New Jersey Law Journal

VOL. 209 - NO 12 MONDAY, SEPTEMBER 17, 2012 ESTABLISHED 1878

INTELLECTUAL PROPERTY & *Life Sciences*

Limiting the Scope of the Computer Fraud and Abuse Act

By William E. Viss

A number of recent federal court decisions illustrate an emerging trend toward a more narrow interpretation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. This shift in the law carries important implications for intellectual property owners, especially those concerned with misappropriation of confidential material at the hands of a wayward employee. The CFAA previously received broad application by a majority of federal district courts. As a result, those accused of violating an employer's internal computer use policy could expect to face civil, and even criminal, CFAA charges, in addition to the usual breach-of-loyalty and contract claims.

By favoring a narrow application of the act based largely on the CFAA's legislative history and predominantly criminal nature, a growing number of jurisdictions has rejected the argument that CFAA liability arises where an employee misappropriates confidential information where the employer previously granted access. As discussed below, while the courts' retreat from the CFAA high-water mark arguably announces a more natural reading of the act, it also leaves employers with fewer means to prosecute claims involving unauthorized use of valuable intellectual property.

The CFAA was originally drafted in 1984 as an anti-hacking measure and prohibits a person from "intentionally access[ing] a computer without authorization, or exceed[ing] authorized access, and thereby obtain[ing] information from a protected computer." 18 U.S.C. § 1030(2)(C). The act allows a party who has suffered damages over $5,000 to bring a civil action, while also providing for criminal sanctions. As a result, the CFAA has become an effective means through which an employer protects against the misuse of company computers and the misappropriation of confidential information. However, legitimate concerns exist that the act was never intended to apply to situations in which no actual "hacking" took place, and that a broad application of the CFAA would criminalize otherwise innocuous employee computer use that happens to violate an employer's computer policy.

In *United States v. Nosal*, for example, a former employee obtained client lists from his employer with aid from co-workers with access to such lists. 676 F.3d 854 (9th Cir. 2012). The former employee subsequently used the information to create a competing enterprise and was charged criminally with aiding and abetting his co-workers in exceeding their authorized access with intent to defraud, in violation of 18 U.S.C. § 1030(a)(4). In reviewing the trial court's decision, the Ninth Circuit held that the phrase "exceeds authorized access," as it appears in § 1030(2)(C), was limited to violations of restrictions on access to information, not restrictions on its use, and dismissed the CFAA claims against Nosal. In doing so, the *Nosal* court made clear that it was reluctant to extend the reach of the CFAA to a factual scenario Congress had not clearly specified: "When choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before we choose the harsher alternative, to require that Congress should have spoken in language that is clear and definite." 676 F.3d at 862-63.

Viss is an associate in the commercial litigation practice at Archer & Greiner PC in Haddonfield, where he focuses on business disputes with an emphasis on intellectual property, environmental litigation and appeals. Steven A. Medina, a law clerk with the firm, contributed to this article.

The court concluded that this narrower approach made for a more sensible application as the CFAA's general purpose, in light of its legislative history, is to punish hackers, not an employee's misappropriation of trade secrets.

The court in *Ajuba Int'l v. Saharia*, also adopted a narrow interpretation of the CFAA. U.S. Dist. LEXIS 66991 (E.D. Mich. May 14, 2012). In *Ajuba*, the plaintiff had granted its employees, including the defendant, Saharia, unrestricted access to confidential material stored on its computers. Saharia allegedly made use of such access to misappropriate the confidential information. The plaintiffs filed a CFAA claim, asserting that Saharia had accessed and used information stored on the plaintiffs' computers for the improper purpose of competing against the plaintiffs in direct violation of Saharia's contractual and fiduciary obligations. The plaintiffs argued that Saharia lost any previous authorization he had to access the plaintiffs' computers, or exceeded such authorization when he accessed the computers in violation of the confidentiality and use limitations.

The court disagreed, ruling that because Saharia had previously received unrestricted access to the plaintiffs' computer system, the plaintiffs lacked standing to allege Saharia had acted "without authority" or in "excess of authority" in violation of the CFAA. The court observed that, while confidentiality agreements and other policies may govern the misuse of a computer system by employees, the plain language of the CFAA does not. Put simply, the *Ajuba* court held that once an employee is granted authorization to access an employer's computer system, that employee does not violate the CFAA by accessing such system and taking confidential information, regardless of how the employee subsequently uses that information. The *Ajuba* court reasoned that this more narrow interpretation was reflective of the CFAA's legislative history and congressional intent.

The Fourth Circuit reached the same conclusion on similar facts in *WEC Carolina Energy Solutions v. Miller*, U.S. App. LEXIS 15441 (4th Cir. July 26, 2012). Mirroring the rulings in *Nosal* and *Ajuba*, the *Miller* court emphasized that the CFAA was primarily a criminal statute, and pursuant to the rule of lenity, favored a strict construction of the act in which a violation of a workplace computer policy would not support CFAA liability.

Despite the recent trend announced by the *Nosal*, *Ajuba* and *Miller* decisions, there remains a split among federal district courts regarding the scope of the CFAA. The First, Fifth and Seventh Circuits, for example, have adopted a broader interpretation of the act, recognizing that a violation of an employer's internal use policies may well lead to CFAA liability. In contrast, the Ninth Circuit, as well as district courts in the Second, Fourth, Sixth, Tenth and D.C. Circuits, have construed the statute more narrowly. In light of the divergence of judicial opinion, the United States Supreme Court will likely be called upon to bridge the divide.

In the meantime, it appears that a narrow application of the CFAA is the more reasoned approach. It fairly positions the act in the context of a social-media savvy and technology dependent public, while leaving the CFAA intact as a tool to prosecute legitimate hacking offenses. The shift toward a more narrow interpretation of the CFAA should therefore be a welcome result to practitioners who have feared that a criminal anti-hacking statute has been stretched beyond its intended metes and bounds. And, as the courts have pointed out, a tailored application of the CFAA will not leave an injured party without the means to recoup damages resulting from the loss of confidential material. For example, a well-counseled employer can rely on other legal instruments — such as confidentiality or nondisclosure agreements, noncompete clauses and non-solicitation agreements — to seek compensation for the loss or misuse of their valuable intellectual property or confidential business information. Prudent employers are therefore best advised to limit their reliance on the CFAA and re-focus their efforts on crafting and enforcing effective employment agreements and computer policies, and implementing technological safeguards. ■