

Believe It, Or Not: Social Media Information Can Be A Trade Secret

Written By **E. Bradley Evans** (ebe@wardandsmith.com) and
Joseph A. Schouten (jas@wardandsmith.com)

June 5, 2013



Because social media is now a vital advertising tool for businesses, it is important that your business be able to protect its social media accounts, messages, and information from unauthorized use or access. Recent court decisions demonstrate that one way your business may be able to protect its social media information is by making it a trade secret.

Introduction

From Twitter®, to Facebook®, to LinkedIn®, social media has become an essential tool used by almost all businesses to market themselves, obtain customers, and establish their brand. Consumers are relying more than ever on social media when making decisions about where to spend their money. Because social media is now a vital advertising tool for businesses, it is important for your business to protect its social media accounts, messages, and information from unauthorized use or access. Recent court decisions demonstrate one way that your business may be able to protect its social media information by making that information a trade secret.

This is consistent with our previous Techwire article, where we discussed the value of trade secret protection resulting from the very flexible legal concept of trade secrets and the broad array of information that potentially fits into that concept. In another Techwire article, we addressed the need for you to think critically about your business's trade secrets on an on-going basis so that you can preserve the trade secret status of your commercially-sensitive information.

Twitter® and Trade Secrets

As mentioned above, a number of courts have recently confronted the issue of whether social media information and access rights should be considered trade secrets. One notable example occurred in a federal court case in California. In that case, the plaintiff brought an action against one of its former employees based on his continued use of a Twitter® account that the plaintiff alleged it owned and that contained trade secrets.

The plaintiff operated a web-based resource for news and reviews pertaining to mobile phones and carriers. It used a variety of social media outlets to promote its services, including Twitter®, Facebook®, and YouTube®. The former employee worked for the plaintiff as a product reviewer and video blogger and was given use of the Twitter® account "@PhoneDog_Noah" and the password for that account in order to disseminate content.

According to the plaintiff, the followers of the account and its password constituted confidential, proprietary, and trade secret information. Upon leaving employment with the plaintiff, the employee changed the account handle to "@noahkravitz," but continued to use the account and refused to relinquish control of it back to the plaintiff. As a result, the plaintiff initiated an action against the employee for, among other things, misappropriation of trade secrets under California's version of the Uniform Trade Secrets Act.

The employee initially argued that the trade secrets claim against him should be dismissed because the items at issue in the case – Twitter® followers and the Twitter® password – could never be trade secrets. Specifically, he argued that the followers of the account could not be a trade secret because they were "publically available for all to see at all times." With regard to the account password, he claimed that it had no independent commercial value – that it merely allowed the individual logging in to view information already widely known. He also argued that he had personally created the password, and that the plaintiff had not undertaken reasonable efforts to maintain its secrecy.

Without a great deal of analysis, the court rejected the employee's argument. The court found that the plaintiff had identified its alleged trade secrets (the account followers and password) with sufficient particularity, and that "[a]t this stage, these allegations are sufficient to state a claim." In essence, the court determined that "whether the password and Account followers are trade secrets...requires consideration of evidence beyond the scope of the pleading." Accordingly, the court allowed the plaintiff to continue to pursue its trade secrets claim against its former employee.

While the court left open the possibility that the employee might be able to eventually defeat the trade secrets claim if the plaintiff failed to show that the account followers and the password were trade secrets, the ruling is significant for employees and businesses that use social media as part of their business promotion. Under the court's ruling, businesses alleging the unauthorized use of social media accounts may have a valid claim for misappropriation of trade secrets and likely will be permitted to develop such claims through the litigation process.

MySpace®/Facebook® and Trade Secrets

In a federal court case out of Colorado, the court reached a similar conclusion involving MySpace® information. The Colorado federal court found that information relating to a MySpace® account is potentially a trade secret. The plaintiff had founded various nightclubs in the Denver area in the 1990s and had employed an individual to assist it in booking DJs to perform at its nightclubs. The employee ultimately left the plaintiff to form another company where, among other things, he opened a nightclub that competed with the plaintiff's.

The plaintiff filed a lawsuit against the former employee and his company. One of the plaintiff's claims was for trade secret misappropriation. Specifically, the plaintiff alleged that the defendants "misappropriated their trade secrets, including login information for profiles on MySpace, [and] lists of MySpace 'friends'...."

Like the employee in the California case discussed above, the defendants claimed that the plaintiff should not be able to pursue its trade secrets claim because a MySpace® profile and "friends" could never qualify as trade secrets. After conducting a much more thorough analysis than the California court, the Colorado court reached the same conclusion. Specifically, the Colorado court concluded that "[w]hether plaintiffs' MySpace friends list is a trade secret is [a] question of fact." Therefore, the court refused to dismiss the plaintiff's trade secrets claim and, instead, allowed the plaintiff the opportunity to further pursue and develop that claim in litigation.

Conclusion

Social media has become a crucial marketing tool for many businesses today. Businesses invest significant resources in establishing and developing their social media networks and messages. Therefore, a business originating social media information obviously would like to keep departing employees or others from using that social media information to compete against it.

The cases discussed above are important for businesses like yours that wish to protect against their social media information being used by a competitor. The cases discussed in this article suggest that if your business can establish the right facts – e.g., that there is some "secret" information and that your business made efforts to protect the secrecy of that information – your business may be able to prevent former employees or others from using your social media information.

Although these cases suggest that trade secret protection for social media is possible, they also make clear that your business will not ultimately prevail on such a claim if it is not thinking critically about trade secret protection for its social media information on a forward-thinking and on-going basis. For example, in order to take advantage of the theory recognized in the cases discussed here, your business should do a number of things proactively to bolster a potential claim that its social media information is a trade secret. These steps include:

- Limiting access to the social media information within the company;
- Obtaining confidentiality agreements with those employees who will have access to the social media information; and,
- Using passwords to protect any sensitive social media information.

By taking steps such as these, and by adequately documenting them, your business will take a big step toward protecting its "social" information and status.

--

© 2024 Ward and Smith, P.A. For further information regarding the issues described above, please contact E. Bradley Evans or Joseph A. Schouten.

This article is not intended to give, and should not be relied upon for, legal advice in any particular circumstance or fact situation. No action should be taken in reliance upon the information contained in this article without obtaining the advice of an attorney.

We are your established legal network with offices in Asheville, Greenville, New Bern, Raleigh, and Wilmington, NC.