

## LINKEDIN TO FACEBOOK: THE RISKS OF TWEETING IN THE WORKPLACE

In the Digital Age we live in now, everything you could want to know about a person is likely just a click away. From the TV shows “liked” on Facebook to today’s lunch as the latest tweet, there is a smorgasbord of information available out in the Interwebs; and for better or worse, more and more employers are mining that data. Some use it in their [hiring decisions](#), but increasingly more companies are [finding reasons](#) to fire employees [over what they’ve said online](#).

### HIRING WITH SOCIAL MEDIA

Social networking sites can be a gold mine for employers, assisting them in [separating the wheat from the chaff](#) of potential hires. A survey done last summer found that [83% of employers used social networking sites](#) such as LinkedIn, Facebook, and Twitter in helping them evaluate job seekers. So does that mean you should lock up your online world so tight that potential employers can’t see how drunk you got last New Year’s? Well, maybe. Or, maybe not. Or even better yet, every law student’s favorite answer: it depends.

Even though hiring managers can peruse tweets and check out applicants’ Facebook walls, it might not be in their best interest to do so. They face [potential liability](#) from accusations of discriminatory hiring practices. Also, because Latinos and African-Americans are [disproportionately underrepresented](#) on social media sites like LinkedIn and Facebook, companies that use these sites face potential [disparate impact](#) claims. [Title VII of the Civil Rights Act of 1964](#) prohibits employers from using policies that adversely impact a protected class, even if the employer did not intend any discrimination. So if an employer is *only* using LinkedIn to gather information about applicants, then the applicant pool may not be diverse enough due to the smaller number of minorities represented on LinkedIn. Thus, minority job seekers could be disparately impacted by this practice.

Another risk hiring professionals run while examining social media data is that they may [stumble upon information](#) they aren’t allowed to ask the applicant. Several topics, like [age, religion, and family status](#), are off-limits in a job interview. Employers can try to mitigate the potential damage by [creating a “wall”](#) between the person who makes the hiring decision and the social media information. To accomplish this, another employee will gather the social media information, delete the protected information, and pass along what’s left to the hiring manager making the decision.

### FIRING WITH SOCIAL MEDIA

While social media has many implications in the world of hiring, [the firing](#) over social media use is getting more recent attention. For instance, look to Aflac [firing Gilbert Gottfried](#) as the voice of the Aflac duck over his insensitive jokes on Twitter about the tsunami crisis in Japan. Also, there was a [high profile firing of a social media firm used by Chrysler](#). The firm employee was

let go after sending out a profane tweet via Chrysler's Twitter account on accident (the [employee meant to tweet the profanity](#) on his personal account). Firing employees for [their comments on the Internet](#) is certainly not a new concept, but some studies estimate that the amount of employers firing over social media abuses is [on the rise](#), from four percent in 2008 to eight percent in 2009.

## NLRB GETTING IT DONE

The employment law community's interest recently spiked in social media firings thanks to the [National Labor Relations Board \(NLRB\)](#) stepping into the arena in two recent cases involving employees who were fired or disciplined for their comments on Facebook and Twitter. The NLRB [filed a complaint last November](#) against an employer who fired an employee for posting negative comments about her supervisor on Facebook. That case [recently settled](#). Last week, the [NLRB filed a complaint against Thomson Reuters](#) for disciplining an employee who tweeted that the company could improve the workplace by dealing honestly with the union.

The NLRB is a federal agency empowered by the [National Labor Relations Act \(NLRA\)](#) to protect the rights of employees and employers. The NLRA protects an employee's right to [discuss working conditions](#) and unionization with other employees. In both the Facebook and Twitter cases, the NLRB found the employers at fault for impinging on this right.

In the Facebook case, a medical technician had [criticized her supervisor](#) in a Facebook status update. Other employees chimed in, supporting the employee's negative remarks. The employer [defended the firing](#), saying that she was not fired for the comments, but instead due to complaints from patients and other staff members. The [NLRB stepped in](#) because the company's social media policy was overly broad and had been used to prohibit employees from discussing working conditions. The case [settled in February](#), with the employer agreeing to change its social media policy so that it no longer restricts employees from engaging in [protected concerted activities](#).

In the [Twitter case](#), a supervisor invited employees to tweet about how the company could improve working conditions, so the employee replied via her twitter account that the company could deal better with the union. The next day, she received a call from management advising her that the company's social media policy prohibited her from saying anything online that would damage the company's reputation. The employee felt intimidated, but the employer defends the action by saying that it did not discipline her. Again, the [NLRB stepped in](#) to defend the worker's right to discuss working conditions and unionization. This case is ongoing.

## IS MYSPACE A SAFESPACE?

Employers need not only be concerned about firing over social media postings if the posting could be construed as discussing working conditions, but they should also be careful how they obtain social media postings. Many people [use privacy settings](#) to control who can see what

they've posted on Facebook, Twitter, or other social media sites, and some sites are [better](#) at ensuring privacy than others. If an employee locks up his/her social media presence, it's [probably a bad idea](#) for an employer to find other means of getting at that data.

In [Pietrylo v. Hillstone Restaurant Group](#), [two employees](#) set up a MySpace group (yes, MySpace still exists!) for past and current employees to vent about their employer. The group was password-protected and invite-only. Eventually, a manager learned of the group and with the help of another manager, convinced an employee with access to give them her login and password. The employees were then fired. Because of the manner in which the managers gained access to the group, the court found that the company had violated the [Stored Communications Act](#) (a really [complicated act](#) that most judges don't even understand, but is essentially violated if you don't have authorization to access stored data). The bottom line for employers: don't snoop where you're not allowed.

## WHAT UP, PRIVACY CONTROLS

With more and more companies monitoring social media sites for employee misconduct and to assist in recruiting efforts, employees and job seekers need to be aware of what they are saying online and who can access that information. Employers may not be able to fire you over what you say regarding working conditions, but that doesn't mean that everything said online is protected from an employer's action.

The news isn't all bad, though. Since more employers are glancing at your online profile, you [can use this to your advantage](#) as an applicant. Companies have been [successful](#) at branding themselves with social media, and so can the employees. Each social media platform can be used to maximize one's presence within a field of expertise. In this way, a public profile can actually help you find a job!

[The Pietrylo case](#) provides good news for employees and job seekers. If you don't authorize your employer (or the company you're seeking employment from) to access your private site, then [the company faces liability](#) if they try to access it through other means. However, publicly available information is fair game, so make sure your privacy settings are secure. Also, even if your tweets are protected or your Facebook privacy settings are maximized, [if your boss is a Facebook friend](#) or following you on Twitter, then what you say is available for their use. Don't become [this person](#). Of course, it also can't hurt to remember [Thumper's law](#) when interacting with others online: "If you can't say something nice, don't say nothing at all."