ARTICLES

# Maintaining Control of a Company's Social Media Accounts

By Joseph J. Blyskal and Delaney M. Busch – November 3, 2015

Careful thought should be given to the level of access and control retained by a company over social media accounts when drafting employee handbooks, nondisclosure agreements, and social media usage policies. That care is essential to avoid potential claims in later litigation that the company failed to preserve electronic data in such accounts. It is obvious that permitting sales employees to access social media in order to maintain sales contacts, develop client leads, and promote the company can drive business and provide a valuable database of clients and contacts for employers. Underscoring their value, many courts now recognize that an employee's social media accounts and online connections may qualify for protection as trade secrets. By definition, in order to maintain the confidentiality of any trade secrets in these accounts, employers must necessarily exercise some level of control over the accounts. Consequently, permitting employees to control social media accounts in connection with company business may broaden the scope of the company's duty to preserve information and data, and provide the same in discovery.

In creating appropriate policies governing employee use of social media, particularly social media accounts that an employer intends to claim contain confidential company information such as client lists and customer preferences, two legal principles must be counterbalanced as a matter of risk management. First, a company must exercise sufficient control over access to the information contained in the accounts to meet the minimum requirements for trade secret protection. Second, a company must be prepared to preserve potentially relevant evidence within its control once it becomes reasonably likely that it may become a party to litigation. Under a broad application of the test for "control" in the discovery context, companies risk expansive preservation efforts and costly discovery where multiple employees maintain social media accounts in connection with their employment and company policies impose restrictions on employee use of the accounts, or provide that the company may access the accounts, notwithstanding that the accounts may not be company-owned accounts. At the same time, failure of a company to control access to these accounts may lead to a finding that the account is not a protectable trade secret. A company should carefully understand its social media platforms and the risks to its trade secrets presented by unfettered access, while also taking care to avoid expanding its discovery obligations or increasing the risk of claims for failure to preserve evidence by having expansive policies that give the employer control over multiple accounts.

**Trade Secret Protection for Social Media Accounts**

Courts now recognize and afford trade secret protection to information contained in social media accounts as well as the accounts themselves. More than a few courts have recognized that social media accounts have intrinsic value beyond the number of connections they contain.

> The trade secret is not merely the list of names but their email and contact information as well as the ability to notify them and promote directly to them via their MySpace accounts. . . . The names themselves, readily available to the public, are not the important factor. The ancillary information connected to those names cannot be obtained from

> public directories and is not readily ascertainable from outside sources, and thus this militates in favor of trade secret classification.

*Christou v. Beatport, LLC*, 849 F. Supp. 2d 1055, 1076 (D. Colo. 2012); *see also* *CDM Media USA, Inc. v. Simms*, No. 14 CV 9111, 2015 U.S. Dist. LEXIS 37458 (N.D. Ill. Mar. 25, 2015) (finding that members of a LinkedIn group may be a protectable trade secret notwithstanding that the existence of the group is known to the public); *Cellular Accessories for Less Inc. v. Trinitas LLC*, No. CV 12-06736 DDP, 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. Sept. 16, 2014) (recognizing that LinkedIn contacts may be protectable trade secrets); *Ardis Health, LLC v. Nankivell*, No. 11 Civ. 5013, 2011 U.S. Dist. LEXIS 120738 (S.D.N.Y. Oct. 19, 2011) (finding that employer had ownership rights in login information to a social media account).

As with other forms of trade secrets, courts are careful to scrutinize the level of access provided to the information in determining whether there is the requisite confidentiality. As a general proposition, the more control the employer retains over who can access the accounts, such as through password protection and limiting the number of employees and which employees may access the account, the more likely a court is to find the information protectable. However, the level of control required is not particularly high. For instance, *PhoneDog v. Kravitz*, No. C 11-03474 MEJ, 2011 U.S. Dist. LEXIS 129229 (N.D. Cal. Nov. 8, 2011), involved a company Twitter account with the handle "@PhoneDog_Noah." The account was used by an employee named Noah to promote the PhoneDog company services. After four years of working for PhoneDog and using the account containing his name, the employee left the company and changed the handle on the Twitter account to "@noahkravitz." The U.S. District Court for the Northern District of California declined to dismiss PhoneDog's claim for misappropriation of trade secrets, suggesting that Twitter followers and a Twitter password for the account may in fact be trade secrets, notwithstanding that the account was managed by and contained the name of the employee. *See also* *Eagle v. Morgan*, No. 11-4303, 2012 U.S. Dist. LEXIS 143614 (E.D. Pa. Oct. 4, 2012) (rejecting claims by founder of company that company misappropriated her likeness by changing the account name, photograph, and password on the LinkedIn account after she left employment, even though she had founded the company and opened the LinkedIn account).

On the other hand, the U.S. District Court for the Eastern District of New York took the opposite view, recognizing that client needs, preferences, hiring practices, business strategies, and network connections may have been protectable trade secrets at a different time when considerable effort and resources were expended to develop the information, but ultimately concluding that, "for good or bad, the exponential proliferation of information made available through full-blown use of the Internet and the powerful tools it provides to access such information in 2010 is a very different story." *Sasqua Grp., Inc. v. Courtney*, No. CV 10-528, 2010 U.S. Dist. LEXIS 93442, at *62–63 (E.D.N.Y. Aug. 2, 2010) (holding that such information was not protectable where adequate safeguards were not taken to protect information and the information was available on the Internet). Notwithstanding that sentiment, the trend appears to be to recognize that even social media accounts, which are public, with much of the

information they contain accessible to outsiders by their very nature, can constitute trade secrets where appropriate controls are in place to limit access to the account.

**The Duty to Preserve Evidence**

As recognized in the often cited *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003), "[i]dentifying the boundaries of the duty to preserve involves two related inquiries: *when* does the duty to preserve attach, and *what* evidence must be preserved?" Presently, this is perhaps truest in the world of social media. In general terms, a party that reasonably believes that it may be involved in litigation has a duty to preserve evidence that it knows to be relevant to the dispute, or which may lead to the discovery of admissible evidence. Fed. R. Civ. P. 26. As with tangible documents, this duty extends to electronically stored information (ESI) within the possession, custody, or control of the party. For purposes of discovery, control "is broadly defined, and includes situations where the party 'has the practical ability to obtain the documents from another, irrespective of his legal entitlement to the documents.'" *Raimey v. Wright Nat'l Flood Ins. Co.*, 76 F. Supp. 3d 452, 470 (E.D.N.Y. 2014). "The party is not required to have legal ownership or actual possession of documents, but documents are in a party's control 'when that party has the right, authority, or practical ability to obtain the documents from a non-party to the action.'" *Oriental Trading Co. v. Yagoozon, Inc.*, No. 8:13CV351, 2014 U.S. Dist. LEXIS 139677, at *2–3 (D. Neb. Oct. 1, 2014) (quoting *In re Hallmark Capital Corp.*, 534 F. Supp. 2d 981, 982 (D. Minn. 2008)).

Given the relatively low threshold of control required for trade secret protection and the broad definition of control for discovery purposes, social media accounts used to promote business or sales present a unique challenge. Common restrictions (read: control) placed on confidential information—such as social media accounts—include limiting access to key employees, implementing a password policy, and requiring nondisclosure agreements. Additionally, social media usage policies often provide that an employee does not have an expectation of privacy when accessing a social media account for work purposes, or from a work station, and place limitations on what the account may be used for and what statements may be made using the account. Often, these policies seek to limit employee conduct after work hours on their personal accounts. Indeed, implicit in each of the foregoing decisions concerning social media accounts is that the company exercises a level of control over the social media. Discoverable information—and the duty to preserve—may include ESI maintained on company social media accounts, such as company Facebook pages, LinkedIn accounts, or Twitter accounts, or individual employee accounts used for work purposes if the employer exercises control over such accounts.

**Practical Considerations**

Absent deliberately considered policies controlling the use, preservation, and confidentiality of information contained in social media accounts, a company may inadvertently permit destruction of ESI on the one hand or waive trade secret protection on the other hand, given the overlapping considerations of control and confidentiality. Notably, information contained on social media accounts is usually stored and managed by the service provider. For instance, the current version of the Facebook "Data Policy" provides: "We store data for as long as it is necessary to provide

products and services to you and others . . . . Information associated with your account will be kept until your account is deleted, unless we no longer need the data to provide products and services." Facebook expressly reserves the right in its"Statement of Rights and Responsibilities" to "stop providing all or part of Facebook to you." Similarly, the LinkedIn "User Agreement" provides that user services may be terminated and that upon termination the right to access is lost.

To avoid potential destruction of ESI or inadvertent disclosure of confidential information contained in these accounts, the terms of service and privacy policies of the platform should be thoroughly reviewed. Careful consideration should also be given to a company's own internal policies governing company data stored on these sites, such as iterations of a company mission statement, representations about services or products, or online feedback in the form of "comments" provided by consumers. Query the result where a company is on notice of litigation but fails to preserve information contained in its Facebook account, and Facebook elects to suspend access to the account for any reason or no reason at all under its terms of use during the pendency of litigation. Similarly, if a company elects to use a social media platform to maintain information it considers a trade secret, query whether and to what extent unfettered access to the information by the service provider—as provided in broadly worded user agreements—could provide an argument that the information is not maintained as confidential.

**Conclusion**

Social media can be beneficial to businesses. However, without appropriate policies in place concerning access to and use of the account, a company may place its trade secrets in jeopardy or risk unintentional destruction of ESI. Knowing who can access the information contained in the accounts, carefully defining the scope of control a company has over employee-accessible social media accounts, and understanding the risks associated with using this technology in competitive industries should help to protect company property and avoid potentially costly discovery mistakes.

**Keywords:** litigation, commercial, business, confidential, discovery, electronically stored information, ESI, inadvertent disclosure, preservation, social media, trade secrets

Joseph J. Blyskal and Delaney M. Busch are with Gordon Rees Scully Mansukhani LLP in Glastonbury, Connecticut.