

Employers Cautioned Against Asking Applicants and Employees for Password Access to Personal Social Media Accounts

Article By:

David L. Woodard

Employers are increasingly asking (or requiring) applicants or employees to provide their Facebook password or other social media account log-in credentials so the employer can review non-publicly available content for anything troubling. Variations on this request are “shoulder surfing,” when an applicant or employee is asked to log in to his or her social media account during an interview or in a manager’s presence to permit review of the account’s contents without directly disclosing log-in credentials, or having an applicant “friend” a hiring manager to enable access to a Facebook account.

Although many states and Congress are still considering whether or not to prohibit such practices, employers should seek advice from legal counsel before asking or requiring an applicant or employee to provide log-in credentials or other means for accessing his or her personal social media account. These practices pose significant risks for employers and, in some situations, are illegal.

Various state and federal privacy laws, including the **federal Stored Communications Act**, make it unlawful to obtain unauthorized access to an individual’s stored electronic communications, including postings on a personal social media account. Requesting or requiring password access to a personal social media account may be viewed as “unauthorized access.” For example, in a case involving a national restaurant chain, a jury found the company liable for obtaining unauthorized access to an employee’s personal online communications on a restricted MySpace group website in violation of the Stored Communications Act when a company manager accessed those communications after the employee’s co-worker gave the manager her log-in credentials to the website and later testified she felt pressured to do so.

Recently, Maryland became the first state in the nation to pass a law prohibiting employers from asking or requiring employees or applicants to provide a user name, password, or other means for accessing their personal online accounts, including social media accounts, email accounts, bank accounts, and other personal accounts accessed through computers or other electronic communication devices. Maryland’s new law, expected to be signed soon by its governor, also prohibits employers from discharging, disciplining, or otherwise penalizing an employee, or rejecting an applicant, for refusing to provide such information. For balance, the Maryland law includes several exceptions and provisions for the benefit of employers, such as cases where an employee is

using a personal online account for business purposes or where an employer is investigating suspected unauthorized downloading of company proprietary information to a personal online account.

Employers also may realize additional unanticipated legal risk from requesting or requiring password access to an employee's or applicant's personal social media account. For example, an employer could expose itself to litigation risks if review of an applicant's or employee's personal online account revealed otherwise unknown information about his or her age, race, ethnic origin, religion, or disability and the individual is subsequently not hired, discharged or disciplined. If review of an applicant's or employee's personal social media account reveals he or she is engaging in a lawfully protected activity, the employer may face a claim of unlawful retaliation if the individual is later rejected for a job or subjected to an adverse employment action. As an example, an employee's online complaints to coworkers as Facebook "friends" may amount to "protected concerted activity" under the National Labor Relations Act if the complaints are about wages, terms of employment, or working conditions.

The risks of possible claims and litigation from an employer's efforts to access an applicant's or employee's personal social media account, as well the impact such efforts can have on recruitment and employee relations, may lead many employers to consider safer alternatives, such as conducting lawful background checks and limiting their monitoring of employee communications to those occurring on company-owned computers and company email systems pursuant to a lawful policy.

Federal Appeals Court Temporarily Enjoins NLRB From Implementing Rule to Post Workplace Notice of NLRA Rights

We informed you in a [recent alert](#) that a District of Columbia federal court upheld the National Labor Relations Board's rule requiring employers to post a workplace notice of employee rights under the National Labor Relations Act. Since that alert, in a separate lawsuit, a South Carolina federal court invalidated the posting rule. Soon thereafter, in an appeal of the aforementioned District of Columbia ruling, a federal court of appeals enjoined the NLRB from implementing the posting rule. In response to these rulings, the NLRB has postponed implementation of the posting rule. Based on this development, employers are not required to post the workplace notice of NLRA rights by April 30. We will keep you informed of further developments.

© 2025 Poyner Spruill LLP. All rights reserved.

National Law Review, Volume II, Number 135

Source URL: <https://natlawreview.com/article/employers-cautioned-against-asking-applicants-and-employees-password-access-to-personal-social-media-accounts>