TIMELY COVERAGE OF HUMAN RESOURCE ISSUES

HUMAN RESOURCES eLINE

August 7, 2014 – Vol. 13, No. 8

TOP 3 REASONS NOT TO "CREEP" ON CANDIDATES' OR EMPLOYEES' PERSONAL SOCIAL NETWORKING WEBSITES

An increasing number of Americans are using social networking websites. Pew Research Center has stated that as of January 2014, 74% of online adults use at least one social networking website, like Facebook (1.28 billion active users), Twitter (225 million active users) or Instagram (150 million active users).

As a result, many employers are wondering if they should be concerned with what candidates and employees are posting on these sites. Should employers require access to these sites as a condition of employment?

While to some this dilemma may seem far-fetched, many employers are arguing that access to these personal accounts is needed to:

- Protect trade secrets or proprietary information from being disseminated online
- Investigate workplace issues such as harassment or threats of violence
- Ensure they are using all available means to screen candidates

This article will discuss the top three legal and practical reasons why employers should not try to go snooping, now referred to as "creeping" onto a candidate's or employee's personal social networking website (SNW) — or at a minimum why employers should exercise extreme caution before doing so. We will also discuss a few best practices for employers to be aware of when workplace issues and investigations involve SNW posts.

Reason 1: State law may prohibit creeping

Since May 2012, when Maryland passed the first password-protection law prohibiting employers from requiring candidates or employees to disclose their usernames or passwords to personal SNW accounts, 15 other states (including Wisconsin and Illinois) have **passed** similar laws. Password-protection legislation is **pending** in at least 17 other states (including Minnesota) and similar federal legislation is also being contemplated.[1]

Password-protection laws have been sweeping through state legislatures due to a few isolated, albeit egregious, cases. In the seminal Maryland case, which led to the first password-protection law, a Maryland correctional facility was concerned it needed to view candidates' SNW to ensure there was no evidence of gang affiliations, which is apparently a valid hiring concern for correctional facilities. Outraged at what appeared to some to be a blatant violation of privacy and potential problem if this practice became widespread, various other states followed suit passing similar password-protection laws.

Unfortunately, however, no two password-protection laws are the same. The laws range widely in what is and is not protected (e.g., prohibiting mandating disclosure of passwords or prohibiting even "shoulder surfing"), as

[1] www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx

well as fines, penalties and remedies. Violations are a misdemeanor in some states and remedies may consist of back wages, attorney fees and other costs.

Some, **but not all**, state laws carve out specific exceptions for employers to monitor SNW use where the employee is using employer-provided equipment or other electronic devices (cell phones or tablets). These nuances between the different state laws has created a legal labyrinth, which can make it very difficult for employers — especially multi-state employers — to attempt to create uniform policies and procedures for not only proper candidate screening, but also workplace monitoring and managing workplace investigations.

In April 2014, **Wisconsin** became the 13th state to pass its own password-protection law, known as Wisconsin Social Media Protection Act ("Act").[2] The law applies to public and private employers, as well as educational institutions and landlords. However, for purposes of this article we will focus only on the law's impact on employers.

The Act prohibits employers from "requesting or requiring" candidates and employees to provide "access information" for their "personal internet account" or "to otherwise grant access to or allow observation of that account." Additionally, employers are prohibited from retaliating in any way against individuals who exercise their rights under the law.

- **Access information** is defined as "a username and password or any other security information that protects access to a personal internet account." Access information does not include an employee's personal email address, so employers remain free to request this from both candidates and employees.
- **Personal internet account** is defined as "an internet-based account that is created and used by an individual exclusively for purposes of personal communication." Arguably, this could prohibit employers from accessing not only personal SNW accounts, but also personal email accounts–provided those accounts are used exclusively for purposes of personal and not professional communication.

Although the Act establishes broad protections for candidates and employees, there are some limited opportunities or exceptions for employers to gain access to accounts. For instance, employers have a right to access "electronic communications devices supplied or paid for in whole or in part by the employer," as well as accounts or services provided, controlled or directed by the employer (such as social media accounts employees set up in connection with their jobs).

Employers may also require employees to grant access or allow observation of their personal internet accounts. **However, employers may not require employees to turn over their passwords or usernames.** The purpose for accessing employee internet accounts would be to view information as part of an investigation into confidentiality breaches, potential violations of the law or general employee misconduct. Employers would need reasonable cause to believe the accounts may contain information that could substantiate the concerns.

Nothing in the Act prohibits employers from:

- Restricting access to SNW or employees' personal email accounts on employer-provided equipment
- Complying with a duty to screen applicants prior to hiring or to retain employee communications that is

[2] https://docs.legis.wisconsin.gov/2013/related/acts/208 see also, http://legis.wisconsin.gov/assembly/republicans/columns/Pages/bies-social-media.aspx

established under state or federal laws, or regulations or rules of a self-regulatory organization
- Viewing information that is publically available online (with caution)

The Act also does not apply to an employee's personal internet account or an electronic communication device of an employee engaged in providing financial services who uses the account or device to conduct business if the employer is subject to the "content, supervision and retention requirements imposed by federal securities laws and regulations" (e.g. FINRA).[3]

Reason 2: Creeping on information publically available may pose unforeseen risks

The majority of password-protection laws permit employers to view information publically available online, when individuals fail to properly secure their online privacy settings.

This should not be seen as a carte blanche invitation to employers to start creeping on publically available SNW information. As we and many other experts have warned, SNW often reveals protected class status such as age, race, religion, military status, disability and sexual orientation, to name a few — all of which can legally have no bearing on hiring or employment decisions.[4]

Rather, employers need to evaluate the industries they are in, the positions they are hiring for, as well as their corporate culture prior to venturing down the creeping path. Most notably, employers should remember that long before SNW, great employees were hired by using good old-fashioned techniques such as well-crafted interview questions, assessment tools and approved background and reference checking practices.

Reason 3: Creeping on SNW can run afoul of the NLRA

The NLRA (the National Labor Relations Act) applies to union and non-union employers and prohibits an employer from having policies or practices that interfere with an employee's right to engage in "concerted activity."

This provision allows employees to come together and discuss the terms and conditions of their employment. To this end, employers need to be aware that their practices of creeping on an employee's SNW may pose risks if employers find something online they disagree with and then take action against the employee for the online post.

For example, the employer might observe the employee complaining about the employer's safety, pay or other practices. Or, more commonly, the employer might view employees' posts complaining about their managers.

Although the posts may not be private or may be brought forward by another colleague who is an online acquaintance of the complaining employee, employers now more than ever need to recognize the risks posed with taking any type of adverse action based on these posts.[5]

The National Labor Relations Board (NLRB), which enforces the NLRA, has been on a mission to heavily scrutinize employers who have policies or practices that attempt to control or limit what employees can and cannot post online about their employers. Therefore, we encourage employers to seek the advice of outside counsel when they become aware of SNW posts that may cause them pause or appear to violate a company policy or regulation.

---

[3] http://www.finra.org/

[4] http://www.associatedfinancialgroup.com/Data/eLineNewsletters/HumanResources/Vol8/No7jul09/hrartjul09.asp

[5] http://www.associatedfinancialgroup.com/Data/eLineNewsletters/HumanResources/Vol10/No6jul11/hrartjul11.asp

If you are an HR Hotline client, we recommend you contact us prior to taking any adverse action against an employee for their online posts.

A multitude of factors can determine whether an employer may take adverse action against the posting employee, including:

- How the employer became aware of the post
- What the post contained
- What, if any, policy or law may have been violated

You can see how the labyrinth continues to twist and turn. For more information on the NLRB's recent stance on SNW boundaries between employees and employers visit the NLRB's website.

Contact us at info@AssociatedFinancialGroup.com or 800-258-3190.

Associated

Associated Financial Group