Courts Hack Away Claims Under the CFAA

By Daniel J. Ballou

I was at my desk recently when I received a call from a friend who worked as a sales manager for a local business. My friend, who I'll call Skip, had helped his employer start the company and had built up a substantial book of business, compiling valuable contacts and other sales information that was stored on the company's computer network. Over the years, he had occasionally e-mailed himself a copy of quarterly sales reports so he could monitor his commissions, and he had used this information, including names, contact information and sales histories, to verify with his employer how much he was owed on a number of lucrative accounts. He had become so successful in sales that he had recently been offered a job at a substantial raise by their biggest competitor, a regional firm anxious to enter the local market. Having decided to take the new job, Skip downloaded the most recent sales information to a USB drive and gave notice he was leaving.

Within a week of starting his new job, Skip had been sued by his former employer in federal court for violation of, among other things, the Computer Fraud and Abuse Act. Specifically, the employer alleged that he had acted "without authorization or in excess of his authorization" when he downloaded the sales information, and that he had done so in violation of the CFAA by breaching company policies prohibiting the disclosure of confidential information and trade secrets. I told him he should make an appointment because we needed to talk.

Skip was one of a growing number of employees who change jobs only to find themselves on the receiving end of a federal lawsuit under the CFAA. The combination of increasing transience among workers and the ease with which computerized data is stored, accessed and transmitted has created a target rich environment for lawsuits against departing employees. In many cases, these suits are filed against nefarious pilferers bent on corporate espionage who are determined to take as much inside information with them as they can to unfairly benefit a competing business. In other cases, the CFAA has become a bludgeon wielded by aggressive U.S. Attorneys and irate employers to enforce the terms of private employment agreements in federal court.

Origins of the CFAA

You would be hard pressed today to find a business that does not store most if not all of its most valuable information on a computer network of some kind, whether on a stand alone desktop PC, a company server or even the ubiquitous "cloud." Whether the information consists of correspondence, e-mails, sales histories, pricing information, technical specifications or other information obtained and developed over the years, the data stored on a company computer is often the most valuable asset the business owns. Moreover, giving employees access to some or all of that information is often a practical necessity for the success of the business. The problem arises when someone who has been entrusted with access ends up using the information against the interests of the employer.

The CFAA was first and foremost a criminal statute enacted by Congress in 1986 as the Counterfeit Access Device and Computer Fraud

PHOTO BY GEORGE FULTON

and Abuse Act, as a response to the relatively new (at the time) crime of computer hacking. The Act was originally used to prosecute everything from garden variety hackers to credit card thieves who had unlawfully accessed protected computers. In 1994, however, the Act was amended to add, among other things, a civil cause of action allowing the recovery of compensatory damages and injunctive relief. With this amendment in place, aggrieved employers could bring civil claims against employees found to have raided company computer files while in the process of leaving the company to work for a competitor.

In my friend Skip's case, he had accumulated the names and contact information of sales leads throughout his employment with the company. Even though he could probably reconstruct much of this information from memory and considered it to be his work product, this kind of data compiled in written or electronic form is generally "work for hire" that most courts would find belongs to the employer. Nevertheless, since his boss did not object when he had downloaded the spreadsheets to monitor his commissions, Skip felt justified in e-mailing himself the last reports before he gave notice. Needless to say, his employer saw things differently. Whether an employee is planning to set up a new business or is being lured away by a competitor, the employer often has no way of knowing that its informational assets have been compromised until it is too late. Once the loss of data has been discovered, the employer often (and justifiably) may move quickly to limit the damage done and protect what assets it can.

Traditionally, employers have had an ample arsenal of weapons under common law and state statutes to recover damages against the "faithless servant," ranging from the right to withhold pay to civil claims for breach of the duty of loyalty or the South Carolina Trade Secrets Act and a variety of possible tort claims. However, as vital business information has become digitized, employers have increasingly used the CFAA as a way to pursue departing employees who take electronic data with them on the way out the door.

The benefits of bringing a claim under the CFAA can be significant for the employer. For instance, CFAA claims can be used to bootstrap state law trade secret, non-compete and tort claims into federal court. So too, the Act does not require proof that the information obtained is confidential or proprietary. Instead, the plaintiff must allege only that the defendant intentionally accessed a computer "without authorization or exceed[ed] authorized access, and thereby obtain[ed] … information from any protected computer." 18 U.S.C. § 1030(a)(2)(C) (2006 & Supp. 2010). Damages recoverable under the CFAA must exceed $5,000, but can include the costs of forensic investigation, recovery and repair of computer systems and other losses resulting from an interruption in service.

Despite the increasing number of federal court claims asserted under the CFAA, recent decisions reflect an unwillingness in some circuits to arm employers with the leverage of a federal criminal statute in what are essentially private, post-employment, state law disputes.

Authorization: access or use?

CFAA liability flows to any person who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer." 18 U.S.C. § 1030(a)(2)C) (2006 & Supp. 2010). The factual circumstances surrounding access therefore are critical to maintaining the cause of action. When a person is an outsider who has no right to access the employer's computer network, courts agree that those who secretly obtain access to a computer network are hackers and are "without authorization" under the Act. Likewise, if an employee or other insider is authorized to access documents on his employer's C: drive, but is prohibited by the employer from accessing password protected financial or human resources files stored on the F: drive, downloading information off of the prohibited drive would generally be viewed as exceeding authorized access, and again violate the Act.

The tougher question arises when an employee has unfettered access to sensitive computer files, but the company has restricted the use of the information through policies contained in an employment agreement or employee handbook. Typically, these restrictions are contained in an employee handbook or employment agreement and prohibit the use or disclosure of certain confidential or proprietary information. Is the departing employee who uses client data she previously compiled to help start a competing business guilty of committing a federal crime and subject to civil liability under the CFAA? The federal courts are divided on this question.

One of the early cases to use the CFAA in the employment context was *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.,* 119 F. Supp. 2d 1121 (W.D. Wash. 2000). Shurgard claimed that a competitor had raided its employees and persuaded them to download confidential files from company computers while they were still employed by Shurgard, but had agreed to work for Safeguard. The district court rejected the argument that the employees were authorized to obtain the data, holding under §112 of the Restatement (Second) of Agency that the moment they acted disloyally to their current employer, they forfeited their authorization to access the information.

This broad, agency-based theory of authorization represents an expansive view of the CFAA that predominated in earlier decisions. Following this trend, in *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit held that an employee hired to compile detailed real estate data violated the Act when he permanently deleted all of the information and damaged the employer's computers before quitting. The court ruled that authorization to access the employer's com-

puter files ended when the employee "acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal." *Id*. at 421. The court found that Citrin's act of sabotaging company files breached his duty of loyalty and automatically terminated any authorization he had to access the computer or the information contained on it.

Under the CFAA, "exceeds authorized access" means to access a computer with authorization and then "to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6) (2006). The federal circuits are generally divided over the question of when and under what conditions an insider exceeds authorization. The *Citrin* camp holds that disloyal actions of the employee automatically terminate any right to access the employer's computers, whether the employer is aware of the disloyalty or not. However, the Ninth Circuit has taken a much narrower approach and held that once an employee is allowed access, he cannot be "without authorization," and for an insider to "exceed authorization," the employer must have affirmatively limited or rescinded permission to access the computer in question. *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009). As a result, the employer's conduct, and not the employee's intended *use* of the information, becomes the focus of the analysis.

Our own district court reached a similar result in *Sloan v. Coe*, No. 0:09–CV–02659–CMC, 2010 WL 4668341 (D.S.C. Nov. 18, 2010). In *Sloan*, the court distinguished between company policies restricting the use of computers and those limiting access. Since the language of the CFAA restricts only access and not use, the court reasoned that an employee who had access to company data did not act "without authorization" or in excess of that authorization, even where it was alleged that he accessed the information with the intent of using it in violation of a company use policy. Our district court reiterated this position in *WEC Carolina Energy Solutions, LLC v. Miller*, No. 0:10–CV–2775–CMC, 2011 WL 379458 (D.S.C. Feb. 3, 2011), finding that employees do not act "without authorization" or "exceed authorized access" by violating an employer's policies prohibiting the *use* of confidential information. Most recently, the Fourth Circuit affirmed the district court, noting that while the employees "may have misappropriated information, they did not access a computer without authorization or exceed their authorized access." *WEC Carolina Energy Solutions, LLC v. Miller,* 687 F.3d 199 (4th Cir. 2012).

Neither *Sloan* nor *WEC Carolina* involved alleged breach of company computer access policies, but only concerned policies prohibiting unauthorized use of information. However, the Eleventh Circuit has held that an employer can restrict employee access to company computers to legitimate business purposes only and that an employee who knowingly used the computers for

personal reasons exceeded his authorization and violated the CFAA. *United States v. Rodriguez,* 628 F.3d 1258 (11th Cir. 2010). In *Rodriguez*, the employer had a clear policy prohibiting the use of its computers for non-business purposes. The court affirmed the CFAA conviction where the defendant admitted he had violated this policy by using social security information obtained from his employer's computers to stalk old girlfriends. *Id.* While requiring more than a breach of a duty of loyalty to trigger liability under the Act, and perhaps splitting hairs, *Rodriguez* approves an employer's adoption of internal policies that effectively define authorized access in terms of legitimate use.

In another recent departure from *Citrin*, the Ninth Circuit Court of Appeals re-affirmed *Brekka* and held that an employee does not exceed authorized access under the CFAA by violating a company use restriction. *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). In *Nosal*, a former employee of Korn/Ferry International convinced his old co-workers to download confidential information that they sent to him to use in a competing business. While these co-workers were authorized to access this database, sending this information to Nosal was a clear violation of Korn/Ferry's policy prohibiting unauthorized use of sensitive information.

In an *en banc* decision, the *Nosal* court rejected liability under the CFAA for violation of the terms of authorized use policies, even where such policies restrict access to legitimate company purposes. Given the wide variety of such policies, such as rules prohibiting using work computers for personal matters, or the terms of service agreements on many popular websites, the *Nosal* court cautioned against allowing private agreements regarding computer use to dictate the boundaries of criminal law. Writing for the 7-2 majority, Judge Kozinski warned of "[s]ignificant notice problems … if we allow criminal liability to turn on the vagaries of private policies that are lengthy, opaque, subject to change and seldom read." *Id*. at 860.

With the recent decision in *WEC Carolina*, the Fourth Circuit has officially adopted the narrow interpretation of "without authorization" and "exceeds authorized access." *Nosal* suggests that an employee's access to workplace computers is either authorized or it is not, and *no* company policy can limit authorized access to only include access for legitimate employer purposes. Whether the Fourth Circuit would agree with this reasoning is unclear, but it clearly applied the rule of lenity in rejecting the CFAA claims in *WEC Carolina*. Eventually, it seems likely the split in the circuits will be resolved in the U.S. Supreme Court or by legislative amendment. As of the date of this article, a number of bills are being considered by the U.S. Senate that could modify how the CFAA is applied, at least in the employment context.

Whether access to protected data can be limited by an authorized use policy remains an open question under the CFAA, but employers and employees alike would be wise to carefully examine existing policies and procedures concerning access to confidential and proprietary data. See *Cvent, Inc. v. Eventbrite, Inc.,* 739 F. Supp. 2d 927 (E.D.Va. 2010) (criticizing the plaintiff for burying its Terms of Use policy barring unauthorized access and suggesting that even a policy governing authorized access should be conspicuous and applied in a meaningful way). If such policies speak only in terms of unauthorized *use* of information, they may well support state law claims but likely will fail under CFAA, at least in the Fourth and Ninth Circuits. Moreover, an employer's failure to regularly enforce even *access* restrictions may present a problem to bringing a CFAA claim after a key employee like Skip leaves with thumb drive in hand.

Conclusion

Perhaps the most reasoned approach under the CFAA would be to embrace its use when employers have properly restricted access to computers and data through a carefully worded, conspicuously placed and consistently applied policy. Too often, even where such policies exist, they are buried in fine print or legalese in documents that the employee rarely sees and the employer does not effectively monitor or enforce. Those who use secrecy and trickery to bypass electronic barriers protecting valuable information should expect to be held liable under the CFAA, but the Act should not be a shortcut around the prudent adoption and use of policies designed to protect valuable company data. With the onus placed upon the employer in the first instance to develop, communicate and enforce clear rules limiting computer access, employees who have "authorized access" to company computers cannot claim surprise when they exceed that authorization to harm the company.

Daniel J. Ballou practices business litigation in Rock Hill at his firm, Hamilton Martens, Ballou & Carroll, LLC.