Who Owns Your Company's Social Media Account – You, Or One Of Your Employees?

Insights
4.05.16

Employers have been asking an important question with more frequency in recent times: who owns the company's social media account – the employer or the employee running the account? Business social media accounts often contain a lot of pertinent and valuable information, and unfettered access to that account could give a departing employee a fast head start towards competing with you.

While the last few years have seen a slew of litigation about these issues, there has been a scarcity of reported decisions by courts. One such decision is a recent federal court opinion from Illinois in the case of *CDM Media USA, Inc. v. Simms.* Although the court's decision doesn't settle any issues, it does highlight some important steps you can take to safeguard your information.

Control Of LinkedIn Group In Question

When Robert Simms was an employee of CDM, a marketing and media services company, he was the contact person for a special LinkedIn group started by the company containing its customers and potential customers. After Simms left the company, CDM wanted the group contact switched over to one of its current employees. It also demanded that Simms relinquish any names, addresses, conversations, etc., garnered from the LinkedIn account. Simms refused to turn over the information.

CDM sued Simms for breach of contract, misappropriation, and violation of the state's trade secret act. The ex-employee responded by asserting that the company had no property rights to the information. He claimed that he was not contractually required to transfer the information because transfer of control of the LinkedIn group was not covered by the confidentiality provision in his non-compete agreement. He also argued that the LinkedIn group account and pertinent communications did not fall under the state's trade secrets act, and thus were not subject to a claim under that statute.

Lack Of Definitive Agreement Led To Confusion

Simms filed a motion to dismiss, asking the court to toss out the claim. The judge split the baby on the motion but essentially left all causes of action intact. In making his ruling, the judge noted that the ownership or control of the LinkedIn group account was not nailed down by the company in any agreement or policy it had relating to Simms or any other employee. If the company had created

some concrete proof of ownership, the unresolved factual issues described by the judge's opinion would not exist.

Other Cases Starting To Crop Up

The CDM case is not the only case of its kind that provides guidance for employers on how to best protect your social media accounts. There have been other lawsuits where at least part of the legal claim at issue is ownership of a company social media account. In a California case, a Twitter feed was found to be company property because of the time and expense the company put into developing and maintaining the account (*PhoneDog v. Kravitz*). Also, in a New York case, a court held that a social media account was owned by the company due to a written agreement which provided for ownership (*Ardis Health, LLC v. Nankivell).*

Lessons To Be Learned

At the very least, you should develop a social media policy that addresses issues including retention of company social media accounts, account information, and communications. You should ensure that all of your employees sign the policy. As part of the policy, make clear that any posting on company social media is the property of the company along with the accounts, the names, etc., associated with the accounts.

Further, the policy should clearly state that when an employee leaves, all account information and communications are to be transferred back to the company. Further, the policy should describe what, if any, information you consider to be confidential. This way, when an employee leaves, the account information stays with your company.

Of course, if you have an employment agreement, you should consider including these provisions in the "Confidentiality" section and inserting a clause requiring the return of all information and cooperation in the transfer of any company accounts. This will at least let your employees know where they stand if they leave the company and will provide you with extra ammunition to keep your information where it belongs.

Final Warning

Before finalizing any policy, you need to keep in mind that several states have enacted statutes that limit the interception and monitoring of social media. Laws are different across state lines, but a typical one can be found in California, where you are prohibited from requiring or requesting employees or applicants to disclose their username or password for their social media account.

Many state laws also prohibit you from requiring the employees or applicants to access their social media account in your presence. However, in many states, you may make a reasonable request that an employee divulge personal social media account information if it is relevant to an investigation of employee misconduct.

Because of the varied obligations you face across the country, you need to stay up-to-date on all the developments in the states in which you do business, particularly if you operate in multiple

developments in the states in which you do business, particularly if you operate in multiple jurisdictions.

A version of this article originally appeared at the Fisher Phillips Non-Compete and Trade Secrets blog, which can be found by clicking here or visiting noncompetenews.com.

For more information, contact the author at ALambert@fisherphillips.com or 214.220.8324.

Related People

Arthur V. Lambert
Senior Counsel
214.220.8324
Email

Service Focus

Privacy and Cyber