



HCCA's interns built a robust library of 2,000 compliance documents for you

Rob Tungseth and Tescia Veldhouse

See page 16

23

**Audit
committee's
role
in
compliance**

Kelly Nueske

29

**Who "owns"
social media—
you or your
employees?**

Karen R. Glickstein and
Latrice N. McDowell

35

**Overpayments
and other common
reasons for denial
of Medicare
enrollment**

Lester J. Perling

39

**DOJ seeks reversal
of decision that could
significantly impair
False Claims Act
enforcement**

Adam S. Lurie and Jodi L. Avergun

by Karen R. Glickstein and Latrice N. McDowell

Who “owns” social media— you or your employees?

- » Companies should consider who “owns” a social media account when the employee leaves the company.
- » Ownership of social media accounts may depend on how the employer uses social media and who opened the account initially.
- » Most social media accounts are considered personal to the employees, who retain access to the accounts when they leave employment.
- » Companies may be liable for violating privacy rights of their employees if they attempt to seize the accounts.
- » Companies should consider updating social media policies to reflect these issues.

Karen R. Glickstein (kglickstein@polsinelli.com) is a Shareholder and
Latrice N. McDowell (lmcdowell@polsinelli.com) is an Associate in the
Kansas City office of Polsinelli PC.

Over the past several years, social media has become a regular source of communication for both employees and employers. Some social media sites, such as Facebook, which were initially perceived as more “personal” and “social” forms of communication, have increasingly been used by businesses as a method of marketing and promoting services. Similarly, more “professionally oriented” social media sites, such as LinkedIn, have gained members and have actively promoted themselves as a way to network online, expanding their format and platform to encourage even more business-to-business and professional interaction. In the case of all social media, the technology encourages increased interaction between a business and its customers for both sharing information and generating business.

As with many types of new technology, the prevalence of social media in the business world raises a number of questions regarding the implications of its use in building practices and increasing business. Because of the very nature of social media, most employees view their social media accounts as personal, even though

they may use the accounts to promote their professional careers, either directly (through posting information designed to increase business and to make their names known in the professional worlds in which they operate) or indirectly (such as simply listing an employer on a Facebook profile page).

Organizations that use social media for business-related purposes (whether marketing based or simply informational), or suggest or require that employees use social media in conjunction with their employment, should ensure that policies exist, or at least are considered, regarding ownership of the account when the employee leaves the business or practice. Cases addressing precisely this issue have begun to wind their way through the court system.

Rise of social media

The increased use of social media in both personal, and especially, professional, contexts has resulted in new questions regarding the use, and potential misuse, of information posted to these websites. As the technology develops, companies and individuals have more frequently turned to the court system to help resolve their disputes.



Glickstein



McDowell

Phonedog v. Kravetz

In 2011, a company sued its former employee in federal court in California,¹ alleging that he had misappropriated company information when he continued to use and maintain a Twitter account after leaving employment. The employee used a Twitter account created by the company to promote himself and the company's services. In the lawsuit the company alleged that it considered the passwords to all of its Twitter accounts "confidential" because the information was maintained in confidence by the company and only provided to employees who promoted the company, thus constituting proprietary, confidential information. When the employee voluntarily left his employment, he had approximately 17,000 followers on Twitter. The company asked the former employee to turn the account over to the company, but he refused. Instead, he continued to maintain and use the account, changing his user name so that it was not representative of the company and continuing to "tweet" to all the individuals who had chosen to "follow" him during his employment.

The company sued the employee for misappropriation of trade secrets, interference with prospective economic advantage, and conversion. The employee filed a motion to dismiss the case, which the trial court granted in part and denied in part, finding that the employer had adequately plead a potential claim for misappropriation of trade secrets and rejecting the employee's claim that the Twitter "followers" were public information. The court did, however, dismiss the interference with prospective economic advantage

claim, because the company did not allege the nature of its economic relationship with the Twitter followers. The district court also denied the employee's motion to dismiss the conversion claim, because the employer admitted that the employee was permitted to use the Twitter account. The parties settled the case before trial.

Maremont v. Susan Fredman Design Group

A slightly different situation was presented to an Illinois federal court when an interior designer sued her former employer and the owner of the company individually, alleging her privacy was violated when her employer accessed her personal Facebook and Twitter accounts while she was off work after a

car accident.² The employee used her Facebook and Twitter accounts, as well as a design blog, to post and disseminate information relating to her interior design work and services. The plaintiff alleged that while she was in the hospital recuperating from the

The company
sued the employee
for misappropriation of
trade secrets, interference
with prospective economic
advantage, and
conversion.

accident, she learned that the defendants had somehow accessed her personal accounts and were authoring Facebook posts and "tweeting" from the Twitter account to promote the company. (It is not clear from the decision how the employer accessed the accounts.) Plaintiff requested that the company stop impersonating her by using her social media accounts, because it appeared to her followers that she had returned to work, but the activity continued. After plaintiff changed the passwords to her personal accounts, the owner text messaged the plaintiff, asking whether she changed her passwords and then ceased all visits and communications with her.

When the plaintiff returned to work, she alleged that she was made to feel unwelcome and that management advised her that the company was having cash flow problems because of increased insurance rates. The plaintiff chose to resign as a result of her employer's conduct and filed suit against her former employer, alleging violations of "false endorsement under the Lanham Act," claiming that her identity was so connected with a product or service that consumers were likely to be misled about her approval of the product or service as a result of the posts by the employer. The trial court denied a motion to dismiss filed by the defendants, finding that the plaintiff sufficiently alleged a claim for false endorsement because she was well-known in the design community, she created a personal following on Facebook and Twitter, and the "tweets" and Facebook postings related to her work. As of early September 2013, the case is still pending.

Eagle v. Morgan

In a lawsuit filed in July 2011 in federal court in Pennsylvania, a co-founder of a banking education company alleged that the company had used her LinkedIn account, which was established using the company email address, to connect with potential and current business acquaintances.³ The company provided both online and in-person services to the banking community. At the time the account was established, the plaintiff was the CEO, and she joined LinkedIn to connect with her clients, potential clients, and friends.

After a change in ownership, the company enacted a social media policy that required employees, including the plaintiff, to create and maintain LinkedIn accounts. Certain employees monitored the LinkedIn accounts and corrected any information that violated company policy. The defendants argued that the LinkedIn account was used for business, and company personnel developed and

maintained all of the connections on the plaintiff's account. The plaintiff's employment was involuntarily terminated in June 2011, three years after she had established the account.

After she was discharged, the plaintiff tried to access her account, but was unable to. A co-worker, who had helped her establish the account, provided the account password to management. The password had been changed so that the plaintiff could no longer access the account. In addition to changing the password, the defendants changed the name on the account (which had been the plaintiff's name) to the name of a new company executive and changed the picture to reflect the new company executive, but left the plaintiff's honors and awards, recommendations, and connections untouched. The plaintiff also alleged that the defendants were using her LinkedIn account to falsely represent that she resigned from the company and that her page caused confusion among her connections and potential connections, damage to her reputation, and loss of good will associated with her name. For example, if someone searched for the plaintiff on LinkedIn, the page would display the name and picture of the new executive but the plaintiff's honors and awards, along with personal comments from her connections, which were still visible on the page.

In her lawsuit, the plaintiff alleged numerous common law causes of action, including the unauthorized use of her name, invasion of privacy by misappropriation of identity, and conversion. The defendants argued that while company policy encouraged employees to create and maintain LinkedIn accounts, the policy also provided for company monitoring of the accounts to address any violations of company policies. In addition, the policy provided that at the end of employment, the company would request and retrieve company information related to the LinkedIn account. At the conclusion of a non-jury trial, the district court found that the plaintiff successfully proved her

claims for unauthorized use of her name, invasion of privacy by misappropriation of identity, and misappropriation of identity. The plaintiff finally regained access to her LinkedIn account after contacting LinkedIn about the dispute.

Practical realities

These cases provide insight in the potential pitfalls a company may experience when an employee promotes himself or herself individually, or markets the company

on a social media platform. The “terms and conditions of use” posted on each social media website, and agreed to by each user when an account is established, also provide guidance as to who “owns” the accounts. For example, the “Ownership and Control of Information” section of Facebook Principles states:

People should own their information. They should have the freedom to share it with anyone they want and take it with them anywhere they want, including removing it from the Facebook Service. People should have the freedom to decide with whom they will share their information, and to set privacy controls to protect those choices.⁴

The Facebook Statement of Rights and Responsibilities provides that, “you will not provide any false personal information on Facebook, or create an account for anyone other than yourself without permission” and “you will not create more than one personal account.”⁵ Because the terms of use for Facebook state that the intent of the service is that individuals have only one

account, it may not be prudent for employers to require employees to create additional accounts for company use, although employers could

certainly create a company Facebook page and ask employees to post material to that page.

The Twitter rules provide that users “may not impersonate others through the Twitter service in a manner that does or is intended to mislead, confuse, or deceive others.”⁶ The rules also note that Twitter “reserve[s]

the right to reclaim usernames on behalf of businesses or individuals that hold legal claim or trademark on those usernames. Accounts using business names and/or logos to mislead others may be permanently suspended.” Unlike Facebook or LinkedIn, Twitter does allow individuals to have multiple accounts or “handles.” LinkedIn’s user agreement appears to recognize that questions may exist as to who should maintain an account, providing that “If you are using LinkedIn on behalf of a company or other legal entity, you are nevertheless individually bound by this Agreement even if your company has a separate agreement with us.”⁷ Perhaps most importantly, the LinkedIn User Agreement specifically states that “...your account belongs to you.”

Companies may want to control the information employees post on social media relating to their employment, but in the terms of use, many of the sites suggest that the social media platforms are just that—social—and are intended for personal use, even if that personal use is for professional reasons. The original intent of social media may have been

...companies must...
consider the implications
of social media accounts
containing business
information and what
happens to that information
if and when an employee
leaves employment...

more “personal,” but the advances in technology and the inexpensive marketing platform provided by these services have resulted in businesses requesting or requiring employees to use the accounts for work-related purposes. Even when an employer has not asked an employee to establish an account, the employer may have reason to want to “capture” information on a personal account, if the owner of the account has used the social media platform to promote himself or herself professionally. Consequently, companies must be proactive and consider the implications of social media accounts containing business information and what happens to that information if and when an employee leaves employment—a result that occurs with great frequency in today’s mobile workforce.

The realities of social media

Social media provides an easy and inexpensive way for a company to connect with customers, patients, and prospects. For example, a director of Human Resources for a medical laboratory or staffing agency can connect with nurses and doctors regarding positions that are available, a nursing home can advertise facility additions and/or improvements on Facebook and Twitter, and a hospital can advertise new technology or advances in medicine via Facebook and Twitter. All types of businesses have begun to use Facebook as a way of self-promotion, sometimes giving access to pages for customers to leave feedback and comments. Social media accounts, when created by individuals, however, are generally intended to promote the particular individual. In a world where employees frequently move from position to position, employers must consider the implications of the mobility of the social media account as well as that of the employee. Especially in those situations where the employer expects employees to use social

media as a “tool” of the business, the business must consider what happens when the employee moves on to the next opportunity, either voluntarily or involuntarily. Factors which should be considered include:

- ▶ Consider a company Facebook page which employees and customers may use to promote the business.
- ▶ Ask employees to keep Facebook accounts personal by not identifying their employer.
- ▶ If Twitter is used as a marketing tool, management should ask the employee to create a separate Twitter handle identifying the company and clarifying that the handle is the property of the company, which, like all company property, must be returned at the conclusion of employment.
- ▶ Companies should consider the implications of employees “connecting” on LinkedIn, if customer information is deemed proprietary to the employer.
- ▶ Companies should create a social media policy which defines what types of company information may be posted to social media, recognizing that any such policy must comply with Section 7 of the National Labor Relations Act.

Conclusion

Although the law regarding ownership of social media accounts is still undeveloped, employers are more frequently facing situations which emphasize the importance of considering this issue in order to avoid potential embarrassment, loss of confidential or valuable information, or liability when an employee changes jobs. ☐

1. *Phonedog v Kravitz*, No. C 11-03474, 2011 WL 5415612 (N.D. Cal. Nov. 8, 2011).
2. *Maremont v. Susan Fredman Design Group*, 772 F.Supp.2d 967 (N.D. Ill. 2011).
3. *Eagle v. Morgan*, No. 11-4303, 2012 WL 4739436 (E.D. Penn. October 4, 2012).
4. Facebook: *Facebook Principles*. Available at <http://on.fb.me/18AR1t9>, (last visited July 24, 2013).
5. Facebook: *Statement of Rights and Responsibilities*. Available at <http://on.fb.me/1a5HjOw>, (last visited August 1, 2013).
6. Twitter: *The Twitter Rules*. Available at <http://bit.ly/176oQ2m>, (last visited July 24, 2013).
7. LinkedIn: *User Agreement*. Available at <http://linkd.in/1dZe1UE>, (last visited July 24, 2013).