CLIFFORD
CHANCE

Client Memorandum April 2012

Ninth Circuit Declares Watching YouTube on Your Work Computer Is Not a Federal Crime: Creates Circuit Split

Employees who use their work computers for personal reasons, like watching YouTube videos, checking box scores, shopping or even stealing confidential documents from their employers, can rest a little easier today because – at least according to the Ninth Circuit – such conduct does not expose them to criminal or civil liability under the Computer Fraud and Abuse Act ("CFAA").

Specifically, just last week, the Ninth Circuit issued its long-awaited *en banc* opinion in *United States v. Nosal*, concluding that the CFAA does not apply to employees who use otherwise authorized access to their employers' computer systems for non-business purposes, even where such use breaches corporate policy or an employee's duty of loyalty to their employer. No. 10-10038 (9th Cir. Apr. 10, 2012) ("Slip Op."). The Ninth Circuit's opinion, however, departs dramatically from decisions by the First, Fifth, Seventh and Eleventh Circuits, each of which have upheld CFAA application in circumstances where employees have used their authorized access to employers' computer systems for unauthorized purposes. Until either Congress steps in and clarifies its intent or the Supreme Court resolves this clear circuit split, the *Nosal* decision will hamper the ability of employers and prosecutors (at least in the Ninth Circuit) to pursue civil claims or criminal charges under the CFAA against rogue employees who misappropriate their employers' confidential information by using a work computer.

By way of background, Congress enacted the CFAA to prevent two different types of unlawful access to computers, or hacking, which the Ninth Circuit refers to as "outside" and "inside hacking."[1] Slip Op. at 3863-64, 3863 n.5. Liability under the CFAA

Contacts

Christopher J. Morvillo
Partner
T: +1 212 878 3437
E: christopher.morvillo
@cliffordchance.com

Polly Snyder
Counsel
T: +1 202 912 5025
E: polly.snyder
@cliffordchance.com

Megan E. Farrell
Associate
T: +1 212 878 8154
E: megan.farrell
@cliffordchance.com

1 "Outside hacking" refers to the traditional notion of hacking, *i.e.*, when an external user, presumably neither the computer owner nor his employee, accesses a computer to misappropriate information. "Inside hacking" takes place when a party with limited authority to access a computer "exceeds" the scope of that authority to access information. At issue in *Nosal*, was the second form, hacking by exceeding authorized access. *Id.*

requires, among other things, proof that a defendant "intentionally accesses a computer *without authorization*, or *exceeds authorized access*, and thereby obtains information from any protected computer."[2] 18 U.S.C. §1030(a)(2)(C). In addition to criminalizing unauthorized access to a protected computer, the statute also provides for a private right of action by a party whose information has been hacked. This includes suits by employers against rogue employees who may have misappropriated confidential employer information by exceeding the scope of their authorized computer access. In other words, the CFAA provides a federal jurisdictional basis for what traditionally has been a state law claim. It is the threat of federal criminal sanctions, however, that has caused many courts, including the Ninth Circuit, to be deeply skeptical of any statutory interpretation that would implicate conduct "beyond that which is inherently wrongful, such as breaking into a computer."[3] Slip Op. at 3864.

In particular, some subsections of the CFAA do not require specific fraudulent intent for liability to attach, and as a result, courts struggle over whether an employee who is otherwise authorized to access data on a work computer "exceeds authorized access" under the CFAA if he or she uses that authorized access for an unauthorized purpose, *i.e.*, to steal that data. The discomfort some courts – like the Ninth Circuit – have with this construct is that criminal liability can arguably turn on the scope of an employer's computer usage policies, possibly leading to overly broad and arbitrary enforcement of the statute. In fact, this is the issue that the Ninth Circuit confronted in the *Nosal* case.

The *Nosal* Case

Mr. Nosal was a high-level executive at an international executive search firm, Korn/Ferry International ("KFT"), from approximately 1994 to 2006, when he left to start a competing firm. Shortly after Mr. Nosal's departure, he used complicit KFT employees to obtain confidential KFT information to use in establishing his own firm. In 2008, Mr. Nosal was indicted in the Northern District of California for, among other things, violating the CFAA. Since then, the CFAA charges against Mr. Nosal have been upheld, then dismissed, then reinstated, and, now dismissed again, providing in the microcosm of one case, clear insight into the debate that is vexing courts around the country. (*See* 2009 WL 981336 (N.D. Cal. Apr. 13, 2009) (upholding indictment); 2010 WL 934257 (N.D. Cal. Jan. 6, 2010) (dismissing indictment in light of the then-recent decision in *Brekka*); 642 F.3d 781 (9th Cir. 2011) (reinstating indictment on the basis that employer use restrictions are in fact limitations which define the scope of permitted access)).

In late 2009, the Ninth Circuit considered a similar issue in *LVRC Holdings LLC v. Brekka*, and began shaping the rule it ultimately applied last week in Mr. Nosal's case. 581 F.3d 1127 (9th Cir. 2009). *Brekka* involved an employee who travelled frequently, and therefore emailed documents to himself in the course of his duties. While still employed, however, Mr. Brekka

---

2 The term "protected computer" is defined as one: "(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or (B) which is used *in or affecting interstate or foreign commerce or communication*, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. § 1030(e)(2).

3 Even courts deciding cases brought by private parties, however, consider the criminal implications of the statute in coming to their decisions regarding the scope of liability. *See*, e.g., *United States v. John*, 597 F.3d 263, 273 (5th Cir. 2010) ("The Ninth Circuit's reasoning in *Brekka* was influenced by its recognition that '[f]irst, and most important, § 1030 is primarily a criminal statute, and §§ 1030(a)(2) and (4) create criminal liability for violators of the statute.' The court explained its view that, '[a]lthough this case arises in a civil context, our interpretation of [the statute] is equally applicable in the criminal context,' and that 'ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity.'") (citing *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009)).

began emailing documents to himself and to his wife so that he could use them in his next business venture. The Ninth Circuit held that Mr. Brekka's conduct did not violate the CFAA because his unlimited authorization to access his work computer did not cease simply because he used that access in a manner contrary to his employer's interest. Rather, the *Brekka* court concluded that CFAA liability turns on the limitations an employer places on an employee's authorization to *access* a computer. 581 F.3d 1127. Thus the failure of Mr. Brekka's employer to establish any limitations on his computer access (including his employer's failure to limit his authority to email documents to a personal computer), absolved him of any CFAA liability for *misuse* of company information. *Id.* at 1135-36.

In its decision last week, the Ninth Circuit reached the question left open in *Brekka*: whether an employee whose *access* has been limited by an employer, and who is accessing information *within* the scope of those limitations, exceeds that access because he is *using* that access for an unauthorized purpose, *e.g.*, a non-business purpose. Setting the stage for the *en banc* opinion, the original Ninth Circuit panel concluded in a 2-1 opinion issued last April, that a person has exceeded authorized access and thus can be found guilty under 18 U.S.C. § 1030(a)(4) when he "violates his employer's computer access restrictions – including use restrictions." 642 F.3d 781, 785 (9th Cir. 2011). That first panel reasoned that "[b]ecause the statute refers to an accesser who is not entitled to access information in a certain manner, whether someone has exceeded authorized access must be defined by those access limitations." *Id.* at 786. Although the original majority opinion acknowledged concerns associated with criminalizing "violations of an employer's computer use policy," including lack of notice and the prosecution of normal and innocuous activity, it was not persuaded by Mr. Nosal's arguments on that front.[4]

Undeterred, Mr. Nosal petitioned the Ninth Circuit for a rehearing *en banc*. In the 9-2 decision issued last week, the *en banc* panel reversed the prior decision and concluded that an employee does not exceed authorized access merely by violating the *use* restrictions of an employment agreement. The court said that interpreting "exceeds authorized access" to allow employers or other parties to utilize a privately negotiated agreement to define the scope of criminal liability would "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute." Slip Op. at 3861. Additionally, the court observed that such an expansive interpretation is unnecessary to prevent the core "internal hacking" activities of an employee who circumvents security measures to access information beyond his authorization. Slip Op. at 3862.

In reaching this conclusion, the Ninth Circuit invoked the rule of lenity, a principle of statutory construction that requires courts to resolve ambiguity in criminal laws in favor of leniency. *Id.* at 3872. Failure to apply this rule could result in the proscription of a broad range of innocuous conduct that citizens would have no reason to know is criminal. *Id.* The court noted that, based on the ambiguity in the statute, everyday internet users, including minors, would be exposed to criminal liability for actions as harmless as checking basketball scores or a Facebook account, or even misrepresenting their height and weight on a dating website. Slip Op. at 3867. In making this point, the court used the example of an employee who spends six hours tending his FarmVille stable on his work computer – an activity that would exceed the scope of use permitted by nearly all employment agreements or policies, if for no other reason than it does not serve a legitimate business purpose.

As farfetched as these risks may sound, such scenarios technically fall within the scope of the 18 U.S.C. § 1030(a)(2), the CFAA subsection that makes it illegal simply to exceed authorized access to a computer and thereby obtain information, regardless of whether there is illicit intent. *Id.* at 3870. In other words, if exceeding authorized *access* means *using* a computer for non-

---

4 In responding to these arguments, the court relied on the specific intent and causation requirements in U.S.C. § 1030(a)(4), stating that they "sufficiently protect against criminal prosecution [of] those employees whose only violation of employer policy is the use of a company computer for personal – but innocuous – reasons." *Id*. at 782. As noted by Judge Campbell in her dissenting opinion, however, such reliance is likely misplaced, especially when considering the potential for prosecution under 18 U.S.C. §1030(a)(2)(C), which does not have a specific intent requirement. *Id.* at 790-791.

business purposes, then watching the Masters Tournament on your work computer is technically a crime. The court thoroughly considered these risks even though *Nosal* was charged under the CFAA provision requiring proof of specific intent, because it found that the same meaning should apply to "exceeds authorized access" regardless of where it appears in the CFAA statute. The court explained that although employees who use work computers for non-business related reasons should perhaps be fired, they should not be arrested as a federal criminal.[5] *Id.* at 3866, 3866 n.7. Thus, at least according to the Ninth Circuit, individuals cannot be found liable under the CFAA for accessing information within the scope of their access permissions even if it is done for a non-business purpose, which the court alternatively defines as misappropriation liability.

A Split Among Circuits – the Road to the Supreme Court

Other circuits, however, disagree, finding that similar misuse *may* be the basis for liability under the CFAA. In *United States v. Rodriguez*, the Eleventh Circuit upheld the criminal conviction of a Social Security Administration ("SSA") employee under 18 U.S.C. § 1030(a)(2) who repeatedly accessed SSA databases (that he was entitled to access) for non-business purposes, acquiring personal information about a variety of individuals for illicit reasons and, as such, had also violated the CFAA. 628 F.3d 1258 (11th Cir. 2010). Specifically, the Eleventh Circuit held that the defendant had clearly violated his own employment agreement as well as SSA policy prohibiting access to personal records for non-business reasons. *Id.* Similarly, in *United States v. John*, the Fifth Circuit affirmed the conviction of a Citigroup employee under 18 U.S.C. § 1030(a)(2) who had used her authorized access to Citigroup's internal computer system to obtain personal customer account information that she and others then used to make fraudulent charges. 597 F.3d 263 (5th Cir. 2010). Even though Ms. John was authorized to view all of the information that she accessed, the court determined that she was liable for computer fraud because her conduct exceeded the scope of Citigroup's official policy, which prohibited misuse of the company's internal computer systems and confidential customer information. *Id.* at 272. *See also Int'l Airport Ctrs. v. Citrin*, 440 F.3d 418 (7th Cir. 2006) (finding that employee who acted adversely to employer violated CFAA because by violating duty of loyalty to his principal he had terminated the agency relationship and with it his authority to access the employer's computer); *EF Cultural Travel BV v. Explorica, Inc*., 274 F.3d 577, 578-79 (1st Cir. 2001) (holding that defendant employees had exceeded authorized access because they used company information contrary to restrictions in their confidentiality agreements and thus were liable under 18 U.S.C. § 1030(a)(4) for using knowledge of codes obtained during the course of employment to create a high-speed computer program to mine their former employer's website for pricing information).

In holding employees responsible for using their authorized access to work computers for an unauthorized purpose, these cases largely rely on the fact that "an authorized computer user often has 'reason to know' that he or she is not authorized to access data or information in furtherance of a criminally fraudulent scheme." *John*, 597 F.3d at 273. *See also Explorica*, 274 F.3d at 583-84 ("Practically speaking . . . Explorica's wholesale use of EF's travel codes to facilitate gathering EF's prices from its website reeks of use-and, indeed, abuse-of proprietary information that goes beyond any authorized use of EF's website."). These courts therefore conclude that interpreting the phrase "exceeds authorized access" under the CFAA to include computer use that violates an employment policy does not offend the notice-related concerns often raised by defendants, as such use will almost always further an illegal purpose.

---

5 The court also highlighted the extremely rare scenario where the user of a dating website misrepresents his or her physical appearance; such a person can hardly be considered a criminal, regardless of the terms of service to which he or she agreed (even ones including a term prohibiting the provision of inaccurate or misleading information).

Conclusion

In line with the holdings of the First, Fifth, Seventh and Eleventh Circuits, the government in *Nosal* argued that concerns regarding the possible but unlikely prosecution of individuals for petty violations of employment agreements are an improper basis for refusing to punish Mr. Nosal's conduct, which Congress intended the CFAA to prohibit. Nonetheless, the Ninth Circuit disagreed and, in an unusual move that seems to frame the issue for appeal to the Supreme Court, implored the other Circuits that have decided the issue to revisit their own views in light of its reasoning. Slip Op. at 3870-71. The government now must decide whether to seek Supreme Court review. Unless and until either Congress or the Supreme Court clarifies the scope of the CFAA, prosecutors in the Ninth Circuit will lose the benefits of a statute that the Department of Justice has come to depend on as a weapon in its war on cyber-crime. Likewise, employers – at least in the Ninth Circuit – will be unable to use the CFAA as a basis for federal jurisdiction when suing employees for misappropriating confidential information in violation of their employment agreements.