New Jersey Law Journal

VOL. 213 - NO 2 JULY 8, 2013 ESTABLISHED 1878

IN PRACTICE

EMPLOYMENT LAW

Finding a Happy Medium: A Revised Employee Social-Media Privacy Bill

This new version may strike the right balance between worker and employer rights

By Caroline Keller and Carlos Lopez

On May 20, by a unanimous vote of 74-0, the New Jersey General Assembly approved a new version of an employee social-media privacy bill, incorporating revisions suggested by Gov. Chris Christie when he conditionally vetoed the bill on May 6. The bill is expected to receive similar support this summer in the Senate, where the earlier version passed 28-0, as well as support from Christie.

Like its predecessor, the revised bill prohibits employers from requiring employees and candidates to disclose user names, passwords or other login information for accessing their social-media accounts like Facebook or Twitter, a protection that cannot be waived by private agreement between an employer and an employee or candidate.

Keller and Lopez are labor and employment attorneys in the New York office of Seyfarth Shaw LLP.

The revised bill also prohibits employers from retaliating or discriminating against any employee or candidate who refuses to provide login information for his or her social-media accounts. A similar law signed by Christie late last year already restricts the ability of colleges and universities in the state to require applicants and students to disclose their social-media accounts and passwords.

Critics of the original bill, including Christie, argued that it went too far in the name of employee privacy and would force employers to sacrifice important and perfectly legitimate business interests. The revised bill attempts to strike a more careful balance between employee privacy concerns and the needs of employers to hire appropriate personnel, manage their operations, and protect their proprietary information.

Gone is a controversial provision of the original bill that would have prohibited employers even from asking an employee or candidate if he or she has any social-media accounts, which Christie recommended be removed because it "paint[ed] with too broad a brush." The governor pointed out that the provision would have prohibited an employer interviewing a candidate for a marketing job from inquiring as to the candidate's use of social networking so as to gauge his or her technology skills and media savvy.

Perhaps the most significant revision in the new bill is the elimination of a private right of action for employees and candidates to bring civil suits seeking money damages, injunctive relief and attorney fees against employers for alleged violations. The concern about this provision — raised during a hearing on the Senate version of the bill in September 2012 — was that it would cause employers to spend a considerable amount of time and money to defend themselves against frivolous lawsuits. The revised bill limits enforcement of the law solely to the N.J. Commissioner of Labor and Workforce Development, which may impose a civil penalty of up to $1,000 for the first violation and up to $2,500 for each subsequent violation.

In addition to scaling back some of the prior bill's more onerous aspects, the revised bill provides for specific employer rights in connection with their employees' social-media use. It redefines a "personal account" as one that is used by an employee or candidate *exclusively* for personal communications unrelated to any business purposes of the employer. Accordingly, if an account is used by an employee for the business purposes of his or her employer, then it is not personal, and therefore not subject to the privacy protections of the bill. Employers may also continue to implement policies pertaining to the use of company-issued electronic devices or social-media accounts used by employees for business purposes. The bill also

specifically allows employers to conduct investigations to ensure compliance with applicable laws or regulations, or prohibitions against workplace misconduct, on the basis of specific information learned about activity on a personal account by an employee. In the same vein, employers may continue to investigate specific allegations that an employee is transferring proprietary information or financial data to a personal account. Finally, employers may continue to view and act on information pertaining to an employee that is available in the public domain.

At present, claims under common-law invasion of privacy and under the federal and state Stored Communications Acts are the only recourse for employees or job applicants with concerns of employers overreaching on their social-media accounts. For example, where an employer was found to have coerced an employee to turn over the password to an invitation-only MySpace chat group, designed by another group of employees to air grievances against the employer, and purposefully accessed the group without proper authorization, the employer was deemed to have violated the federal and state Stored Communications Acts. *See Pietrylo v. Hillstone Rest. Group d/b/a Houston's*, 2009 WL 3128420, at *1 (D.N.J. Sept. 25, 2009). In contrast, the New Jersey Wiretapping and Electronic Surveillance Control Act has been found to protect only those electronic communications "in the course of transmission or are backup to that course of transmission," and thus would not cover post-transmission access, such as Facebook postings. *See Ehling v. Monmouth-Ocean Hosp. Servs. Corp.*, 872 F. Supp. 2d 369, 372 (D.N.J. 2012). Common-law right-of-privacy claims may cover such instances, but it is clear that, without the weight of a social-media law, electronic privacy determinations are still made on a case-by-case basis. The New Jersey Supreme Court has recognized a reasonable expectation of privacy in personal emails, even when these personal email accounts are accessed on company computers. *See Stengart v. Loving Care Agency*, 201 N.J. 300 (N.J. 2010).

Should New Jersey enact a social-media privacy law, it would be the eighth state in the nation to do so, though more than 20 states are currently considering their own social-media privacy laws. Like New Jersey, on June 6, the New Hampshire State Senate voted to ban employers from requiring employees or job applicants to disclose a user name or password to personal social-media or email accounts. The bill, however, does not prevent employers from enforcing workplace policies about company equipment, from obtaining employee or applicant information already in the public domain, or prevent the employer from investigating whether the employee is complying with securities or financial laws based on the person's personal website used for business purposes. The Rhode Island House of Representatives approved a similar measure the following day, barring employers from requiring access to personal social-media accounts from workers, job applicants, students or prospective students.

Also pending is federal legislation, the Social Networking Online Protection Act (SNOPA), H.R. 537, which was reintroduced in February by Reps. Eliot Engel (D-N.Y.), Janice Schakowsky (D-Ill.) and Michael Grimm (R-N.Y.). Under SNOPA, the Secretary of Labor could impose a fine of up to $10,000 against employers that unlawfully request social-media user names, passwords or other login credentials from employees or job applicants, or for retaliating against employees or applicants who refuse to provide such information, and/or seek injunctive relief in federal court. As of now, SNOPA encompasses social networks like Twitter, MySpace and Facebook, but, unlike most state social-media privacy laws, it also protects email accounts. These same constraints would also apply to schools from kindergarten through university level, preventing schools from obtaining such information about students and prospective students during the application process.

When SNOPA was originally introduced in April 2012, no state had yet limited employer or personal access to personal social-media accounts. The issue gained national attention when the ACLU, on behalf of Robert Collins, a former corrections officer at the Maryland Division of Corrections, challenged the division's blanket requirement that applicants for employment with the division, as well as current employees undergoing recertification, provide the government with their social-media account usernames and personal passwords for use in employee background checks. During his recertification interview Collins was asked for, and turned over, his Facebook username and password, and sat waiting while the interviewer reviewed his Facebook account, given the justification that this information was necessary for the division to ensure that those employed as corrections officers were not engaged in illegal activity or affiliated with any gangs. Although the division agreed to discontinue this practice, Collins' story served as the springboard for Maryland becoming the first state to enact a social-media privacy law, expressly prohibiting employers from requesting or requiring the disclosure of usernames or passwords to personal social-media accounts, in May 2012.■