

Reprinted with permission

From the Tampa Bay Business Journal:

<http://www.bizjournals.com/tampabay/print-edition/2011/07/01/employers-take-risks-when-asking-for.html>

## Guest Column

# Employers take risks when asking for access to social media sites

Premium content from Tampa Bay Business Journal - by Cathleen Bell Bremmer

Date: Friday, July 1, 2011, 6:00am EDT

### Related:

[Technology](#), [Human Resources](#)

We are a Google, **Facebook** and Twitter generation. Social media platforms such as blogs, social networking sites and video sharing — fueled by the instant access of smart phones and related personal devices — have gained in popularity and are used in one form or another by this generation of workers both current and prospective.

Social media has no boundaries and does not discriminate on the basis of race, sex, age, religion, socio-economic status or any other protected category. It allows a freedom of expression and speech unrivaled by other media forms.

Although not immune from abuse, the lure of this new world is too hard for many to resist. It is no wonder that employers and employees alike are posting to and viewing social media sites regularly.

There is no question that social networking can impact the employment arena from applications through the hiring and ongoing employment relationship.

### **Out-of-bounds monitoring**

The existence of Internet policies is not new as some have been in place since the dawn of email. As social media usage has exploded, employer monitoring of employee Internet usage has gained momentum.

Now some employers are taking monitoring to a new level by asking applicants for logins and passwords so that as prospective employers they can access the candidates' "private" lives as part of the hiring process.

Is this risky? Yes. And employers that do this increase their chances for a lawsuit.

Googling or accessing a candidate's private social media site enables the employer to learn unnecessary — and potentially unlawful — hiring information. Once this information is learned, it can not be "unlearned."

Federal, state and local laws prohibit employers from discriminating against job applicants and employees because of their race, religion, gender, national origin, age, disability and other protected classifications. These laws preclude employers from asking applicants certain topics during the employment application process and often well after hiring (e.g. disability status, marital status, religion, age, pregnancy status).

For example, assume an applicant with a particular religious belief is rejected based purely on something lacking in their qualifications. It is easy to defend a religious discrimination lawsuit brought by the applicant if the hiring manager(s) never asked the prohibited questions and had no idea of the applicant's religious affiliation.

Change the scenario. Assume instead that the hiring manager does not ask the prohibited question directly but gains access to the applicant's personal social media site and learns that he holds beliefs contrary to the manager's beliefs. Even if the applicant's religion had nothing to do with the hiring rejection, the employer loses any chance of saying that the decision makers did not know of the religious background, a prohibited inquiry that the manager has now accessed through the social media site.

### **Impact of current law**

Employers face other challenges with respect to accessing applicant or employee social media sites. Depending on the employer, the employee or applicant's constitutional privacy rights could be implicated.

The Fair Credit Reporting Act often applies during the employment background check process. If the third party conducting background checks uses information learned off of a site that impacts an applicant's ability to obtain employment, there will be employer liability if the act's procedures are not followed.

The Stored Communications Act also prohibits unauthorized access to password-protected websites. The law is undeveloped as to whether employer policies that make disclosure of private, password protected websites a condition of employment is considered "authorized" access under that act.

With the rise of social media usage and employer access to private sites, employers that don't have a social media policy in place should carefully consider establishing one.

Such policies should notify employees that the employer will monitor both company and personal site viewing and should give examples of prohibited conduct both within the company and outside. Employers should educate their employees about the policies and fairly enforce standards set.

Requiring employees or applicants to provide private sites and passwords, however, may have legal consequences that even a well-written policy may not protect.

Cathleen Bell Bremmer is a board-certified labor and employment lawyer in the Tampa office of Carlton Fields PA. Bremmer can be reached at [cbell@carltonfields.com](mailto:cbell@carltonfields.com) or 813.229-4326.