The Coverage Inkwell

Emerging Coverage Issues in Intellectual Property, Privacy, and Cyber Liability

White and Williams LLP

Joshua A. Mooney
mooneyj@whiteandwilliams.com

December 14, 2012

THE ORACLE SAYS: FOR CFAA CLAIMS, ALLEGE "HACKING" AND PLEAD WITH PARTICULARITY (SOMETIMES)

In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (discussed in a prior issue of *The Coverage Inkwell*), the 9th Circuit held that wrongful use of a computer system does not fall within the perimeters of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. Specifically, the court held that the phrase "exceeds authorized access," as defined in the CFAA, is limited to "violations of restrictions on access to information, and not restrictions on its use." Thus, where access to a computer system is allowed, but that system is used wrongfully, there is no actionable CFAA claim. In reaching this decision, the *Nosal* court relied upon a parade of horribles, including whether to permit wrongful use cases under the CFAA could lead to the federal incarceration of workers who visited ESPN.com at the workplace in violation of their employers' policies. (Some law clerk must really like ESPN.com!)

Since the 9th Circuit's decision in *Nosal*, and a subsequent 4th Circuit decision in *WEC Carolina Energy Solutions v. Miller*, 687 F.3d 199 (4th Cir. 2012), I have read numerous blogs and articles on the subject, usually beginning with the question: can lying on [insert social media site, usually Facebook] land one in prison? While the thought is startling (no, I don't lie on Facebook), generally I have found such discussions unhelpful for appreciating the real-world implications of *Nosal*. (And when I say real world, I don't mean the MTV show, which was anything but.)

Oracle American, Inc. v. Service Key, LLC, 2012 WL 6019580 (N.D. Cal. Dec. 3, 2012), on the other hand, highlights some effects of the *Nosal* decision's reasoning. The decision also adds another twist to CFAA litigation that is worth noting: some claims brought under the CFAA can be subject to the heightened pleading standards of Fed. R. Civ. Pro. 9(b). The case is as follows:

Oracle supplies hardware and software systems. *Id.* at * 1. Customers who purchase Oracle hardware have the option of purchasing an annual contract for technical support services, which includes software updates such as patches and fixes for its proprietary firmware and operating system software. *Id.* Customers who enter into a technical support agreement with Oracle are provided with access credentials (*i.e.,* a log-in and password), which allow them access to Oracle's support websites to

download the patches, updates, and other support software. *Id.*. As one might imagine, access to these websites is subject to Oracle's Terms of Use, and only users who have entered into a technical support agreement with Oracle are authorized to receive software updates from Oracle's websites. *Id.*

Defendants Service Key and DLT Federal Business Systems (collectively, DLT) became a member of the Oracle Partner Network (OPN), which is a membership program for third-party companies interested in reselling Oracle hardware and/or software. *Id.* To facilitate their role as resellers, OPN members receive log-in credentials to access Oracle's support websites. According to Oracle, DLT fraudulently used such access to obtain Oracle's proprietary software patches and software updates, which it then provided to its own customers even though they had not entered into technical support agreements with Oracle. *Id.* In addition, DLT allegedly distributed its access credentials to Oracle's website to third parties. *Id.*

Oracle filed a multi-count complaint against DLT, including claims for Violation of the CFAA, 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), and (a)(6)(A), alleging that DLT violated the statute (1) by accessing Oracle's websites to obtain updates and patches in order to provide unauthorized support services to DLT's customers, and (2) by disseminating access credentials to third parties and thereby allowing direct access to the websites. *Id.* at *2, 3. The cited sections of the CFAA prohibit the following:

> • "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] ... information from any protected computer." 18 U.S.C. §1030(a)(2);
>
> • "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value .... 18 U.S.C. §1030(a)(4); and
>
> • "knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if—[¶] ... such trafficking affects interstate or foreign commerce[.]"18 U.S.C. §1030(a)(6)(A).

Id. at *3. DLT moved to dismiss most of the claims, including the CFAA claims. *Id.* at *2

The Court began its analysis by describing the purpose of the CFAA, which is "designed to target hackers who accessed computers to steal information or to disrupt or destroy computer functionality, as well as criminals who possessed the capacity to access and control high technology processes vital to our everyday lives." *Id.* at *3 (quoting *LVRC Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)). "The Act proscribes various computer crimes, 'the majority of which involve accessing computers without authorization or in excess of authorization, and then taking specified forbidden actions, ranging from obtaining information to damaging a computer or computer data.'" *Id.* The CFAA, however, "only reaches computer hacking that is intended to procure or alter information, not the misappropriation of such information." *Id.* (citing *Nosal*.)

In the case before it, the court determined that *Nosal* precluded the first two CFAA claims alleged by Oracle—that is, that DLT accessed Oracle's websites to obtain updates and patches in order to provide unauthorized support services to DLT's own customers. In a nutshell, the Court reasoned that because DLT had access credentials, it did not have to hack into Oracle's website, thereby coming within the prohibitions of the CFAA. Discussing *Nosal*, the Court explained:

> The *en banc* panel of the Ninth Circuit affirmed the district court's dismissal of the CFAA counts, holding that the plain language of the CFAA targets the unauthorized procurement or alteration of information—i.e., computer "hacking"—not the misuse or misappropriation of such information. . . .The court reasoned that to conclude otherwise "would transform the CFAA from an anti-hacking statute into an expansive misappropriation statute."

Id. at *5.

Here, the Court concluded, Oracle's first two CFAA claims would do just that—transform the CFAA from an anti-hacking statute into an expansive misappropriation statute. It also held that the *Nosal* decision was not limited solely to claims brought under § 1030(a)(4):

> Oracle alleges that DLT used its "access credentials for Oracle's support websites for the unauthorized purpose of accessing and taking Oracle's proprietary software products, such as certain software patches and updates," and, in turn, used and distributed these products to provide support services to third parties "who could not legally receive them[.]" [Citation omitted.] Such allegations, even if taken as true, are not actionable under CFAA.

Id. (emphasis in original).

The Court specified that Oracle's claims were doomed because they did not allege that DLT had accessed (*i.e.,* hacked) Oracle's website without authorization:

> [Oracle] does not allege that DLT accessed Oracle's website without authorization. To the contrary, Oracle expressly avers that DLT was authorized to access its websites. What Oracle takes exception to is DLT's accessing the websites for the ostensibly improper "purpose" of using its authorized access to provide support services to third parties. [Citation omitted.] This conduct—using legitimate access credentials to access websites and then distributing information obtained from such access to third parties who have no right to receive such information—is precisely the type of conduct that *Nosal* held was beyond the scope of the CFAA.

Id. at *5 (emphasis in original). As a result, the Court dismissed Oracle's claims under sections 1030(a)(2)(C) and (a)(4) *Id.*

The Court, however, also held that *Nosal* does not apply to claims brought under § 1030(a)(6)(A), reasoning that such a claim is not dependent upon whether a system was "hacked" into:

> DLT responds that *Nosal* is not limited to subsection 1030(a)(4), but applies to the entirety of the CFAA. Perhaps so, but that is entirely beside the point. Oracle's claim under subsection 1030(a)(6) is not dependent upon whether DLT "hacked" into Oracle's websites; rather, Oracle is alleging that DLT distributed and/or facilitated the distribution of access credentials to Oracle's support websites to "unauthorized third parties." [Citation omitted.] Thus, *Nosal* interpretation of "exceeds authorized access" is not germane to and does not preclude Oracle from proceeding with a claim under subsection 1030(a)(6).

Id. at *5.

However, the Court also held that Oracle's claim under § 1030(a)(6)(A) must be pleaded with the same particularity as fraud claims, as required by Fed. R. Civ. Pro. 9(b), because the claim itself was grounded in fraud. *Id.* at *6. Noting that the 9th Circuit itself had not yet addressed the issue of whether a CFAA claim must be pleaded with particularity under Fed. R. Civ. Pro. 9(b), the Court stated that the heightened pleading standard can be required even where fraud is not a necessary element of a claim, if "a unified course of fraudulent conduct is alleged" as the basis of the claim. *Id.* at *6. Such claims, the Court explained, are deemed to be "grounded in fraud" and require Rule (b)'s heightened pleading standard. *Id.*

In the case before it, the Court first observed that the pleading standards of Rule 9(b) apply to § 1030(a)(4), which is violated "only if a defendant acts 'with intent to defraud' and its conduct 'furthers the intended fraud.'" *Id.* The Court then found that Oracle's (a)(6)(A) CFAA claim also was subject to the heightened standard because Oracle's claim was "grounded in" fraud:

> Among other things, Oracle avers that DLT fraudulently induced customers of Oracle to cancel their support agreements with Oracle by claiming that it could provide support services at a lower cost than Oracle. [Citation omitted.] In addition, DLT is alleged to have "falsely represented to its customers and potential customers that they could still obtain—from [DLT]—software patches and updates for their Oracle computer products[.]" [Citation omitted.]. To facilitate its scheme, DLT allegedly accessed Oracle's support websites and engaged in the fraudulent trafficking of passwords to facilitate third-party access to those websites and update so that DLT could provide support services to these customers. [Citation omitted.] In view of these allegations, the

> Court finds that under *Kearns*, Oracle's CFAA claims are subject to the particularity requirements of Rule 9(b).

Id. at *6.

What does this case mean? There are a couple of things to take away. First, when facing a CFAA claim, examine exactly what is being alleged and the basis of the claim. If the claim alleges in effect that a computer system was wrongfully accessed through validly-issued credentials, under *Nosal*, any claim under § 1030(a)(2) and (a)(4)will face dismissal. In other words, the complaint needs to allege hacking of some sort. (And, don't read *Nosal* narrowly.) Second, is there a fraud or unified course of fraudulent conduct involved? If so, the heightened pleading standards of Fed. R. Civ. Pro. 9(b) can apply.

Questions are welcome.

The Coverage Inkwell

Joshua A. Mooney | Counsel
1650 Market Street | One Liberty Place, Suite 1800 | Philadelphia, PA 19103-7395
Direct 215.864.6345 | Fax 215.399.9613
mooneyj@whiteandwilliams.com | whiteandwilliams.com
Assistant: Dana Genovese | 215.864-6331

White and Williams LLP