The Coverage Inkwell

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

White and Williams LLP

Joshua A. Mooney
mooneyj@whiteandwilliams.com

October 11, 2013

FALSE ACCOUNTS ON SOCIAL MEDIA DOES NOT VIOLATE THE COMPUTER FRAUD AND ABUSE ACT

Let me take a moment to thank everyone for another successful Coverage College. This year, we had over 600 attendees from 130 different companies and traveling from 18 different states. I also wish to thank everyone who attended the Cyber and Technology Insurance Master Class that I gave with my colleague Jesse Dunbar. We had a packed house. Thank you!

No question about it, fake profiles are a fact of life in social media. Facebook has estimated that almost 10% of its accounts are duplicates or false. *See* Somini Sengupta, *Facebook's False Faces Undermine its Credibility,* N.Y. Times, Nov. 12, 2012.[i] Anyone who knows Twitter knows that there are fake accounts abound, some of which can be light-hearted and humorous. *See* Caitlin Moore, *Fake Twitter: The parody accounts to lighten up your news stream,* Wash. Post, Mar. 6, 2012[ii]. Law enforcement also has made use of fake social media accounts, and continues to do so in greater numbers. *See* Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool,* CNN, Aug. 20, 2012;[iii] Jessica Roy, *New NYPD Social Media Guidelines Says It's Okay to Use Fake Facebook Profiles to Monitor Citizens*, Observer.Com, Sept. 12, 2012.[iv]

I raise these examples not to state the obvious, but to illustrate why more and more courts are reluctant to endorse broad interpretations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("CFAA") to involve violations of policies governing computer use or websites, even where the conduct in question may not be innocent or well-intentioned. *Matot v. C.H.,* -- F. Supp. 2d --, 2013 WL 5431586 (D. Or. Sept. 26, 2013) is a perfect example.

In *Matot*, plaintiff, who was an assistant principal at a middle school, alleged violation of the CFAA in a civil action brought against students at his school and their parents. The CFAA claims were based on alleged use "without authorization" of social media services (e.g., Facebook and Twitter) in that the defendants violated terms of use of the social media services by creating fake accounts using the plaintiff's name and likeness. *Id.*, at *1. Plaintiff alleged that the students then used the fake accounts to invite other students to communicate with "him" and to publish false and defamatory statements and images about or attributed to him. *Id.* at *3.

The court dismissed the CFAA claims. In doing so, it relied upon previous decisions rendered by the Ninth Circuit regarding the scope of the CFAA, *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012) and *LVCR Holdings, LLC v. Brekka*, 581 F.3d 1127 (9th Cir. 2009), as well as the rule of lenity, which requires courts to construe criminal statutes narrowly. *Id.* at *1.

Specifically, the court focused its discussion on potential prosecutorial abuse should the CFAA be construed broadly to include the type of claim alleged in the case before it. It noted the Ninth Circuit's disapproval of the criminal prosecution in *United States v. Drew*, where a mother, who had cyber-bullied her daughter's classmate by posing as a 16-yeard-old boy, was charged under the CFAA. *Id.* at *2. Noting the wide existence of fake social media accounts, the court agreed with the *Nosal* court's concern that a broad interpretation of the CFAA could turn "millions of unsuspecting individuals" into perpetrators of computer crime. *Id.* at *3. The court explained:

> The CFAA's focus is "on hacking" rather than the creation of a "sweeping internet-policing mandate." *This court cannot fail "to consider the effect on millions of ordinary citizens caused by" recognizing plaintiff's claim.* Plaintiff alleges that defendants created false social media profiles in his name and likeness. Yet, as indicated in *Nosal*, "lying on social media websites is common." For example, in June 2011, Facebook predicted that approximately 83 million of 855 million active users were duplicates, false or undesirable. Twitter is also thought to have a large number of "fake" accounts. More recently, police departments have taken to creating false profiles for the purpose of law enforcement. Were this court to "adopt the [plaintiff's] proposed [argument], millions of unsuspecting individuals would find that they are engaging in criminal conduct," in addition to any civil liability.

Id. at *3 (internal citations omitted) (emphasis added).

Some may read this case as yet another decision that narrows the scope and reach of the CFAA. But I am not so certain that is right. Although the court rejected Plaintiff's theory and dismissed his claims, it also cautioned against reading the Ninth Circuit's decisions too broadly.

When discussing *Brekka*, the court suggested that concluding whether or not the CFAA applied merely by determining whether the defendants in question had access to the computer or network used would wrongly narrow the statute beyond its intent:

> Likewise, this court doubts that even the *Brekka* Court would enforce its "without authorization" language to the extent implicated. For example, if a hacker targeted a United States governmental website for malicious purposes, such a hacker may be "authorized" to access the website under *Brekka* because many governmental websites are open

> to the public. In other words, if interpreted strictly, *Brekka* could preclude CFAA application of "without authorization" to hackers who breach governmental websites that are open to the public.

Id. at *1. The court's suggested solution is to not apply *Brekka* outside an employment context: "strict adherence to *Brekka's* bright-line rule outside of the employment context appears to be in conflict with the underlying legislative purpose." *Id.* But such a construct seems too artificial to be reliable.

The court also interpreted the Ninth Circuit's decision in *Nosal* to permit liability under the CFAA for employees who may have had access to a network, but not to a database in question. The court stated that, under *Nosal*, "exceeds authorized access would apply to inside hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)." *Id.* at *2 (quoting *Nosal*). "The [*Nosal*] Court further provided that 'hacking' colloquially refers to 'someone who's authorized to access only certain data or files but accesses unauthorized data or files.'" *Id.* (quoting *Nosal*, 676 F.3d at 856–57). This appears to be where the "solution" is heading.

What does this case mean? Since *Nosal*, more and more courts have construed the CFAA narrowly when interpreting the phrases "without authorization" and "exceeds authorized access" under the statute. In doing so, they have rejected the breach of agency test and the intended-use analysis previously promulgated by the Seventh and Fifth Circuits. Thus, this case illustrates that the pendulum continues to swing in favor of narrowly construing the CFAA, even where the conduct in question is not innocent, in light of the fear that a broad interpretation of the statute would criminalize widespread behavior. Some readers might observe that the *Matot* district court is in the Ninth Circuit and that, therefore, it had no choice but to rule as it did. I won't argue with that. However, the *Matot* opinion makes clear that the court agreed with the Ninth Circuit's fears and was not just following *Nosal*.

Yet, the court also took the opportunity to observe that the Ninth Circuit's decisions should not be read so broadly as to neuter the statute. While a violation of the CFAA should not exist for the mere reason that the defendant violated a term of use for a computer or website, the court also reasoned that whether or not a party is free and clear of the proscriptions of the statute should not hinge solely on whether allowable access to the computer or website existed. This is where things get interesting.

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

---

[i] http://www.nytimes.com/2012/11/13/technology/false-posts-on-facebook-undermine-its-credibility.html.
[ii] http://www.washingtonpost.com/blogs/arts-post/post/fake-twitter-the-parody-accounts-to-lighten-up-your-news-stream/2012/03/01/gIQALpiptR_blog.html.
[iii] http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html.
[iv] http://betabeat.com/2012/09/new-nypd-social-media-guidelines-say-its-okay-to-use-fake-facebook-profiles-to-monitor-citizens/.