LAW360

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

Using Social Media In The Workplace May Get Dicier

Law360, New York (April 07, 2014, 5:35 PM ET) -- Social media is playing an increasingly important role in how businesses operate as companies seek to leverage their broad reach and influence to increase brand awareness, better understand market perception and market their products or services to current and potential customers. Additionally, many companies are using it to assist in the hiring process, while others face the issue of whether — and how — to discipline employees for their work-related social media activities.

Some companies have even gone so far as to request or require their employees or prospective employees to disclose personal social media account information. This practice has been highly criticized by privacy groups and also carries certain legal risks — requesting the information is now prohibited in a number of states and using information from social media sites to make hiring decisions can implicate state and federal discrimination laws.

Companies must be careful not to run afoul of employees' statutory or common law rights when deciding whether and how to monitor employees' social media activity, and what actions they may permissibly take when they encounter activity that might warrant employee discipline.

Employers Requesting Social Media Passwords

Social media sites have been around for more than a decade now, however the practice of companies requesting social media account information from their current or prospective employees is a relatively new phenomenon, one that was highly publicized when The Associated Press ran a story about a New York statistician being asked for his Facebook password during a job interview.[1] That story, which prompted a critical response from privacy groups and the public, compelled legislators across the country to introduce legislation to ban the practice.

Within weeks of the AP story, Maryland became the first state to enact a social media privacy law prohibiting employers from requesting social media account information from current or prospective employees. Since then, 12 additional states have enacted similar laws including: Arkansas, California, Colorado, Illinois, Michigan, Nevada, New Jersey, New Mexico, Oregon, Utah, Vermont and Washington.[2] In addition, related legislation has been introduced or is pending in more than 20 other states.[3] Although each state's enacted or proposed law is unique in some respects, their general purpose is the same: to prohibit employers from requesting that their current or prospective employees disclose their private social media account information.[4]

Social media privacy issues are also being discussed in Congress. After Sens. Charles Schumer and Richard Blumenthal asked the U.S. Department of Justice and the U.S.Equal Employment Opportunity

Commission in March 2012 to investigate whether employers requesting personal social media account information violates federal law bills have been introduced in both houses to ban the practice: the Social Network Online Protection Act and the Password Protection Act of 2013.

These bills, if enacted, would, like their state counterparts, prohibit employers from requesting that their employees or prospective employees disclose personal social media account information. Although it does not appear that either bill will be enacted during the current legislative session,[5] it is reasonably foreseeable that similar legislation will be enacted in the future given the number of states adopting similar laws. Therefore, even companies that are not located in jurisdictions with enacted social media privacy laws should keep apprised of this issue.

Social Media May Implicate Discrimination or Retaliation Laws

Companies that base their hiring decisions or other employment-related actions on social media should also be aware of certain other legal risks, whether or not the company requests personal social media account information. One such risk is a potential claim that an employment decision (e.g., hiring, discipline or termination) constitutes unlawful discrimination or retaliation.

Existing federal laws, including Title VII of the Civil Rights Act of 1964, the Americans with Disabilities Act, the Age Discrimination in Employment Act and the Genetic Information Nondiscrimination Act, prohibit employers from basing employment decisions on factors such as age, race, national origin, religion, marital status and genetic information. In addition, many state laws protect additional characteristics (e.g., sexuality), provide statutory or common law privacy protection or protect legal off-duty activities.

Although there are relatively few decisions addressing employment discrimination in the social media context, recent cases suggest that courts may be receptive to such claims. In Gaskell v. University of Kentucky,[6] the plaintiff, a leading candidate for the director position at a new campus observatory, alleged that the university discriminated against him because a member of the university's search committee noted that he had published an online article about the Bible and his belief in Creationism. Although the university argued at summary judgment that its decision not to hire the plaintiff was based on valid scientific concerns, the court concluded that there was a genuine issue of material fact as to whether the committee member's opinion about the online article and the plaintiff's religious beliefs were a factor in the employment decision.

Similarly, in Neiman v. Grange Mutual Casualty Co.,[7] the court denied a motion to dismiss the plaintiff's claim that the company's decision to not hire him was age discrimination. Although the defendant argued that it lacked knowledge of the plaintiff's age because the interview was by telephone, the court held that the plaintiff's allegation that the defendant knew his age because he had posted his college graduation year on his LinkedIn profile was sufficient to state a claim at the pleading stage. The court emphasized that "[i]t is not difficult to determine that someone who graduated from college in 1989 probably was over the age of 40 in 2010. This is enough to place [the company] on notice that [the plaintiff] is subject to the protection of the laws against age discrimination."

As the foregoing decisions suggest, companies that consider social media when making employment decisions should be cognizant that protected information is often posted on social media sites and that viewing such sites may pose a risk that the company will obtain information about a protected class or protected activity. If this protected information ultimately reaches the decision-maker, either directly or indirectly, an applicant or employee may use that fact to challenge an employment decision in a

subsequent state or federal lawsuit. Consequently, the company may ultimately have to spend a significant amount of time and resources defending itself in a lawsuit that possibly could have been avoided.[8]

Social Media May Implicate the Stored Communications Act

Companies also should be aware that the unauthorized monitoring or accessing of their employees' personal social media accounts may implicate the federal Stored Communications Act, which generally prohibits intentional, unauthorized access to electronic information. Although the SCA was enacted almost 30 years ago, well before the advent of social media, courts recently have started applying the SCA to social media.

For example, in Ehling v. Monmouth-Ocean Hospital Service Corp.,[9] the plaintiff, a paramedic, alleged that her hospital employer violated the SCA by temporarily suspending her after she posted on Facebook that paramedics, who were responding to a shooting at a Holocaust museum, should have refused to treat the suspected shooter and that the responding security guards needed target practice. Although the plaintiff used Facebook's privacy settings to limit her posts to her Facebook friends, one of those friends, who also was a co-worker, took screenshots of her posts and sent them to hospital management.

The court ultimately dismissed the plaintiff's SCA claim at summary judgment. Before doing so, however, the court held that the SCA applied to the plaintiff's Facebook posts because "[t]he legislative history of the SCA suggest[ed] that Congress wanted to protect electronic communications that are configured to be private." The court emphasized that because the plaintiff's posts were electronic communications not accessible to the general public (i.e., she used Facebook's privacy settings) and Facebook is an electronic communication service that archives posts and messages, the SCA applied to the posts.

Nonetheless, this was insufficient to create a genuine issue of material fact because it was undisputed that the plaintiff's co-worker, and Facebook friend, voluntarily sent the screenshots to hospital management. Therefore, the court concluded that the hospital was an authorized recipient of the plaintiff's posts, and the SCA's "authorized user" exception applied.[10]

In Rodriguez v. Widener University,[11] the plaintiff, a student employee, alleged that his university employer violated the SCA by suspending him for a Facebook post containing images of weapons. The university moved to dismiss the complaint arguing that it received the post from one of the plaintiff's Facebook friends. However, the court denied the motion because there were no allegations in the complaint that the plaintiff's Facebook profile lacked privacy settings, that his posts were available to the general public or that a Facebook friend provided the university with the post. Consequently, there was insufficient information at the pleading stage to dismiss the plaintiff's SCA claim for failure to state a claim.

As the foregoing cases suggest, it appears that courts may apply the SCA to social media posts. Although viewing social media content that is publicly available is not likely to run afoul of the SCA, companies should be careful not to access employees' private social media accounts without authorization.

For example, although the Ehling court concluded that the hospital's conduct was not actionable because it fell within the SCA's "authorized user" exception, the result may have been different had the hospital solicited the posts or previously demanded access to the plaintiff's account.[12]

Social Media May Implicate the National Labor Relations Act

Finally, companies should be aware that basing employment decisions on employee social media activity, or enacting social media policies governing employee social media use, may implicate the federal National Labor Relations Act.[13] Since August 2011, when then National Labor Relations Board General Counsel Lafe Solomon issued the first of three reports discussing employee social media use and the NLRA,[14] the NLRB has proactively applied the NLRA to cases involving social media.

For example, in Butler Medical Transport LLC,[15] two former employees filed charges with the NLRB after being terminated for making Facebook posts implicating their employment. The first employee posted on a former co-worker's Facebook wall that he should "think about getting a lawyer and taking [Butler Medical] to court" and "contact the labor board too." The second employee, during his shift, posted disparaging and vulgar remarks about his employer concerning the condition of his work vehicle. In reviewing the terminations, an NLRB administrative law judge concluded that the first employee's posts were protected under the NLRA, but upheld the second employee's termination because his post was maliciously untrue.

Although Butler Medical argued that the first employee's posts were not protected, because they were accessible to the company's customers and other third parties, the administrative law judge cited long-standing NLRB precedent that employee conduct does not lose NLRA protection merely because it may have an adverse effect on the company's business. According to the judge, the posts were protected because they were a response to a former employee's post about being fired for commenting to a patient about the condition of the company's ambulances, and the condition of company vehicles was a matter of mutual concern.

With regard to the second employee, the administrative law judge concluded that the posts were not protected because they were maliciously untrue. Not only did company maintenance records show that the ambulance had not broken down when the second employee made his post, the employee later testified at an unemployment insurance hearing that his post referred to a private vehicle. Therefore, because the employee made the posts with knowledge they were false, the posts were not protected under the NLRA.

Finally, the administrative law judge concluded that the company's social media policy, under which the first employee was terminated, was also unlawfully overbroad. The policy, which included a promise by employees to "refrain from using social networking [sites] which could discredit Butler Medical Transport or damage[] its image," violated the NLRA because the employees would reasonably construe its language to prohibit protection Section 7 activity. Moreover, the judge emphasized there was no evidence that the company had effectively communicated a narrowed interpretation of the policy to its employees. Therefore, because the policy had been applied to restrict the Section 7 rights of the first employee, it was unlawful.

As Butler Medical demonstrates, along with other recent NLRB social media decisions, companies should be mindful that employment decisions that are based on social media activity may implicate the NLRA. Not only does the NLRB currently have several social media cases pending,[16] but the board's chairman recently emphasized that "the social media cases have been very helpful in terms of raising the public's awareness of the NLRB."[17] Therefore, companies should stay apprised of the NLRB's social media decisions to better understand when employee social media activity will be protected concerted activity.

Conclusion

The scope of law governing social media is constantly evolving. Given how strong the reaction among some state legislators has been to social media privacy concerns, along iwth recent judicial decisions involving employment discrimination, SCA claims based on social media activity and the NLRB's recent focus on social media, this is a rapidly developing area to which companies should pay close attention.

—By Marcia E. Goodman, Lori A. Zahalka and Richard E. Nowak, Mayer Brown LLP

Marcia Goodman is a partner in Mayer Brown's Chicago office.

Lori Zahalka and Richard Nowak are associates in Mayer Brown's Chicago office.

The opinions expressed are those of the author(s) 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.

[1] See Shannon McFarland, Job Seekers Getting Askedfor Facebook Passwords, USA Today, Mar. 21, 2012, http://www.usatoday.com/tech/news/story/2012-03- 20/job-applicants-facebook/53665606/1.

[2] Wisconsin will likely be the 14th state to ban employers from requesting social media account information because its social media privacy bill is currently awaiting Governor Scott Walker's anticipated signature.

[3] For a list of the states with enacted and pending litigation, see National Conference of State Legislatures, Employer Access to Social Media Usernames and Passwords, http://www.ncsl.org/research/telecommunication s -and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014.

[4] The only exception is New Mexico's social media privacy law, which does not expressly prohibit employers from requesting social media information from their current employees. The law (S.B. 371) provides that "[i]t is unlawful for an employer to request or require a prospective employee to provide a password in order to gain access to the prospective employee's account or profile on a social networking web site or to demand access in any manner to a prospective employee's account or profile on a social networking web site."

[5] For updated information on pending US legislation, see GovTrack, http://www.govtrack.us.

[6] 2010 WL 4867630 (E.D. Ky. Nov. 23, 2010).

[7] 2012 WL 5029875 (C.D. Ill. Apr. 26, 2012).

[8] For example, although the defendant in Neiman ultimately prevailed at summary judgment, it took more than two years of litigation to resolve the matter. See Case Opinion, No. 11-cv-3404 (C.D. Ill. Apr. 2, 2013), available at http://www.ilcd.uscourts.gov/sites/ilcd/files/opinions/Ni eman-sj%202%20opn.pdf.

[9] 2013 WL 4436539 (D.N.J. Aug. 20, 2013).

[10] The SCA's "authorized user" exception applies when: (i) access to the electronic communication was "authorized," (ii) "by a user of that service," (iii) "with respect to a communication ... intended for that user." See 18 U.S.C. § 2701(c)(2).

[11] 2013 WL 3009736 (E.D. Pa. June 17, 2013).

[12] See Pietrylo v. Hillstone Rest. Grp., 2009 WL 3128420, at *3 (D.N.J. Sept. 25, 2009) (describing how the "authorized user" exception does not apply if the "purported 'authorization' was coerced or provided under pressure").

[13] The NLRA, which governs most private sector employers, prohibits certain unfair labor practices and protects the rights of employees to engage in certain types of activities. Specifically, Section 7 provides that employees have the right "to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection," and Section 8(a)(1) prohibits employers from interfering with, restraining, or coercing employees in the exercise of their Section 7 rights.

[14] All three social reports are publicly available through the NLRB's website at: http://www.nlrb.gov/news-outreach/news-story/acting-general-counsel-releases-report-employer-social-media-policies.

[15] Nos. 5-CA-97810, 5-CA-94981, 5-CA-97854; Sept. 4, 2013.

[16] For example, the issue in Triple Play Sports Bar, No. 34- CA-012915, is whether simply "liking" a co-workers Facebook post is protected concerted activity under the NLRA.

[17] See Abigail Rubenstein, NLRB Chairman Lays Out Approach to Social Media Cases, Law360, Jan. 21, 2014, http://www.law360.com/articles/502701/nlrb-chairman¬lays-out-approach-to-social-media-cases.

All Content © 2003-2014, Portfolio Media, Inc.