Bloomberg BNA

BNA's
Health Law Reporter™

Employers Beware: Requiring Applicants or Employees to Provide Social Networking Passwords or Access to Private Accounts May Violate the Law

By Catherine T. Barbieri

Researching candidates through social media, and monitoring employees' online comments, have become routine practices for many companies. However, when health-care organizations and other employers require their applicants or employees to divulge their social networking usernames or passwords, or to ''friend'' them on social media sites, they may be violating the law.

It is now customary for most employers to use social media to screen their applicants. A recent survey conducted for CareerBuilder.com as of 2015 found that, 52 percent of hiring managers use search engines to research candidates, up from 43 percent in 2014 and 39 percent in 2013.

While many employers are looking for information that supports the candidate's qualifications for the job, an applicant's social media presence also can tell a potential employer a lot about that person, including whether they have any personal views or practices that may be contrary to the organization's mission or code of conduct. It should come as no surprise to anyone applying for a job that potential employers will be scouring their publicly accessible social media accounts for any disqualifying posts, blogs or tweets.

Catherine T. Barbieri is a partner in Fox Rothschild LLP's Philadelphia office. She is a member of the firm's Partnership Advancement Committee, representing corporations in high level, employment-related litigation in both state and federal courts nationwide. She can be reached at cbarbieri@foxrothschild.com.

Some employers continue to monitor social media accounts after an individual is hired. They do this for a variety of reasons, most notably to protect trade secrets and other proprietary information, and to ensure that their employees are complying with the company's policies, including any non-harassment policies. Many companies in the financial services sector are required by statute to monitor certain employees' correspondence with customers or prospective customers.

While some employers limit their review of social media accounts to whatever is publicly available, others take it a step further and require that applicants or current employees provide their passwords and usernames so that the company may access their private social networking accounts. Some employers will actively initiate a relationship with an applicant or employee on social media to gain access to their otherwise private account.

The same CareerBuilder survey found that 35 percent of employers who screen via social networks have requested to ''friend'' or follow candidates who have private accounts, and of that group 80 percent say that they have been granted permission.

Legislative Responses

State lawmakers have taken issue with these practices, citing employee privacy concerns. Increasingly, states are enacting legislation that would ban the practice of employers requesting the social media usernames and passwords of their applicants or current employees.

In 2012, Maryland became the first state in the nation to prohibit employers from requesting or requiring that an employee or job applicant disclose their user name and password to access a social networking account. In 2015, similar legislation was introduced or considered in at least 23 states, and 9 states enacted similar laws.

Connecticut adopted a law that bars employers or potential employers both from requesting or requiring employees or potential employees to provide passwords or usernames to their personal online accounts as a condition of employment, or inviting the employer or potential employer to join their personal online account network.

 ISSN 1064-2137

Currently, 22 states have laws that ban some or all of the social media research practices discussed in this article.

Another practice that recently has gained some attention is ''shoulder surfing,'' in which an employer has an employee access their social media account while management watches. The ACLU publicly criticized the Virginia State Police for requiring applicants to sign on to their Facebook and Twitter accounts so that job interviewers could read their private communications, although the Virginia password protection law that went into effect as of July 1, 2015 does not ban the practice.

A number of other states, including California and New Jersey, have banned shoulder surfing. Some states, including Colorado, also bar the practice of asking applicants or employees to change their privacy settings in a manner that would permit an employer to access their personal online account.

Congress has considered similar, federal legislation. The Social Networking Online Protection Act—which was introduced in 2013 and would have prohibited employers from requesting, or discriminating against an applicant or employee who refused to provide, a username or password—died in Congress. The Password Protection Act of 2013, which would have amended the federal criminal code to subject a fine on any employer that engaged in the same conduct, also stalled in Congress.

Best Practices for Social Media Monitoring

Given this rapidly changing area of the law, employers that are currently requiring applicants or employees to provide their social networking passwords, or to invite the employer to their online account network, must ensure that those practices do not violate the laws in the states in which their employees are working.

Companies operating on a national or international level should assume that some or all of their employees are protected by password protection or other social media privacy laws.

To ensure that their recruiting or social media monitoring efforts do not violate any laws, employers should strongly consider the following measures:

1. Employers should preclude their managers and external search firms from requesting or requiring applicants or employees to provide their social networking usernames or passwords, to permit access to social media sites through shoulder surfing, to change their privacy settings to permit the employer to access their social media accounts, or to ''friend'' managers on their sites.

Employers may still view publicly available information on applicants' or employees' social networking sites, and co-workers generally may still friend each other in social media, without running afoul of the law.

2. To reduce the potential risks to employers associated with their review of even publicly available blogs, posts or tweets, employers should conduct any review of applicants' social media sites only after an initial interview.

What employers may learn about an applicant online—such as their race or ethnic background, medical history, religious or political affiliations or marital status—could give rise to a discrimination complaint if the individual is not hired. Employers would be prudent to limit online research to those candidates who are otherwise qualified, performed well in an interview and are likely to receive an offer.

There are any number of reasons why information learned in reviewing social media information may disqualify the applicant from employment, including when there is evidence of bragging about illegal activity, a propensity for violence or racist or other inappropriate remarks.

If an employer determines that the information learned about the applicant through social media research, and not some other reason, is the basis for denying or revoking an offer of employment, it needs to document its findings and how the disqualifying comments violate a company policy or principle.

3. Likewise, if information about harassing or other inappropriate posts or tweets by an employee is brought to the employer's attention, it needs to document how that information was received. Most often, other employees who are friends or followers of the offending employee will have access to their account and provide a copy of the comments in question to the employer.

Employers should resist the urge to obtain direct access to the offending employee's private posts through online access offered by another employee.

4. Consistent with point three above, while a number of the state password protection and social media privacy laws provide exceptions that would permit requests for usernames or passwords in connection with certain investigations, this issue needs to be reviewed carefully with legal counsel before any such exception is invoked.

5. Employers should ensure that any adverse action taken against an applicant as a result of social media research by a consumer reporting agency complies in all respects with the Fair Credit Reporting Act.

6. Any monitoring of employee's social media sites should go no further than necessary to protect the employer's business interests or to comply with any statutes that may require it. It should be conducted only by trained individuals who are aware of the limits of permissible monitoring, including any local or state laws that may apply.

7. Every employer should have a social media policy that prohibits the use of any social media to harass or bully co-workers, or to leak trade secrets or other proprietary or confidential company information. Remind employees that the company's confidentiality and nonharassment policies extend to their use of social media.

Conclusion

Social media research and monitoring permit health care organizations and other employers to hire effectively, protect their proprietary information, and enforce their policies concerning workplace conduct.

In this rapidly evolving area, employers need to ensure that their use of social media for these purposes does not run afoul of the law.

  HLR ISSN 1064-2137