Employers Using Social Media to Monitor Employees: Risks and Liability

Tuesday, March 30, 2010

According to a Career Builder survey in 2009, forty-five percent of employers use social media sites like Facebook, MySpace, Twitter, and LinkedIn to screen job applicants. Some applicants include a blog address or something of the sort on a resume, but even if such information is not supplied, it is easy enough for employers and human resource personnel to unearth a prospective employee’s online footprint. This can be both beneficial and detrimental for the applicant. On one hand, a personal blog devoted to a subject related to the job one is applying for (say, a hopeful-human resources director’s personal blog about employment law issues and developments) can make the applicant more desirable. On the other, an applicant’s uploaded pictures of a booze-filled tropical getaway hardly reinforce the image of a consummate professional.

Last year alone, two percent of employers said in this survey that polled managers and human resources personnel that they terminated workers for content posted on these social media sites, and one percent of workers were terminated due to videos they posted on media sharing sites like YouTube.

An employee’s problems regarding the discovery of social media outlets are many and well-publicized, but employers are also on dangerous ground when seeking to screen possible applicants using these technologically oriented methods. While it is true that employers can often be held liable for what their employees do and say online (e.g., defamation, improper disclosure of confidential or protected information, violation of FTC guidelines for blogging, etc.), employers do not enjoy immunity from the law when they scour Facebook, LinkedIn, Twitter, or hosted blog servers for applicants. In fact, the likelihood of employers running afoul of anti-discrimination and privacy laws when they take a peek at pictures or tweets or recent blog posts is troubling.

Violation of Privacy

The first concern when it comes to employers pulling up Facebook accounts and Twitter feeds and personal blogs is for the prospective employees’ privacy. Intrusion upon a party’s seclusion or solitude is a tort, and it is not difficult to imagine how such a cause of action might arise in the instance of an employer poking around online and digging up information on an employee or prospective employee.

In order to prevail on the facts, an employee must allege an intentional intrusion (physical or otherwise) on his or her solitude or seclusion or private affairs or concerns, which would be highly offensive to the reasonably prudent person. An employer can defend on the grounds that the employee did not have a reasonable expectation of privacy.

Though simply conducting a web search for a prospective applicant’s name and web presence certainly doesn’t meet the high standard for invasion of privacy, it is nonetheless an issue that an employer needs to be aware of.
Discrimination: Religion, Ethnicity, Political Activism, Gender, Protected Activity

Discrimination in the workplace takes many forms. An employer risks liability early on in the search to fill an open position by discriminating between potential hires based on things like the applicants’ religion, ethnicity, political affiliations and activism, sexual orientation, gender, and even activities that are protected under the National Labor Relations Act.

An employer’s examination of an employee’s or potential hire’s social network sites may provide the basis for claims under employment discrimination statutes if the employer used such methods of off-resume information-seeking to seek out information about the employee that was legally protected in some way. The problem escalates further if the employer takes some adverse action against the employee or potential hire within a short time after learning of the subject matter of the protected status or activity. Indeed, the employee or prospective employee may use that adverse action or treatment as circumstantial evidence of employment discrimination or retaliation.

Several examples spring to mind. One of the first things employers look for upon successfully locating a prospective employee’s Facebook page are pictures. Facebook allows its users to upload a large number of pictures from cameras and hard drives and arrange them into albums that are displayed fairly conspicuously on the user’s profile page. From these pictures, as well as the default “Profile Picture” that is displayed with every user’s name (unless privacy settings are modified) and on every user’s main page, an applicant’s race or ethnicity is immediately apparent. Facebook also has an information input field for religious affiliation, and many users include that as part of their profile.

Religious and ethnic discrimination is a pressing concern, particularly in a post-9/11 world climate. Arab and Muslim citizens nationwide suffered from the stigma suddenly attached to their ethnicity and religious convictions, a stigma which carried into the job market. Several lawsuits were filed in which the plaintiffs prevailed in showing that they were denied entrance into organizations or were terminated or suffered from adverse actions early in the hiring process due to their ethnicity or religion. If a plaintiff can prove that an employer used information garnered from social media websites to eliminate him or her from the selection process on the basis of race or religion, the employer will surely be held liable under the pertinent anti-discrimination statutes.

Similar concerns apply to gender and sexual orientations. If plaintiffs can show that they were discriminated against in the hiring process, or wrongfully terminated based on their gender or sexual orientation as gleaned from updates on Twitter, pictures on Facebook, or accounts on their personal blogs, the employers will be similarly liable.

Another concern that often goes overlooked is a potential employee’s political affiliations or activities. As social media sites enable the raw proliferation of personal information, such formerly underestimated liabilities are now articulated in warnings. As a first year law student, I remember sitting in a large lecture hall during a mandatory presentation put together by the Career Services Department and listening to the department head warn us about not putting any political information on our resumes, and to remove it from our Facebook settings.

“Law firms don’t want to know who you voted for,” she stated plainly. “You might be happy that Barack Obama is the new president of the United States. I can assure you that there are law firms right across the street where the people are not happy. Adding onto your resume that you’re a member of his fan club will not help you. If you worked as a campaign staffer or made cold calls for a candidate, participated in any kind of electioneering, and you really want to include that, go ahead. But consider removing the candidate’s name or finding a way to make it more general. You do not want to alienate yourself from the person making the hiring decision. Because they do look at that sort of thing, and it does factor into their decision.”

Even if political affiliation is left off the resume, it is often left on the Facebook profile, or reflected in blog posts or Twitter updates. It is, of course, difficult to prove that an employer used such information as the basis of an adverse action against a potential hire, but it is an issue that both employees and employers need to be aware of.

Another issue of workplace concern is protected activity, which may be embodied in the form of union membership or support. The National Labor Relations Act defines five unfair labor practices for which the employer will be held liable under the act:

1. Interference with, restraint, or coercion of employees in the exercise of their §7 rights of organization;
2. Domination of or interference with the formation or administration of any labor organization, or financial (or
It is clear that the third classification of unfair labor practices in §8 of the NLRA is the one of immediate relevance to this discussion. It is possible to learn from Facebook pages, Twitter updates, or personal blogs what a prospective employee’s feelings toward a union or unionization are. Pro-union or pro-management beliefs are intensely personal and often form the rational basis of discussions and discourse that are not expressly about employment at all, but framed in more general terms. Whatever the scope of the representation of the belief, it is very possible to glean from blog articles or Facebook status updates or even the posting of links on a user’s Facebook page where that user’s support rests.

Section 8(a)(3) expressly forbids discrimination in the hiring process based on an individual’s labor beliefs, whether that individual supports or opposes organization. If an employer can be shown to have used information about an individual’s labor beliefs found through social media outlets in order to discriminate against that person in the hiring process, that employer will have acted in direct violation of the NLRA and will be found to have committed an unfair labor practice.

These are some of the concerns that must be addressed when it comes to how employers may face legal repercussions for scouring various social media sites for job candidates. There are many companies, such as Smarth and Teneros, that offer services and software that enable companies to weed out social media postings for employees and prospective hires. The software searches through the databases of sites like Facebook and LinkedIn for the applicant’s name and pulls up whatever is linked to that name for the employer to consider during the hiring process, or during the ordinary course of business for employers seeking to monitor current employees.

With such services readily available, and often for a reasonable price, it is even more important for employers to understand that there are legal consequences to having personal information on their job candidates at their fingertips, to this previously unthinkable extent.

And for employees, words of caution don’t seem to resonate but always bear repeating: do not put anything up online that you do not want prospective employees to see. Even if you think it is unlikely that they will, err on the side of caution. As a lowly first year law student, I learned that it was not at all uncommon for an interviewing firm to have another low-level associate ‘friend request’ an applicant on Facebook in order for the hiring manager to gain access to the previously restricted page. Even if you have rigid privacy settings, you can never be aware of what one of your ‘Facebook Friends’ might be doing with your information.

You do not need to tweet while intoxicated. You do not need to upload an entire Facebook album of a particularly revealing Halloween costume. You do not need to write an expletive and hate-filled blog post about recent political events. Some things are better left unsaid.

And for employers seeking to minimize liability or unethical conduct at large, some things are better left un-Google'd.

©2019 Social Media Law Student