WILMERHALE

En Banc Ninth Circuit to Consider Scope of Computer Fraud and Abuse Act

2011-11-09

On October 27, the U.S. Court of Appeals for the Ninth Circuit ordered rehearing *en banc* in *United States v. Nosal*, a case that presents the question of whether an employee who violates his employer's computer-use policy also "exceeds authorized access" to a protected computer in violation of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030(a)(4). The case raises important issues for private employers of all sizes, for companies concerned with protecting proprietary information, and for Internet companies and users concerned with whether violations of website terms of service will also create civil or criminal liability under the CFAA.

Background

According to a June 2008 indictment, Mr. Nosal previously worked as an executive at a recruitment firm. The Government contends that, after leaving the firm, and even though he was allegedly subject to various non-compete obligations, Mr. Nosal conspired with several remaining employees to obtain information about the firm's clients and contacts with the goal of creating a competing business. The remaining employees had permission to access the firm's computer systems, but only for official purposes and subject to disclosure limitations.

The Government charged Mr. Nosal with conspiring with the remaining employees to exceed their authorized access to the firm's computer systems in violation of 18 U.S.C § 1030(a)(4), which states that whoever

> knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period....

Mr. Nosal moved to dismiss the § 1030(a)(4) counts, arguing that the phrase "exceeds authorized access" precludes an individual from using access to one part of a computer network to enter an

otherwise forbidden part of a network, but that it does not preclude an individual from accessing files that are otherwise freely available. Nosal asserted that the files at issue were open to all employees and that neither he nor his alleged co-conspirators exceeded their authorized access to those files.

The district court agreed with Mr. Nosal and dismissed the § 1030(a)(4) counts, holding that under the Ninth Circuit's decision in *LVRC Holdings Inc. v. Brekka*[1], employees do not exceed authorized access to a computer network for CFAA purposes unless they clearly lack authority to enter or use the portion of the network at issue.[2]

A three-judge panel of the Ninth Circuit reversed and held that "an employee 'exceeds authorized access' under § 1030(a)(4) when he or she violates the employer's computer access restrictions—including use restrictions."[3] The panel reasoned that *Brekka* did not require a different result because *Brekka* stands for the proposition that whether an employee "exceeds authorized access" under the CFAA turns on the actual limitations established by the employer. The employer in *Brekka* had not established clear policies on the use of a computer that an employee was authorized to access. If an employer gives unrestricted access to a computer system, then there can be no violation of the CFAA for exceeding authorized access to the system. But if the employer clearly restricts access, including with respect to use, then violations of those restrictions can trigger CFAA liability.[4] According to the panel, the employer in *Nosal* had imposed clear policies restricting its employees' access to its databases to queries run for legitimate business purposes.

Rehearing *En Banc*

On October 27, the Ninth Circuit granted Mr. Nosal's petition for rehearing *en banc*. The *en banc* court, consisting of 13 judges, will hear argument in the case during the week of December 12. A party interested in filing an *amicus curiae* brief should do so by the end of November in order to give members of the *en banc* court an opportunity to read the brief before oral argument.

The *en banc* court's decision in *Nosal* regarding the scope of liability under § 1030(a)(4) could have tremendous significance for private employers and employees in the Ninth Circuit and for Internet companies and users nationwide. The Ninth Circuit is the largest circuit in the country by any measure. It includes California and thus encompasses Silicon Valley and its myriad computer and Internet companies.

If the Ninth Circuit accepts the proposition that "exceeds authorized access" for purposes of CFAA liability turns on restrictions established by an employer, then that will clarify that companies in the Ninth Circuit with proprietary or trade-secret information should carefully consider how employees access their computer networks and how policies are communicated to employees about permission to use company systems. Greater clarity in workplace policies on this topic would increase the likelihood that CFAA civil (or even criminal) remedies would be available in future disputes about confidential company information.

The ramifications of the *en banc* court's decision may not be limited to the Ninth Circuit. Other courts of appeals have struggled to determine precisely what it means to exceed authorized access to a computer under the CFAA. The First, Fifth and Eleventh Circuits have adopted a view similar to that of the *Nosal* panel, essentially holding that employees exceed authorized access for CFAA purposes if they violate employer policies governing access to a network.[5] If the *en banc* Ninth Circuit reverses the *Nosal* panel decision, that will increase the likelihood of a circuit split and U.S. Supreme Court review of the issue.

Congress has taken note of the potentially broad scope of the CFAA. The Senate Judiciary Committee recently approved a bill that would amend the definition of "exceeds authorized access" in the CFAA to preclude civil and criminal liability for access to a protected computer based solely on a violation of "a contractual obligation or agreement, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or non-government employer." Personal Data Privacy and Security Act of 2011, S. 1151, § 110. The Personal Data Privacy and Security Act is currently awaiting action on the floor of the Senate. Developments in *Nosal* may affect the prospects for legislative revisions to the CFAA, either through the Personal Data Privacy and Security Act or several other pieces of cybersecurity legislation also pending in Congress.

---

[1]581 F.3d 1127 (9th Cir. 2009).

[2]*See United States v. Nosal*, 642 F.3d 781, 782 (9th Cir. 2011).

[3]*Id.* at 784.

[4]*Brekka*, 581 F.3d at 1129-1130.

[5]*EF Cultural Travel v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001); *United States v. John*, 597 F.3d 263 (5th Cir. 2010); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010). The *John* court noted that the facts before it required it to decide only that a violation of § 1030(a)(4) could be established when an employee gained access in violation of an employer's computer use policy and the employee knew or reasonably should have known that use in furtherance of a crime was prohibited under the policy. *John*, 597 F.3d at 271. In *International Airport Centers, LLC v. Citrin*, 440 F.3d 418 (7th Cir. 2006), the Seventh Circuit held that an employee accesses an employer's computer system "without authorization" if the employee violates a state-law duty of loyalty and uses the access in a manner contrary to the interests of the employer. *See also* Orin Kerr, *Should Faking a Name on Facebook be a Felony?*, Wall St. J., Sept. 14, 2011.

Authors

Benjamin A. Powell

PARTNER

Co-Chair, Cybersecurity and Privacy Practice

Co-Chair, Artificial Intelligence Practice

benjamin.powell@wilmerhale.com

+1 202 663 6770

Jason C. Chipman

PARTNER

jason.chipman@wilmerhale.com

+1 202 663 6195

Patrick J. Carome

RETIRED PARTNER

+1 202 663 6000