Lesser-Known Social Media Legislation

by Robert T. Quackenboss

A wave of social media privacy legislation is rushing through state legislatures from Maine to California. To date, 10 states have enacted laws protecting social media passwords of employees and applicants, 30 similar bills are pending in state legislatures, and two have been introduced at the federal level. Lawyers, employers and the media have focused principally on two central aspects of most bills: prohibitions on employers requesting social media passwords from employees and applicants, and related non-retaliation provisions.

But the legislation contains several lesser-known privacy provisions representing additional pitfalls and nuances that should guide employers as they continue to navigate social media challenges.

Shoulder Surfing

While every piece of state legislation on social media prevents employers from asking employees or applicants for their social media usernames and passwords, 11 bills also contain provisions that prohibit employers from requiring employees or applicants to access their personal social media in the presence of the employer. This practice, known as "shoulder surfing," allows the employer to view the content that an employee or applicant has posted on Facebook or other social media without having to ask for a username or password.

Although "shoulder surfing" might seem less intrusive than asking for a social media password, employers should be wary, as four states—California, Illinois, Oregon and Washington—have already made this practice illegal. Further, California and Washington do not allow an employer to even request that an employee or applicant access social media in the employer's presence.

Mandatory Friending

A less intrusive means of monitoring employees' activities on social media is to require employees or applicants to add their employer or supervisor to their social media contact list. If an employer or supervisor is included on an employee's contact list, they can view content that the employee posts to the social media network. Requesting a password or "shoulder surfing" would then be unnecessary—the employer or supervisor could simply log on to the social network site with their own account and view everything an employee posted, including pictures, comments and complaints about work.

However, 10 state bills ban requiring employees or applicants to connect with either an employer or a supervisor on social media networks. This practice has already been outlawed in Arkansas, Colorado, Oregon and Washington.

In Arkansas, the law prohibits even requesting or suggesting that an employee or applicant "friend" an employer or supervisor. In Colorado, Oregon and Washington, a request that an employee "friend" an employer is permitted, as long as the employee or applicant is not coerced or otherwise required to do so. Oregon's and Washington's laws are broader in whom they cover—in Oregon, employees and applicants also cannot be forced to friend employment agencies, and in Washington, they cannot be forced to add any person to their friend list. This creates special challenges with professional networking applications such as LinkedIn, where colleagues might naturally expect to connect with one another despite a hierarchical differential between manager and employee.

Social Media Privacy Settings

Six bills contain provisions that prohibit employers from requiring, requesting

To date, 10 states have enacted laws protecting social media passwords of employees and applicants, 30 similar bills are pending in state legislatures, and two have been introduced at the federal level.

or even suggesting that an employee or applicant change the privacy settings on his or her social media network. For example, on Twitter, everything that a user posts is automatically viewable by the public. On Facebook, however, a user can select the privacy settings for much of the content they post, making it viewable by the public, by friends only, by friends of friends, or by only a specific group of friends. If the content is made public, then anyone with access to the Internet can view it, even people who do not have a Facebook account.

The prohibition against this practice is a broad one, and employers in Arkansas, Colorado and Washington—the three states that have enacted this provision into law—should understand the details of these restrictions in managing workplace social media matters.

Employee Misconduct Investigations

Almost half of the proposed bills and six of the 10 enacted state laws contain exceptions to allow an employer to investigate allegations that an employee's activity on a social media network violates the employer's policies against employee misconduct.

In most of the legislation, including enacted laws in California, Oregon, Utah and Washington, the employer can demand that the employee share the specific social media content that is at issue, but the employer cannot request the employee's login information. In some bills, however, and in the laws enacted in Arkansas and Michigan, the employer can demand the employee's social media username and password, but only for the purpose of conducting an investigation into the specific allegations of work-related misconduct.

Enforcement Mechanisms

It is important that employers be aware of the enforcement mechanisms in these bills, as they vary widely from state to state. Half of the bills provide for either civil enforcement of the statute, a private right of action, or both. Four states—Colorado, Michigan, Utah and Washington—have enacted enforcement mechanisms into law.

In Colorado, a violation can result in a fine of up to $1,000 for the first offense, and up to $5,000 for each subsequent offense. Michigan's law makes a violation of the act a misdemeanor with a fine of up to $1,000, and provides for a private cause of action by an employee or applicant against an employer who violates the act. In a Michigan private lawsuit, a plaintiff can recover up to $1,000 in damages, plus reasonable attorney fees and costs. Utah also provides for a private cause of action, but damages are limited to $500.

Washington, on the other hand, provides for a private cause of action that allows a plaintiff to recover reasonable attorney fees and costs and places no limit on the amount of damages he or she can recover. A prevailing defendant in Washington can also recover attorney fees and reasonable expenses, but only if the judge finds that the lawsuit was frivolous. Four other states—Georgia, Nebraska, Ohio and Rhode Island—have pending legislation that also places no limit on the amount of damages a successful plaintiff can recover.

The proposed federal bill H.R. 537, the Social Networking Online Protection Act (SNOPA), imposes civil damages of up to $10,000, and also provides for equitable relief that includes requiring an employer who violated the act to employ, reinstate or promote an applicant or employee who was not hired, was fired or was not promoted because of information obtained in violation of the act.

Proposed legislation in Maine contains a provision for similar equitable reinstatement relief, and provides that a plaintiff can recover damages of $1,000, court costs, reasonable attorney fees and three times any lost wages. Most other states with pending enforcement provisions limit any penalty or damages to $1,000 or less, except Pennsylvania and Connecticut, which provide for penalties of up to $5,000 and $10,000, respectively.

Balancing Privacy Rights

Social media privacy protections appear destined for uniform enactment in all 50 states. Employers must continue to balance their business interests with employees' privacy rights as they manage their workforce. They must also be aware of the guidelines at both the local and federal levels, potential penalties and the important exceptions that can aid employers in cases of misconduct. ■

***Robert T. Quackenboss** is a partner in the labor and employment practice at Hunton & Williams LLP. He counsels and speaks frequently on the development of social media programs and their compliance with privacy and labor laws.*

RISK MANAGEMENT
Reprinted with permission from *Risk Management*, October 2013 issue, pages 10-11.