Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Are Social Networking Contacts Trade Secrets?

Law360, New York (December 11, 2012, 12:48 PM ET) -- Use of social media by businesses has not only increased exponentially in the past few years, but is now a ubiquitous tool in marketing strategy. From your local food truck to national insurance companies, businesses make use of online accounts such as Twitter and LinkedIn to gain customers and maintain market advantage.

But who owns these social media profiles and contacts, and are they viable trade secrets? Legal instinct and traditional trade secret law may lead one to think that because social networking profiles and contacts are generally known to the public, they cannot possibly be trade secrets. The answer, however, is not so simple.

While the case law is still in its infancy, at least two courts have suggested that social media profiles, contacts and login/password information to those accounts could be possible trade secrets. No matter how these cases are resolved, trade secret litigation over social media accounts is on the rise, and businesses would do well to have robust policies regarding social media use, maintenance and account ownership.

Social Networking Contacts as Traditional Trade Secrets

In Christou v. Beatport LLC, the issue centered around a nightclub's Myspace list of "friends" as well as login information for profiles on Myspace. Christou owned multiple nightclubs and employed the defendant to help him promote the clubs. The defendant eventually left to open a competing nightclub. The District of Colorado considered Christou's misappropriation of trade secrets claim to be viable.

The court looked to factors set out by the Tenth Circuit:

- Whether reasonable steps were taken to protect the secrecy of information;
- Whether access to information was restricted;
- Whether employees knew customers' names from experience;
- Whether customers commonly dealt with more than one supplier;
- Whether customer information could be readily obtained;
- Whether customer information is readily ascertainable from outside sources;
- Whether the owner of the customer list expended great cost and effort over a considerable amount of time to develop the files; and
- Whether it would be difficult for a competitor to duplicate the information.

Though the defendant argued that a list of Myspace "friends" could not be a trade secret because it is broadcast to the world, the court, in applying the factors above, observed that the plaintiff had secured the Myspace profiles and limited access to the profiles through passwords that were given only to employees who required access to promote the nightclubs.

The court also noted that "friends" or contacts on social networking sites are more than just simple lists of names of potential customers. "Friending" a business or individual grants access to personal information as well as contact information. The court agreed with the plaintiff that a "friends" list could be similar to a database of contact information, and thus that type of information ancillary to the public list of names is not readily ascertainable from outside sources.

Furthermore, the court explained that it appeared the plaintiff spent some cost and effort in developing its social network accounts, that the defendant was hired in part to maintain the lists and profiles, and that it could be difficult for the defendant to duplicate the Myspace lists with ease or within a time frame that would be useful to him. Upon review of the above factors, the court left open the possibility that the Myspace "friends" list could be a trade secret.

Similarly, in PhoneDog v. Kravitz, plaintiff employer PhoneDog survived a motion to dismiss a misappropriation of trade secrets claim. As a PhoneDog employee, Kravitz maintained the Twitter account "@PhoneDog_Noah," promoted through Twitter on behalf of PhoneDog, and garnered some 17,000 followers through that account.

After his employment ended, Kravitz kept the account (and password to the account) but changed the display name on the account to his name, removing any reference to PhoneDog in the display name. PhoneDog sued Kravitz for misappropriation of trade secrets, citing the list of Twitter account followers and the account password as trade secrets.

Kravitz argued that the identity of the Twitter followers on the account was available to all at all times, and thus could not be a trade secret. The Northern District of California ignored this argument as premature and allowed PhoneDog's claim to continue.

Both the PhoneDog and Christou determinations were in the context of the courts' denial of defendants' motions to dismiss, so whether the nightclubs' or PhoneDog's social networking contacts will eventually hold up to be trade secrets in the long run awaits a thorough factual inquiry.

Employers May Still Lay Claim to Contacts, Even if Not Trade Secrets

At the end of last year, the Eastern District of Pennsylvania in Eagle v. Morgan found that a person's LinkedIn account connections do not constitute trade secrets, as the connections are generally known in the wider community.

Linda Eagle was an executive at Edcomm, and under her management, Edcomm implemented a policy requiring employees to create and maintain LinkedIn accounts. Eagle's account was used for Edcomm business, and Edcomm employees developed and maintained her account.

When Eagle's employment was terminated, Edcomm changed the password to her LinkedIn account and replaced her picture and name with that of the interim executive. Eagle brought action against Edcomm under the Computer Fraud and Abuse Act and Lanham Act, and Edcomm counter-claimed for, among other things, misappropriation. The court granted summary judgment for Edcomm on Eagle's federal claims earlier this month.

Though the court dismissed a misappropriation of trade secrets claim based on the fact that a person's LinkedIn connections are publicly known, the court did not dismiss Edcomm's misappropriation of an idea claim. Because Edcomm employees developed and maintained the LinkedIn connections, which were the route through which Edcomm did business, the court allowed the claim to survive.

The Eagle case shows that even if courts do not classify social networking contacts as a traditional trade secret, employers could still be deemed to own these lists via other analyses.

Importance of Social Media Policies

Time-consuming litigation over who owns social media content when an employee leaves can be avoided by the implementation of a robust social media policy or agreements that cover such content. Even if litigation is inevitable, the existence of such policies and agreements can be a huge advantage.

For example, in Ardis Health v. Nankivell, defendant Nankivell was hired to maintain websites, blogs and social media pages in connection with the online marketing of plaintiffs' products. She alone had all the access information to the social media accounts.

At the start of her employment, she signed a work product agreement that covered the social media access information and that stated she must return such information upon her departure. When she was terminated, plaintiffs asked Nankivell to turn over the account information, but she refused, making it impossible for plaintiffs to update their online marketing presence.

In the context of a preliminary injunction, the Southern District of New York ruled that Nankivell must return the access information because it was uncontested that plaintiffs owned the information, due to the signed agreement.

As Ardis Health indicates, having a solid written social media policy or agreement that covers social media content can be an invaluable asset. Below are a few elements to consider in a social media policy:

- Define what social media is and explain what the policy covers.
- Provide concrete examples of conduct abiding by the policy and conduct that would violate it.
- Make clear that social media contacts obtained while working on behalf of the company are the property of the company.
- If employees maintain social media accounts on behalf of the company, specify that they must give login and password information to the company before their departure.
- Keep the policy up to date. The way businesses and individuals connect via social media changes as technological innovation changes — fast. Make sure the policy captures the most current developments.
- In addition to a written social media policy, consider periodic training sessions regarding the policy. Explain to employees what a trade secret is, and give concrete examples of why the social media policy matters. Including employees in the discussion creates a sense of collaboration, rather than control.
- Have employees sign the written policy or a separate agreement that states they will follow the policy.

While this is by no means an exhaustive list of elements to include in a social media policy, with these points in mind, businesses can be better prepared to face trade secret challenges regarding social media content.

--By Michael H. Bunis and Diana T. Huang, Choate Hall & Stewart LLP

Michael Bunis is co-chairman of the trade secret group at Choate Hall & Stewart in Boston. Diana Huang is an associate in the firm's Boston office.

The opinions expressed are those of the authors and do not necessarily reflect the views of the firm, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.