Bloomberg BNA

Daily Labor Report®

SOCIAL MEDIA

In response to the growing popularity of social media websites, some employers have started demanding access to employees' and applicants' private social media accounts, Sheppard Mullin attorneys Eric Raphan and Sean Kirby say in this BNA Insights article.

They discuss the new law in Maryland banning such practices, as well as pending state and federal legislation. Raphan and Kirby also recommend considerations employers should take into account before engaging in such a practice and steps that employers should take to ensure compliance with applicable laws.

Access Denied: Employers Should Avoid Seeking Access to Social Media Accounts

BY ERIC RAPHAN AND SEAN KIRBY

The social media revolution has continued to grow in light of the ever-increasing popularity of social media websites such as Facebook, Twitter, and LinkedIn. As a result, a number of employers have implemented the practice of demanding that employees and prospective employees provide employers with access to their private social media accounts.

While obtaining such access may seem like a reasonable way for employers to determine whether current and prospective employees are complying with office policies, are being productive at work, and will be positive contributors to the employer on a going-forward basis, a growing number of states, as well as the federal government, have proposed legislation to ban such practices.

Given the quickly developing legal landscape on this issue, and the potential liability that exists for failing to comply with this new wave of legislation, there are certain steps that employers should take to ensure compliance with applicable laws. In addition, even if an employer conducts business in a state where employers remain permitted to demand access to private social media accounts, there are a number of considerations an employer should take into account before engaging in such a practice.

Eric Raphan is a partner and Sean Kirby is an associate in Sheppard Mullin's Labor and Employment practice group, based in the firm's New York office.

Maryland Department of Public Safety and Correctional Services

This issue recently gained national attention when Robert Collins, a former corrections officer at the Maryland Department of Public Safety and Correctional Services, challenged the MDPSCS's demand that he provide it with access to his private Facebook account. MDPSCS attempted to justify its demand by reasoning that it needed to check the Facebook pages of its corrections officers in order to ensure that they were not engaging in any gang-related activity. Mr. Collins contacted the American Civil Liberties Union and ACLU agreed to represent him.

ACLU alleged that the MDPSCS's conduct violated Section 2701 of the Stored Communications Act, the First and 14th amendments of the U.S. Constitution and constituted an invasion of Mr. Collins's privacy. Shortly thereafter, the MDPSCS agreed to cease demanding access to social media accounts. While ACLU believed that it had a variety of grounds upon which to challenge the MDPSCS's practices, Maryland did not have a specific law that clearly addressed this issue.

As a result of the attention that Mr. Collins's case received, the Maryland Legislature moved quickly and, in May 2012, enacted Maryland Labor and Employment Code § 3-712, which became the first law in the United States to expressly prohibit employers from requesting

 ISSN 0418-2693

or requiring the disclosure of usernames or passwords to personal social media accounts (85 DLR A-12, 5/2/12). In addition to banning the practice, the statute also prohibits employers from taking, or threatening to take, any disciplinary action against employees or applicants who refuse to disclose such information.

Other States Follow Maryland's Lead

Following Maryland's swift action, a number of states have decided to follow Maryland's lead.

In Illinois, Gov. Pat Quinn (D) is expected to sign legislation that would amend the Illinois Right to Privacy in the Workplace Act (104 DLR A-3, 5/30/12). This legislation would bar employers from requesting or requiring any employee or prospective employee to provide their passwords or related social media account information to the employer. The legislation would also block an employer's attempt to avoid the no-password prohibition by also making it illegal for employers to require employees and prospective employees to display portions of their social networking profiles for the employer's review.

In New York, Sens. Liz Krueger (D-Manhattan) and Mark Grisanti (R-Buffalo) have introduced a bill to amend the New York Labor Law to protect the privacy of employees' and prospective employees' social media accounts. The bill in its current form would prohibit employers from: (1) requiring an employee or applicant to disclose any log-in name, password, or other means for accessing a personal social media account; and (2) penalizing an employee or refusing to hire an applicant because the individual refuses to disclose such information. If an employer is alleged to have violated this provision, the bill provides that the state attorney general may apply for injunctive relief against the employer and for civil penalties. The bill further provides that the aggrieved individual may commence an action against the employer for equitable relief and damages.

Similarly, the state of California is considering a bill introduced by Sen. Leland Yee (D-San Francisco) titled the Social Media Privacy Act. The SMPA would prohibit employers and postsecondary educational institutions from requiring an employee, student, or prospective employee or student to disclose his/her social media account username and password. The bill also would provide that employers and educational institutions cannot retaliate against individuals who refuse to provide such information.

In addition to Illinois, New York, and California, a number of states, including Michigan, Minnesota, New Jersey, and Washington, are all in various stages of pursuing their own versions of laws that, in one way or another, would prohibit employers from requesting access to the social media accounts of their current or prospective employees.

Some of the bills contemplate providing protections to the employer by: (1) allowing the employer to recover costs and attorneys' fees if the employee's/applicant's suit is deemed frivolous; (2) carving out an exception where the employee is accused of harassing a co-worker or divulging the employer's trade secrets; or (3) clarifying that an employer has no affirmative duty to investigate social media sites when deciding whether to hire an applicant.

Federal Government's Response

Not to be outdone by the states, the federal government has also taken a number of steps toward making it illegal for employers to demand access to private social media accounts.

To begin, Sens. Richard Blumenthal (D-Conn.) and Charles Schumer (D-N.Y.) have requested that the Department of Justice and the Equal Employment Opportunity Commission launch a federal investigation into these practices (58 DLR A-10, 3/26/12).

In addition, on April 27, Reps. Jan Schakowsky (D-Ill.) and Eliot Engel (D-N.Y.), introduced the Social Networking Online Protection Act, which would prohibit employers from requiring current or prospective employees to provide their username or password to access online content (85 DLR A-10, 5/2/12).

Similarly, on May 9, Blumenthal and Sen. Martin Heinrich (D-N.M.) introduced the Password Protection Act of 2012 (90 DLR A-6, 5/9/12). As with the Social Networking Online Protection Act, the intent of the Password Protection Act of 2012 is to prevent employers from forcing current or prospective employees to share information from their personal social networking accounts.

Compliance With These Laws

With numerous states and the federal government moving quickly to enact legislation to prohibit an employer's access to private social media accounts, it is important that employers begin taking steps now to revise its hiring practices in order to ensure compliance with these laws.

First, since all of the foregoing statutes prohibit employers from requesting access to the social media accounts of current and prospective employees, employers need to take the necessary steps to ensure that their employees understand these limitations. To accomplish this, it is best to circulate revised interviewing and management guidelines that remind human resources representatives, supervisors, and managers not to request an employee's password or otherwise seek access to an employee's social media account.

Second, employers should review their employee handbooks and policies to ensure that their social media policies are consistent with the new legislation. To the extent necessary, these policies should be updated to make it clear to employees that they will not be requested to provide management with access to their social media accounts. However, well-drafted handbooks and policies are of limited use without properly training human resources representatives, supervisors, and managers on how to apply them. Thus, employers should ensure that these individuals understand what information they can ask of current and prospective employees and what information is prohibited.

Third, when interviewing prospective employees, employers should avoid asking questions about that prospective employee's use of social media, what sites they frequent, and what accounts they maintain. By avoiding this line of questioning, the employer can protect itself against claims that the employer used this information to make a determination regarding whether to discipline a current employee or hire a prospective employee.

  DLR ISSN 0418-2693

Finally, if an employer is inclined to use the internet to investigate current and prospective employees, it must do so in a manner that is consistent with the law. This means that employers must ensure that their human resources representatives, supervisors, and managers limit such searches to publicly available user information to the extent such searches are permissible under applicable laws. These human resources representatives, supervisors, and managers should also be reminded that they cannot fraudulently gain access to users' profiles by, among other things, pretending to be somebody else in order to gain access to someone's social media account.

Protecting Your Business Even if Your State Permits Demanding Access to Social Media Accounts

For those employers that do business in a state that does not yet prohibit employers from seeking social media account access (and assuming federal legislation is not enacted), there are still a number of issues for employers to consider if they decide to demand access to social media accounts.

Indeed, viewing an employee or applicant's private social media account may subject the employer to legal action that it would not otherwise be subjected to. Consider the employer that views a social media account and learns information about the employee or applicant that the employer did not previously know about such employee or applicant.

For example, assume that the employer learns from the social media account that the employee or applicant is ''90 days sober'' or is married to a member of the same sex and then takes an adverse action against such employee or applicant for an unrelated reason. By viewing the employee or applicant's social media account, the employer has subjected itself to a discrimination claim that it would not otherwise have been subjected to. The employer can no longer argue as a defense to the claim that it was unaware of the employee or applicant's protected characteristic. Moreover, the temporal proximity between the time that the employer viewed the social media account and the date upon which the employer took the adverse action could create an inference that the employee or applicant was subjected to the adverse action because of his or her protected characteristic.

Likewise, maintaining a policy requiring employees to provide access to their social media accounts can create issues with respect to the consistent enforcement of such policy. With the vast array of comments, photos, and other messages that individuals place on their social media accounts, an employer could quickly find itself having difficulty deciding what content ''crosses the line'' and what content may be considered to be in bad taste, but not worthy of discipline. Inconsistent enforcement of this policy could create additional liability for the employer.

Moreover, viewing an employee or applicant's social media account may create a duty to act that the employer would not otherwise have. Consider the employer that views an employee or applicant's social media account and sees that the individual has posted a message on his/her own page stating ''having a bad day and looking to take it out on someone.'' That employer may now be obligated to act to ensure that the employee does not arrive at work and injure a co-worker. Moreover, the employer that fails to act may be liable if the employee does, in fact, come to work and injure a co-worker.

Finally, employers that monitor the social media accounts of its employees may be deemed to be in violation of its employees' Section 7 rights under the National Labor Relations Act. Pursuant to Section 7, employees are protected from being disciplined for engaging in protected concerted activity. However, by monitoring the content of employee social media accounts, an employer could be perceived as chilling an employee's Section 7 rights to discuss working conditions with other employees via social media.

Given the potential liability that can arise from requiring employees and applicants to provide an employer with access to their social media accounts, employers in states that do not regulate such practices should still consider forgoing this practice and making use of other lawful alternatives. For instance, an employer can monitor the activity of its employees on company-owned computers and email systems provided that the employer makes it clear to the employees that they have no expectation of privacy when using such systems. As for applicants, instead of asking for social media account access, employers should consider conducting standard background checks of applicants that include obtaining any information that is publicly available without the use of a password.