

# Asking Prospective Employees for Social Media Credentials

May 2012

By Steven W. Sufas and Mary Cate Gordon

---

## Does Curiosity Kill the Cat?

A recent trend in the human resources community is to ask prospective employees for usernames and passwords to social media sites in order to allow the hiring employer access to otherwise private information about the candidate's "online identity." A prospective employee's social media site can provide a wealth of information both quickly and cheaply, including how they spend their free time, with whom they associate, and their professional and personal interests. Generally, users protect information like this from the general public with privacy settings, but employers can quickly bypass this privacy wall by merely demanding access. In doing so, however, employers may inadvertently expose themselves to liability under existing laws.

This article addresses legal concerns in accessing a prospective employee's social media information.

## Protected Class or Medical Information

Social media sites can provide information that an employer normally is prohibited from soliciting or relying upon during the hiring process (age, religion, disability, race, etc.). Learning about this type of information could subject an employer to violations of federal and state anti-discrimination statutes, either for gathering improper data during the application process for a refusal to hire allegedly based on protected characteristics.

## Off-Duty Conduct

Employers relying on social media searches may come across photos, videos or comments of applicants engaging in activities that may be construed as "unbecoming," but which are not unlawful. Several states, including California, Colorado and New York, have laws prohibiting employers from making employment decisions or discriminating against employees based on what is otherwise lawful off-duty conduct.

## Section 7 Rights

The National Labor Relations Act (NLRA) protects employee conduct that constitutes concerted activity for mutual aid or benefit, even where the issues do not even involve unionization. Social media sites often contain such protected speech, like information or complaints about working conditions, co-workers or compensation. The National Labor Relations Board's (NLRB) acting general counsel has made the application of Section 7 rights in the context of social media a high enforcement priority for the agency.

## Criminal Records

Many states have laws limiting the use of arrest and conviction records in employment decisions. The Equal Employment Opportunity Commission (EEOC) likewise takes the position that such inquiries can have an unlawful disparate impact on minorities and thus cannot be considered unless the information is job related and consistent with business necessity.

## Privacy

While job applicants have no reasonable expectation of privacy in publicly disseminated information (even Facebook says so), accessing information that would otherwise remain private could violate the applicant's common law rights.

Additionally, litigation has already begun against employers that have improperly utilized social media credentials. For example, a federal court in New Jersey recently upheld a jury verdict holding an employer liable for violations of the federal Stored Communications Act (SCA), 18 U.S.C 121, <http://bit.ly/HaphsC>, and New Jersey's parallel electronic surveillance statute (N.J. Stat. §2A:156A-3), where an employer representative twice requested and then utilized an employee's login credentials for a MySpace account. The manager who requested this information had learned that the site was maintained by employees who were critical of management. After the manager accessed the site, the employees involved were later terminated. The jury found that the employer coerced the employees into turning over the access information and therefore violated the laws in question. *See, Pietrylo v. Hillstone Restaurant Group d/b/a Houston's*, No. 06-5754 (Dist. Ct., D. NJ 2009), <http://bit.ly/JpxUZs>. Note that this conduct is also a likely unfair labor practice under the NLRA.

## Proposed Legislative Action

Because this trend in seeking prospective employees' passwords has gained both popularity and notoriety, both federal and state lawmakers have reacted by proposing measures that seek to ban the practice.

On March 21, 2012, Sen. Richard Blumenthal (D-CT) announced that he is drafting a bill to outlaw employers from asking prospective employees to turn over Facebook login credentials. Romm, Tony, "Dem: Facebook Passwords Off-Limits," *Politico*, (Mar. 21, 2012), available at [www.politico.com](http://www.politico.com). Blumenthal told the press that he believes such coercive inquiries are an "unreasonable invasion of privacy" and should be prohibited like other unreasonable employment practices, such as polygraph tests. U.S. Representatives Ed Perlmutter (D-CO) and Patrick McHenry (R-NC) have announced that they are working on similar legislation.

Just a few days later, on March 25, 2012, Blumenthal (along with Sen. Charles Schumer (D-NY)) released a statement asking the EEOC and the Department of Justice to launch a federal investigation to determine whether employer demands for social media credentials violate federal law. *See, "Blumenthal, Schumer: Employer Demands for Facebook and Email Passwords as a Precondition for Job Interviews May Be a Violation of Federal Law; Senators Ask Feds to Investigate," Richard Blumenthal, United States Senator for Connecticut* (Mar. 25, 2012), available at <http://blumenthal.senate.gov/>. Blumenthal cited privacy concerns and employer exposure to discrimination claims as the basis for this investigation.

In addition to federal action, several states are in the process of drafting and considering bills that would prohibit employers from asking for social media credentials from prospective employees. Maryland is the first state to pass such a law. On April 9, 2012, the "User Name and Password Privacy Protection" Act passed the Maryland legislature, officially banning employers from asking employees and job applicants for their social media site passwords (*see*, H.B. 964, <http://bit.ly/IIUvWq>). *See also, "Maryland Introduces Bills to Protect Students' Social Media Privacy Rights,"* in the March 2012 issue of *Internet Law & Strategy*, <http://bit.ly/Ihfbdy>. California's "Employer Use of Social Media Act," currently in committee, seeks greater regulation of social media use by employers, including regulation of employers seeking login credentials (*see*, AB 1844, <http://1.usa.gov/IIVqWF>). Illinois' "Right to Privacy in the Workplace Act" is being revised in committee to prohibit requesting social media login information (*see*, 820 ILCS 55/, <http://1.usa.gov/IhdHAD>). Washington's proposed "Facebook Bill," introduced on April 6, would likewise bar companies from demanding passwords or other account information in order to access social media sites (*see*, SB 6637, <http://1.usa.gov/IYzRpn>). New Jersey lawmakers have announced an intention to introduce a similar bill when the Legislature resumes its regular session this month. The bill sponsor has been quoted as saying that asking for the login credentials of prospective employees is akin to asking someone to turn over the keys to their house.

Facebook itself has commented on the issue, announcing that "[i]n recent months, we've seen a distressing increase in reports of employers or others seeking to gain inappropriate access to people's Facebook profiles or private information. This practice undermines the privacy expectations and security of both the user and the user's friends.

It also potentially exposes the employer who seeks this access to unanticipated legal liability." Egan, Erin, "Protecting Your Passwords and Your Privacy," *Official Facebook Blog* (Mar. 23, 2012), <http://on.fb.me/lhfwna>. Facebook goes on to opine that users should "never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account ...." The blog post also warns of potential employer liability in accessing information through an employee's (or prospective employee's) social media profile. The Facebook Statement of Rights and Responsibilities ([www.facebook.com/legal/terms](http://www.facebook.com/legal/terms)) specifically forbids sharing passwords and letting others access a private account.

## Suggestions for Employers

There is certainly a temptation to utilize applicant or employee social media content. But before jumping in, employers should carefully evaluate their specific needs for accessing social media in the hiring process. If an employer's current hiring practices are working, it may be unnecessary to embark on a program of social media access. However, if an employer has an identifiable business justification or has difficulty securing desired information from prospective employees, social media access may be useful. For example, employers may need to investigate whether an employee or applicant has been divulging trade secrets, violating the terms of restrictive covenants or engaging in unlawful harassment of co-workers on social media sites.

Notwithstanding the potential risks, if employers still want to pursue access to an applicant's social media information, they should consider designating an individual who is not involved in the hiring decision to review social media content and filter out any protected information from the process. Third-party services also are available to conduct such screening, but the Federal Trade Commission recently issued a closing letter cautioning that such companies are subject to the Fair Credit Reporting Act (*see*, <http://1.usa.gov/lhfPI4>).

In short, before undertaking a broad foray into social media monitoring, employers should be cautious to carefully define what they want to accomplish and whether social media investigations will achieve those goals, while keeping a close watch on state and federal legislative efforts to assure legal compliance.

---

**Steven W. Suflas** is the managing partner of Ballard Spahr's Cherry Hill, NJ, office and a member of the firm's Labor & Employment and Appellate groups. He can be reached at [suflas@ballardspahr.com](mailto:suflas@ballardspahr.com). **Mary Cate Gordon** is an associate in Ballard Spahr's Litigation Department and a member of the firm's Health Care and the Labor & Employment groups. She can be reached at [gordonmc@ballardspahr.com](mailto:gordonmc@ballardspahr.com).