Ninth Circuit Scales Back CFAA Application to Data Misappropriation Cases

BY ILANA RUBEL AND SEBASTIAN KAPLAN

Fenwick
FENWICK & WEST LLP

Aggrieved employers have often turned to the Computer Fraud and Abuse Act (the "CFAA") in suing former employees that allegedly absconded with information from company computers. Such suits face bleak prospects in the Ninth Circuit after the ruling in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012). In *Nosal*, the *en banc* court held an employee could not be liable under the CFAA for "exceeding authorized access" to an employer's computer by accessing proprietary information in violation of the employer's written computer use policies. In so holding, the Ninth Circuit reversed its initial panel decision, and entrenched its split from other circuits that interpret the CFAA more broadly. *Nosal* clarifies the Ninth Circuit's view that the CFAA targets true "hacking," and not violations of company computer use policies or website terms of service.

Background

Defendant Nosal, a former employee of an executive search firm, allegedly convinced several former colleagues to download and transmit lists of executives so that he could compete with his former employer. The employer had required employees to sign agreements that they would only use company information for legitimate business purposes, and further featured prominent warnings in its database against unauthorized use.

Nosal was criminally charged with violating the CFAA's prohibition on "exceeding authorized access" to a protected computer, on the grounds that taking of the employer's information for hostile competitive use was clearly unauthorized under the employer's written policies and employment agreements. But Nosal moved to dismiss, arguing that the CFAA's "exceeds authorized access" prong does not apply here. Because the employees in question had authorized *access* to the computers, Nosal argued, it did not matter whether their ultimate *use* of the obtained information was authorized.

Illustrating the extent to which opinions (and Circuits) differ on this issue, the district court granted Nosal's motion, the Ninth Circuit panel reversed, the Ninth Circuit *en banc* vacated the panel and affirmed the district court's dismissal, and now the matter is stayed pending possible petition to the Supreme Court for certiorari.

The Ninth Circuit's Decision

In affirming the district court, the *en banc* Ninth Circuit held that "the phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions." For more than a decade, courts have wrestled with the scope of the terms "authorization" and "access." The issue boils down to whether a computer owner can allow access to its computer for certain purposes, but not others. The Ninth Circuit has now clarified that the CFAA is not triggered where there is merely unauthorized *use* of information—the defendant's *access* itself must have been without or in excess of authorization. Thus, under *Nosal*, if a business wants to protect sensitive information, it must either limit access, or rely on legal remedies other than the CFAA.

The *Nosal* opinion expresses grave concern that the broad reading advocated by the government could criminalize much innocuous activity. In particular, the Court notes that the phrase "exceeds authorized access" appears in another section of the CFAA, § 1030(a)(2)(C), which has no requirement of fraudulent purpose, and requires only that the person who "exceeds authorized access" has "obtain[ed] . . . information from any protected computer" (i.e. any computer that can connect to the Internet). The government's view, the Court feared, could "make every violation of a private computer use policy a federal crime."

Judge Kozinski notes the ubiquity of transgressions of computer use policies, wryly observing that the universe of those who use a computer in violation of computer use restrictions "may well include everyone

who uses a computer." Judge Kozinski colorfully cautioned, "[u]nder the government's proposed interpretation of the CFAA . . . describing yourself [on a dating website] as 'tall, dark, and handsome,' when you're actually short and homely, will earn you a handsome orange jumpsuit." The Court reasoned that a narrow interpretation, requiring that access itself must be unauthorized, best comports with Congress's intent to criminalize computer hacking.

The opinion concludes by recognizing that the Ninth Circuit is at odds with the Fifth, Seventh, and Eleventh Circuits, each of which adopted broader interpretations of the CFAA's authorization requirement.

Implications

The *Nosal* opinion mostly preserves, and slightly expands, the status quo limitations on the CFAA. The Ninth Circuit had already adopted a narrow interpretation of the CFAA's access prong in *LVRC Holdings LLC v. Brekka*. *Brekka* found the term "without authorization" did not apply to an employee who took confidential information from his employer merely because the employee breached his duty of loyalty to his employer, but *Brekka* did not involve breach of a signed employee agreement. Now, in the Ninth Circuit, it is clear that even where the use violates written agreements as well as employer computer use policies, CFAA liability does not ensue as long as the employee was authorized to access the computer. In other circuits, however, contractual use restrictions remain enforceable through the CFAA.

While *Nosal* involved criminal charges, the CFAA provision at issue also extends to civil actions. The implications of the decision cover a range of scenarios:

Employment Agreements—Companies adopt a variety of technology acceptable use policies, or restrict the use of confidential data through employment agreements. Under *Nosal*, these are not valid bases for bringing a CFAA claim against an employee, although they are still useful for CFAA litigation outside the Ninth Circuit and for raising breach of contract, trade secret misappropriation, and related state law claims. However, insofar as the CFAA has historically been a popular hook for suing former employees in federal court, *Nosal* throws cold water on such a strategy in the Ninth Circuit.

Website Terms of Use—Website owners have also invoked the CFAA as a means of enforcing website terms, arguing that a website user "exceeds authorized access" by accessing a site in violation of its terms. Frequently, the defendant users are competitors scraping data from the plaintiff's website. *Nosal* can be expected to preclude such cases in the Ninth Circuit; if the user could access the site, the fact that the nature of the use violated the site's terms would not render the access unauthorized so as to trigger a CFAA violation. The Northern District of California addressed the website scenario in *Facebook v. Power Ventures*, holding that defendant Power Ventures could not be liable under the CFAA for allegedly violating Facebook's terms of use, but could only face CFAA liability if it had circumvented "technical barriers" such that the access itself was not authorized. *Nosal* corroborates this view, noting the "general purpose" of the CFAA is to "punish hacking—the circumvention of technological access barriers—not misappropriation of trade secrets."

Privacy Policies—Plaintiffs' lawyers have recently filed a spate of class action lawsuits pleading the CFAA against companies that collect demographic information in alleged excess of what consumers "authorize." Under *Nosal*, consumers will have difficulty pleading a CFAA claim under the theory that they did not authorize disclosure by the defendant companies. *Nosal* may push Plaintiffs' lawyers to file future privacy class actions outside the Ninth Circuit.

Looking Forward

Thus far, only one case has substantively interpreted *Nosal*. In *Weingand v. Harland Financial Solutions*, the Northern District of California district court rejected the argument that *Nosal* limited CFAA liability to violations of technical access barriers, and found that one could state a CFAA claim by alleging access without permission, even if not barred by technical means. That court read *Nosal* to preclude CFAA causes of action based on use restrictions, but not to require actual "hacking" through technical protective measures in order to give rise to a CFAA claim. The *Weingand* opinion referenced the Ninth Circuit's *Brekka* opinion, which stated that if an employer fired an employee, but had not yet revoked login credentials, the employee would violate the CFAA by using that login. This interpretation, however, appears in tension with *Nosal,* which suggests that even where

terms of use purport to deny any permission for access (as with Facebook's prohibitions on third party access to user accounts), violation of those terms could not trigger a CFAA violation. Thus, even within the Ninth Circuit, it remains a murky question as to whether violation of a command against access, where access is not technically barred, can be a CFAA violation.

The Supreme Court has yet to address the CFAA. Although many hoped that the high court would do so on certiorari from the Ninth Circuit's *Nosal* decision, the Solicitor General decided last week not to pursue an appeal of the *en banc* decision. Only a week before, the Fourth Circuit in *WEC Carolina Energy v. Miller*, wholly adopted the Ninth Circuit's *Nosal* holding, creating a new potential for this issue to reach the Supreme Court.

If you have any questions about this publication, please contact Ilana Rubel (irubel@fenwick.com) and Sebastian Kaplan (skaplan@fenwick. com) of Fenwick & West LLP.