ROBERTS
CARROLL
FELDSTEIN
& PEIRCE
ATTORNEYS AT LAW RCFP.COM

# Employer Access To Employee Social Media: Just Don't Ask

**By:**

JAMES A. MUSGRAVE, ESQ.

In March, Senator Richard Blumenthal (D-Conn) announced that he would be introducing a bill that would bar employers from requesting Facebook or email passwords from employees or job applicants. In April, Maryland became the first state in the country to pass such a bill. The Maryland law, which passed unanimously in the Senate, 49-0, and by a huge margin in the House, 129-8, bans employers from:

> requesting or requiring that an employee or applicant disclose any user name, password, or other means for accessing a personal account or service through specified electronic communications devices.

Maryland was thrust into the role of trailblazer in large part because the issue of access to Facebook accounts came to the forefront following news reports that the Maryland Department of Corrections had demanded the Facebook passwords of correctional officers who were being re-certified. In other words, the Department was not merely interested in viewing the publically available information its employees had posted on Facebook. Instead, the Department wanted access to posts, comments and pictures which were private – at least in the sense that the user had chosen only to allow friends or family to be able to view them.

Similar bills have been introduced in Illinois and California, and have been discussed in Massachusetts and New Jersey. According to Kelly Sheridan and Elizabeth Suever of our Government Relations Practice, legislation regulating employer demands for access to social media accounts and passwords has not been introduced in Rhode Island. Though, given the clear appeal to legislators, as evidenced by the one sided votes in Maryland, it would not be a surprise if legislation is introduced in the General Assembly in short order.

Even in the absence of an absolute prohibition, employers should be circumspect in demanding access to employee or applicant social media accounts for several reasons. First and foremost, it may well be bad for business.

The public is strongly opposed to these demands, viewing them as unwarranted invasions of privacy - a view shared by courts. When litigants have demanded access to their opponents' Facebook accounts, courts have refused to allow what they deem "digital fishing expeditions." See, e.g., *Caraballo v. City of NY*, Index No. 75535/08 (N.Y. Sup. Ct.; Mar. 4, 2011). Given the strong public sentiment against such demands, the news media have covered the issue of password demands extensively and deemed it a "trend" even though the practice is far from widespread. Therefore, if you decide to ask your employees for their passwords, you might well find Channel 10 at the door and your company the subject of an unwanted news story.

Second, while there is not (yet) a federal or Rhode Island statute which specifically bars an employer from demanding access to an employee's social media accounts, there are a number of laws that could be in play depending on the circumstances. Chief among them is the National Labor Relations Act or the NLRA.

The NLRA protects the right of employees to form a union. That's all well and good, you say, but my employees are not unionized, so I have nothing to fear. Not quite. The NLRA not only regulates the relationship between unions, union members and employers, it also protects employees who engage in "other concerted activities for the purpose of collective bargaining or other mutual aid or protection."



ROBERTS, CARROLL, FELDSTEIN & PEIRCE INCORPORATED
Ten Weybosset Street | Providence, RI 02903-2808 | Phone 401.521.7000 | Fax 401.521.1328
Member: Legal Netlink Alliance • An International Alliance of Independent Law Firms

Generally speaking, "protected concerted activity" occurs when two or more employees act together to improve their terms and conditions of employment. Therefore, if an employee posts on Facebook expressing displeasure with her work environment, and she has "friended" co-workers, her comments could constitute protected concerted activity. Taking disciplinary action against an employee who has engaged in protected concerted activity would violate the NLRA. Similarly, an attempt by an employer to obtain Facebook passwords of employees who use Facebook to communicate about work, could be construed as a form of surveillance. Employer surveillance of "protected concerted activity" outside of the workplace is an unfair labor practice.

In addition to the NLRA, employers should be wary of the Stored Communications Act, which makes it illegal to access electronically stored communications without authorization. Conditioning a job offer or continued employment on handing over a password could be viewed as coercive and akin to access without authorization.

Finally, Rhode Island has created a cause of action for violations of an individual's right to privacy. Among other things, that law gives Rhode Islanders "the right to be secure from unreasonable publicity given to one's private life." An employer that gained access to an employee's private Facebook account could face liability if a supervisor or manager shared some salacious bit of information he/she gleaned from the account. Likewise, the privacy statute creates liability for "an invasion of something that is entitled to be private or would be expected to be private and the invasion was or is offensive or objectionable to a reasonable man…" See R.I.G.L. 9-1-28.

Return to:
IN THE
NEWS





ROBERTS, CARROLL, FELDSTEIN & PEIRCE INCORPORATED
Ten Weybosset Street | Providence, RI 02903-2808 | Phone 401.521.7000 | Fax 401.521.1328
Member: Legal Netlink Alliance • An International Alliance of Independent Law Firms