



## Social Media Passwords and Employees: What Business Owners Need to Know

By Tracy Leahy  
April 18, 2013

The use of social media for both personal and business use has led some employers to demand Facebook passwords from employees and job applicants. On Dec. 28, 2012, Michigan became the fourth state to implement legislation prohibiting this practice. California, Maryland, and Illinois also prohibit access to password protected social media accounts.

### **What is the Michigan Internet Privacy Protection Act?**

Michigan's Internet Privacy Protection Act prohibits an employer or school from requiring an employee, student or applicant, to provide password or login information to social media and other Internet accounts. The law also prohibits an employer or school from retaliating against (disciplining, discharging or refusing to hire) an employee or student who refuses to provide this information.



### **Why protect social media passwords?**

The legislation was enacted to protect employees and job applicants from having to decide whether to compromise their personal privacy for their job. The legislation followed the widely publicized but relatively rare practice of a handful of employers, including the Maryland Department of Public Safety and the city of Bozeman, Mont., who demanded Facebook passwords from job applicants and current employees.

### **Employees aren't completely off the hook**

Michigan's law does not protect anything in the public domain. If an employee's Facebook settings are not set to private, that information is fair game. In addition, the law allows employer's to investigate social media use in the following situations: 1) Where the employer pays for the device; 2) Where the internet account is provided to the employee for a business purpose; 3) Where the employee transfers the employer's confidential, proprietary or financial data without the employer's authorization; and 4) To ensure compliance with applicable laws and work rules.

### **[SYSTEM-AD-RIGHT]What happens to companies violating the law?**

A person who violates the Act is guilty of a misdemeanor punishable by a fine of not more than \$1,000, plus reasonable attorney fees and costs. A person who believes the Act has been violated must make a written demand for money damages and provide documentation of the violation at least 60-days before a lawsuit it filed.

### **Use of social media in hiring**

Vetting candidates for employment based on public social media postings is legal but problematic, and should be done with caution. Social media postings may be inaccurate, difficult to evaluate or generate a false reason not to hire an individual. In addition, social media postings may reveal that an applicant is a member of a legally protected class (e.g., provide information regarding the applicant's age, race, disability, or national origin). Employers should balance the reliability, accuracy and utility of the discovered information with the risk that it will reveal

protected information. Companies should establish policies detailing when social media sites will be reviewed, who will conduct the search, what information will be searched, and how the information will be evaluated. A firewall should be created to protect hiring managers from the search results. Human Resources departments should maintain records of social media searches that were conducted during the hiring process to protect against failure to hire claims based on an applicant's protected status.

*Tracy Leahy is a Senior Attorney at Clark Hill PLC. Tracy represents businesses in litigation alleging discrimination, retaliation, and violations of the FMLA, the ADA and the FLSA. Leahy also provides advice to employers concerning general labor and employment issues. She can be contacted at [tleahy@clarkhill.com](mailto:tleahy@clarkhill.com).*