appear simple at first blush, the case law is complex, and its development tested doctrinal limits and generated unique extensions and limitations, such as constructive trespass and adverse possession.

Our lack of social conventions makes courts reticent to extend the scope of the CFAA to activity that is questionably criminal. *Brekka* reveals the Ninth Circuit's discomfort with criminalizing the relatively innocuous act of an employee emailing himself some files for unclear motives. Reading *Citrin*, however, reveals that the Seventh Circuit was cavalier in extending the scope of the CFAA because the judges found firm ground in traditional agency law; *Citrin* is not really a decision about computers or technology at all.

Rodriguez and *Nosal*, in turn, are part of a vanguard of cases that avoid the difficult question of defining nascent and inchoate social norms by focusing on the explicit and specific conventions between the parties—employment agreements, company policies, and the like. This focus on parties' agreements reflects the same theme pervading other recent Supreme Court decisions, such as *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), which held the City did not violate the Fourth Amendment by searching its employee's text messages. The Supreme Court held the search was reasonable because the clear employer policy stated that the employer was entitled to search its employee's text messages if the employee exceeded the allotted number of messages in a given month. In an area where new technology presents difficult questions, courts are likely to look for confidence in deciding access and authorization issues based on the agreements of the parties.

In the long run, these agreements between parties will help generate the social norms that will define how we understand what people are allowed to do with computers. In the short run, however, attorneys and their clients concerned about a computer breach should focus on the specific agreements made with employees, vendors, joint venture partners, and other entities that will have access to a client's computer network. Litigators facing the fire-drill caused by a trade secret misappropriation should immediately request the company policy on technology use and consider other means a client may have informed its employees about the parameters of acceptable computer use.

In *Pulte Homes, Inc. v. Laborers' International Union of North America*, 648 F.3d 295 (6th Cir. 2011), the Sixth Circuit began the process of codifying certain norms regarding internet use by reversing a district court's dismissal of a company's CFAA claim against a labor organization for orchestrating an email protest campaign targeting its executives. The campaign was successful enough that the volume of email and voice mail overloaded the plaintiff's computer systems and prevented some of its employees from accessing their work email and phones.

Although not discussed by the Sixth Circuit, an important point of context is that the defendant's actions resembled a common form of hacking known as a denial of service (DOS) attack. A hacker launching a DOS attack generates thousands of requests for a specific website in an attempt to overload the server and shut the site down. The defendant's actions in *Pulte* were quite different, as it did not use an automated system to send thousands of emails (although it did use an automated calling machine). Nevertheless, *Pulte* reflects that courts are beginning to recognize that opprobrium of these kinds of activities has permeated social awareness sufficiently to create a plausible inference of intent.

In *Facebook v. Power.com*, No. C 08-05780 JW, 2010 WL 3291750 (N.D. Cal. July 20, 2010), Judge Ware attempted to clarify the norms regarding appropriate internet use, specifically how website owners access competing websites. Facebook sued Power.com for accessing its social network to collect information on Facebook users' friends, an alleged violation of Facebook's terms of service. Facebook moved for judgment on the pleadings or partial summary judgment on its California Computer Crime Law, California Penal Code section 502 claims.

Interpreting California Penal Code section 502 in accord with the CFAA, Judge Ware held that constitutional notice requirements prohibited finding Power.com's activities illegal based solely on Facebook's terms of use. Instead, Judge Ware held access to a website can only be unauthorized if the defendant circumvented technical barriers. This solution is similar to requiring property owners to build a fence to put potential trespassers on notice. Whether this technical barriers requirement will survive the Ninth Circuit's en banc resolution of *Nosal* and whether technical barriers provide sufficient constitutional notice on their own remain open questions.

Congress has been dealing with the same issues, although in less detail. Senator Leahy has proposed revising the CFAA to limit liability to exceeding authorized access to seven categories of sensitive information. Senators Grassley and Franken, going a step further, seek to amend the CFAA to eliminate liability based only on the violation of an acceptable use policy or terms of service agreement, effectively adopting *Brekka*.

Business litigators should be aware that courts are reluctant to hold that novel forms of computer access and use create liability under the CFAA. At the same time, the recent decisions in *Rodriguez*, *Nosal*, and *Pulte* suggest that courts are increasingly willing to accept that breaches of private agreements and actions that resemble recognized forms of hacking are sufficient to survive dismissal. Undoubtedly, these cases will increase the prevalence of CFAA litigation, at least until Congress steps in to provide clarity on this murky subject.

Sebastian E. Kaplan is an associate in the Litigation Group of Fenwick & West LLP.