MILLER CANFIELD

Hey Employers: Employee Social Media Passwords are (Mostly) None of Your Business (Not that You've Been Inquiring)

May 16, 2013

"Likes," "tweets," "hashtags," and "wall posts" are all words that have quickly entered our lexicon through the continuing explosion of growth that is social media. By breaking down communication barriers and encouraging interactions amongst each other – often publicly, instantly, and permanently – social media has dramatically changed how humans interact with each other, including within the workplace.

For the most part, employee use of social media has not required a fundamental rewriting of federal and state labor and employment laws. Employers may continue regulating employee use of social media as long as they do so within the traditional parameters of the law. It's the regulation at the edges, however, that has made it more difficult for employers.

One of those "edges" is the extent to which employers may require applicants or employees to disclose login credentials for electronic accounts, including social media accounts. A few well-reported incidents in the past couple of years garnered significant attention from the media, privacy advocates, and state and federal legislators.

In 2011, the Maryland Department of Public Safety and Correctional Services suspended its practice of requiring applicants to provide social media login and password information, instead modifying it to require applicants to log into their accounts and let an interviewer watch while the potential employee clicks through wall posts, friends, photos and anything else that might be found behind the privacy wall. Similarly, a Michigan teacher's aide was suspended in 2012 after failing to provide her school district with access to her Facebook account after a parent complained about a picture on her Facebook page.

Opponents of such practices assert that they are illegal under the Stored Communications Act, constitute an unlawful invasion of privacy and, for public employees, are a violation of constitutional privacy rights. Moreover, Facebook's official position is that requiring the login and password disclosure could not only "potentially expose[] the employer who seeks ... access to unanticipated legal liability," it also "violat[es] Facebook's Statement of Rights and Responsibilities to share or solicit a Facebook password."

Late last year, Michigan joined seven other states in enacting legislation governing such conduct. Effective December 28, 2012, Michigan's Internet Privacy Protection Act (IPPA) prohibits employers from requesting that an employee or applicant grant access to, allow observation of, or disclose information that allows access to or observation of "personal internet accounts," such as Gmail, Facebook and Twitter. Violators of the IPAA are guilty of a misdemeanor punishable by a fine of not more than $1,000. Individuals may bring a civil action to enjoin the violation and may recover not more than $1,000 in damages plus reasonable attorney fees and court costs. The IPPA also regulates educational institutions from engaging in similar conduct towards prospective or current students.

Under the IPPA, an employer may not discharge, discipline, fail to hire, or otherwise penalize an employee or applicant declining such requests. In contrast to other states, however, the IPPA contains several exceptions when an employer can request such information, including:

- Accessing devices paid for, in whole or in part, by the employer, as well as monitoring, reviewing or accessing data that is either on such devices or travels through or stored on an employer's network;

Continued

- Accessing an employer's account;
- Investigating, disciplining or discharging an employee for transferring certain employer information – proprietary or confidential information or financial data – without the employer's authorization;
- Conducting an investigation for the purpose of ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct;
- Restricting or prohibiting an employee's access to certain websites while using an electronic communications device paid for, in whole or in part, by the employer or while using an employer's network or resources, in accordance with state and federal law;
- Complying with a duty to screen employees or applicants prior to hiring or to monitor or retain employee communications that is established under federal law or by a self-regulatory organization as defined in the Securities and Exchange Act of 1934; and
- Viewing, accessing, or utilizing information about an employee or applicant that can be obtained without any required access information or that is available in the public domain.

In addition to these exceptions, the IPPA expressly provides that employers do not have a duty to search or monitor the activity of a personal internet account and are not liable for failing to request or require that an employee or applicant grant access to, allow observation of, or disclose information that allows access to or observation of their personal internet account. Finally, an employer can plead as an affirmative defense to an IPPA action that it acted to comply with requirements of a federal law or a law of this state.

Critics of these "Facebook Password" laws argue that the laws are a solution in search of a problem, asserting that with the exception of a few widely reported incidents, employers do not engage in such conduct. A SilkRoad study from late 2012 seemingly validates this argument, finding that 97 percent of employers do not request social media password from employees or applicants. Nonetheless, regulating such conduct has seemingly struck a legislative nerve across the country – at least 23 other states and Congress are considering similar legislation. In short, stay tuned.