LOS ANGELES
Daily Journal
www.dailyjournal.com
WEDNESDAY, JULY 13, 2016

PERSPECTIVE

CFAA decision showing influence in Facebook case

By Jonathan H. Blavin

Last week, a divided panel of the 9th U.S. Circuit Court of Appeals delved yet again into contours of the Computer Fraud and Abuse Act (CFAA), which provides, as an element of the offense, that a defendant have "knowingly … access[ed] a protected computer without authorization or exceeding authorized access."

The 9th Circuit revisited the government's prosecution of David Nosal, a former director of the executive search firm Korn Ferry, who was charged with violations of the CFAA after he (and his compatriots) downloaded information and source lists from Korn Ferry to launch a competitor. Although many viewed Judge Alex Kozinski's en banc decision in *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (*Nosal I*), as narrowing the scope of the CFAA, *United States v. Nosal*, 2016 DJDAR 6746 (9th Cir. July 5, 2016) (*Nosal II*), likely will be seen as adopting a more expansive construction of what access "without authorization" means under the statute.

Nosal and his accomplices downloaded information from Korn Ferry at first using their own passwords before leaving the company in violation of its computer use policy, and then after they left, through borrowing the access credentials from a current employee. In *Nosal I*, the 9th Circuit considered the dismissal of counts stemming from Nosal and others' downloading of material through the use of their credentials while they were employed by Korn Ferry. The 9th Circuit affirmed. The court expressed concern that interpreting the "without authorization" or "exceeding authorized access" language to mean in violation of computer use restrictions would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." 676 F.3d at 859. The court discussed a litany of examples of use restriction violations which could be federal crimes under this interpretation of the CFAA, such as a minor using a website that "forbade minors from using its services," letting someone else log into your Facebook account, or "describing yourself" on a dating website as "'tall, dark and handsome,' when you're actually short and homely."

Following *Nosal I*, some district courts in the 9th Circuit dismissed CFAA claims on the basis that the plaintiffs had only alleged the unauthorized "use" of a computer system or data, and not the technological circumvention of access barriers. *See Incorp Servs. Inc. v. Incsmart. Biz Inc.,* 11-4660 (N.D. Cal. Aug. 24, 2012) (dismissing CFAA claim where there are "no direct or clear allegations of 'hacking' … being, broadly, 'the circumvention of technological access barriers,' not violation of 'use restrictions'").

> Although many viewed [*Nosal I*] as narrowing the scope of the CFAA, [*Nosal II*] likely will be seen as adopting a more expansive construction of what 'unauthorized access' means under the statute.

After remand by the 9th Circuit, the government filed a superseding indictment with the remaining CFAA counts based on the occasions when Korn Ferry's systems where accessed using an employee's borrowed login credentials. The district court denied Nosal's motion to dismiss the remaining CFAA counts, rejecting the argument that *Nosal I* limited the statute's applicability "to hacking crimes where the defendant circumvented technological barriers to access a computer." *United States v. Nosal*, 930 F. Supp. 2d 1051, 1060 (N.D. Cal. 2013). Alternatively, the court held that "the indictment sufficiently allege[d] such circumvention." A jury convicted Nosal on all counts.

In *Nosal II*, the majority — Judges Margaret McKeown and Sidney Thomas — affirmed Nosal's conviction. The 9th Circuit emphasized that this case was different than *Nosal I*, where "authorization was not in doubt," given that the employees "unquestionably had authorization from the company to access the system; the question was whether they exceeded it." *Nosal I* "did not address" whether "Nosal's access to Korn/Ferry computers *after* both Nosal and his co-conspirators had terminated their employment and Korn/Ferry revoked their permission to access the computers was 'without authorization.'" Thus, although *Nosal I* made clear that the "unauthorized use of information" is not covered by the CFAA, Nosal was charged here "with unauthorized access."

The majority concluded "that given its ordinary meaning, access 'without authorization' under the CFAA is not ambiguous" and that "[i]mplicit in the definition of authorization is the notion that someone, including an entity, can grant or revoke that permission," which the panel found consistent with the approach taken by other circuits. In response to Nosal's argument that the "CFAA only criminalizes access where the party circumvents a technological access barrier," the majority held that "[n]ot only is such a requirement missing from the statutory language, but it would make little sense because some § 1030 offenses do not require access to a computer at all." The court further noted that, at any rate, a "password requirement is designed to be a technological access barrier."

Judge Stephen Reinhardt dissented. Among other issues, he noted that the "majority's construction would base criminal liability on system owners' access policies," which "is exactly what we rejected in *Nosal I*." For its part, the majority responded by stating that while it was "mindful of the examples noted in *Nosal I*" that "ill-defined terms may capture arguably innocuous conduct," the "circumstance here — former employees whose computer access was categorically revoked and who surreptitiously accessed data owned by their former employer — bears little resemblance to asking a spouse to log in to an email account to print a boarding pass."

Nosal II already is having an impact on the law. On Tuesday, the 9th Circuit issued its decision in *Facebook Inc. v. Power Ventures Inc*., 13- 17102 (9th Cir. July 11, 2016). In that case, individuals who used Facebook and other social networking sites could log on to the website of the defendant, "Power," and aggregate their social networking information from these various sites on a central platform. Facebook sued Power under multiple laws, including the CFAA. Relying on *Nosal II*'s discussion of the revocation of permission to access, the panel stated that "initially, Power users arguably gave Power permission to use Facebook's computers to disseminate messages. Power reasonably could have thought that consent from *Facebook* users" was "permission for Power to access *Facebook*'s computers." (Emphasis in original). The panel concluded, however, that "Facebook expressly rescinded that permission when Facebook issued its written cease and desist letter to Power" and "then imposed IP blocks in an effort to prevent Power's continued access." Thus, the panel held that "the consent that Power had received from Facebook users was not sufficient to grant continuing authorization to access Facebook's computers after Facebook's express revocation of permission."

As Power demonstrates, Nosal II promises to have a continuing effect on the contours and scope of the CFAA.

Jonathan H. Blavin *is a partner at Munger, Tolles & Olson LLP. You can reach him at Jonathan.Blavin@mto.com.*

JONATHAN BLAVIN
Munger, Tolles & Olson