

**Facebook, and Twitter, and LinkedIn! Oh my!  
The evolving influence of social media in the workplace**



licensed under Attribution-NonCommercial-ShareAlike 2.0 Germany | Ludwig Gatzke | <http://flickr.com/photos/stabilo-boss/>

V 216-736-7226  
F 216-621-6536  
E [jth@kjk.com](mailto:jth@kjk.com)

One Cleveland Center  
20th Floor  
1375 East Ninth Street  
Cleveland, OH 44114-1793  
216.696.8700  
[www.kjk.com](http://www.kjk.com)

Cleveland and Columbus

**Jonathan T. Hyman**

Kohrman Jackson & Krantz P.L.L.  
Cleveland, Ohio

Ohio Employer's Law Blog: [www.ohioemployerlawblog.com](http://www.ohioemployerlawblog.com)  
[www.twitter.com/jonhyman](http://www.twitter.com/jonhyman)  
[www.facebook.com/ohio.employer.law.blog](http://www.facebook.com/ohio.employer.law.blog)

**Think Before You Click:  
Strategies for Managing Social Media in the Workplace**  
Available at [www.thompson.com/public/offerpage.jsp?prod=CLKDL](http://www.thompson.com/public/offerpage.jsp?prod=CLKDL)

**Table of Contents**

**Introduction .....4**

**What is Social Media, and Why Should You Care? ..... 5**

    Facebook and Twitter and blogs, oh my! ..... 5

    Can employers base employment decisions on employees’  
    personal internet activities? ..... 6

    Employee disloyalty and Facebook..... 7

    Tweeting away your job ..... 9

    A textbook example of Facebook firing.....10

    Employees’ social networking continues to confound employers .11

**The Social Media Policy .....12**

    Employer electronic monitoring survey illustrates the importance  
    of clearly defined policies ..... 12

    Drafting an appropriate social networking policy ..... 13

    Drafting a social networking policy: 7 considerations.....14

    Companies are banning social networking. Should you?.....16

    Is it wrong to “friend” your boss on Facebook? ..... 17

    Is LinkedIn a risk for employers? .....18

**Legal Risks ..... 19**

    Does your social networking policy violate federal labor laws?....19

    Employees aren’t the only ones who have to watch what they  
    post: Social media as retaliation ..... 20

GINA and Social Media ..... 21

**Social Media and Litigation..... 22**

Discovery of social networks in employment disputes ..... 22

More on discovery of social networks: Subpoenas to websites  
proving to be difficult ..... 24

More on the lack of privacy in social media..... 26

Court compels production of social networking user names,  
logins, and passwords, and dispels any notions of personal privacy  
..... 27

## **Introduction**

It is no coincidence that the founder of Facebook was *Time Magazine's* 2010 Person of the Year. 2010 was the year of social media, and it is only poised to increase in importance and influence. Social media permeates every aspect of today's HR—from hiring employees (what is and is not appropriate online fodder for evaluating candidates?), managing employees (what is the proper use of social media by employees, both on and off duty?), firing employees (for what reasons can employers terminate employees for their online activities?), and litigation with employees (when is social media discoverable in employment disputes?). Businesses need to know the rules of this evolving road, from how to legally use Facebook to recruit, to how to draft and implement a social media protocol and policy, to how to manage employees' privacy expectations, how to use social media as a sword in litigation, and how to train your employees in the appropriate use of this crucial workplace tool.

## What is Social Media, and Why Should You Care?

### Facebook and Twitter and blogs, oh my!

(Originally published at [www.ohioemployerlawblog.com/2009/06/do-you-know-facebook-and-twitter-and.html](http://www.ohioemployerlawblog.com/2009/06/do-you-know-facebook-and-twitter-and.html))

Cave drawings were likely the earliest form of social networking. Today people tweet their thoughts for the world to see. In between we've had instant messaging, MySpace, Facebook, and blogs. The next several big things are already being hatched by some students at Stanford or MIT. Online social networking is here to stay – the only change will be in what form it takes.

According to a recent survey conducted by Deloitte, 22% of employees say that they use some form of social networking five or more times per week, and 15% of employees admit they access social networking while at work for personal reasons. Yet, only 22% of companies have a formal policy that guides employees in how they can use social networking at work.

Before we can figure out what to do about these exploding media at work, we first need to know exactly what we are dealing with. So, for the uninitiated, the following is a short lesson on the various types of social networking that are likely being accessed from your workplace right now.

- i **Blogs:** Blog is short for weblog. Blogs either provide commentary on news or a particular subject (such as the [Ohio Employer's Law Blog](#)), or serve as an online diary. Most are text-based, but blogs can also focus on art, photos, videos, and audio (you may have heard of podcasts). There are hundreds of millions of blogs on the internet, many updated as often as every day.
- i **Facebook:** Facebook started as an online tool for college and university students to connect with each other. It has since expanded to allow anyone over the age of 13 with a valid email address to open a free account. It is loosely organized into a variety of networks based on schools, location, employers, charities, and other causes. Connections are known as "friends." People update with short written blurbs about what they're doing, pictures, video, and the like. Users can also post

on friends' pages. If you're not on Facebook, I guarantee someone you know is. In fact, Facebook has over 600 million registered users, and is the biggest website in the world. Even my mom has a Facebook page.

- i LinkedIn: LinkedIn is an online network for professionals. It allows people to search and connect via alma mater, location, employer, or various user-created groups. It has over 90 million members.
- i Twitter: Twitter is latest big-thing in social networking. It is what is known as "micro-blogging." "Tweets" are text-based posts of up to 140 characters, displayed on the user's profile page and delivered to followers, other users who have subscribed.

Employers have three options to try to regulate social networking by employees at work: 1) turn off their internet access; 2) institute progressively harsher discipline against employees caught Facebooking or tweeting at work; or 3) draft a reasonable policy that recognizes the intersection of technology in the workplace and employees' lives, and establishes reasonable baseline expectations about what is and is not acceptable use at work. Only the latter option makes any real sense.

### **Can employers base employment decisions on employees' personal internet activities?**

(Originally published at [www.ohioemployerlawblog.com/2007/11/can-employers-base-employment-decisions.html](http://www.ohioemployerlawblog.com/2007/11/can-employers-base-employment-decisions.html))

Courtesy of *The Washington Post* comes this gem:

Kevin Colvin, an intern at the Anglo Irish Bank of North America ... e-mailed his manager on the afternoon of Oct. 31 claiming "something came up at home" in New York and that he needed to miss work the next day. For whatever reason, perhaps managerial intuition, his boss decided to inspect Colvin's Facebook page on Nov. 1 and apparently found pictures of the intern dressed as a

fairy, beer in hand, at a Halloween party in Massachusetts.

Rather than reprimand him, the manager decided to have a little fun. He shot Colvin an e-mail back stating: "Thanks for letting us know -- hope everything is ok in New York. (cool wand)" with the fairy picture attached. And if that weren't embarrassing enough, the manager reportedly BCCed the rest of the company. Those images are now being forwarded to offices around the world for cubicle dwellers to enjoy.

The internet now provides a plethora of social outlets -- blogs, social networking sites such as MySpace, Facebook, and Twitter, video repositories such as YouTube and Break, and even an entire alternate universe, Second Life. Once someone puts something out on the internet, it becomes fair game for anyone and everyone to see, employers included. The WP article cites a vault.com survey in which 82 percent of employers responded that negative information from an online profile would affect their decision to hire an applicant. Presumably a similar but likely small number would also consider negative online information in a decision to continue the employment of a current employee. It is hard to imagine that an employer is somehow invading an employee's privacy by viewing something that is publicly available on the web. If an employee is at-will, and standards are otherwise neutrally applied, there should not be anything unlawful about making a hiring or employment decision based on an employee's personal internet presence, especially if you catch the employee in a lie, such as was the case with Kevin Colvin.

### **Employee disloyalty and Facebook**

*(Originally published at [www.ohioemployerlawblog.com/2009/03/employee-disloyalty-and-facebook.html](http://www.ohioemployerlawblog.com/2009/03/employee-disloyalty-and-facebook.html))*

Dan Leone was a lifelong fan of the Philadelphia Eagles. One could only imagine that when his favorite team hired him as a game-day stadium employee, it was his dream job. Last week, the Denver Broncos signed free agent safety Brian Dawkins, the team's emotional leader and one of the franchise's historical great players.

Upset with the Eagles's decision not to resign Dawkins, Leone chose to vent on his Facebook page, updating his status: "Dan is [expletive] devastated about Dawkins signing with Denver ... Dam Eagles R Retarded!!"

*The Philadelphia Inquirer* reports on the team's termination of Leone:

Less than two days after posting the Dawkins remarks, Leone said, he was contacted by Leonard Bonacci, the team's director of event operations. According to Leone, Bonacci said they needed to talk about Leone's Facebook page, and Leone agreed. Leone - who deleted the comment - figured that the two would sit down and that he could apologize to Bonacci in person. But Leone said Bonacci never got back to him after that.

Two days later, Leone said, he received a call from Rachel Vitagliano, the team's guest services manager. Leone said she fired him over the phone. The conversation lasted less than 10 minutes.

No warning. No suspension. No face-to-face meeting. Just a quick call to tell Leone he'd been terminated.

All over the Internet, the Eagles are taking a beating for Leone's. For example, according to an ESPN.com poll, 80.5% believe the Eagles were not justified in firing Leone.

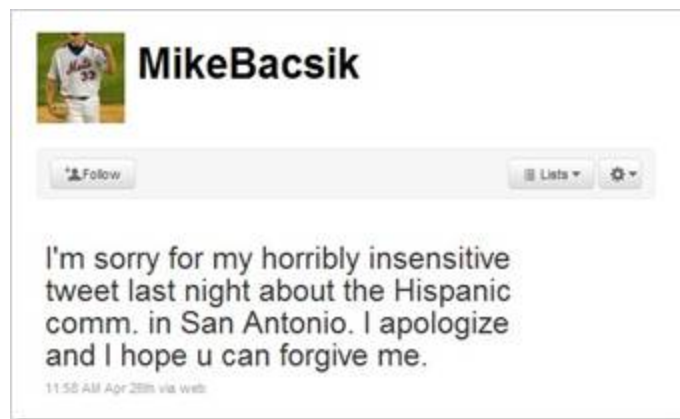
Let me take the other side. It may seem heavy-handed for the Eagles to take a stand against a part-time seasonal employee. If an employer wants to effectively enforce a policy, it has to do so across the board. The Eagles are sending the message that it will not tolerate its employees publicly making negative statements about the organization. While some will consider it unfair for this message to be sent at Leone's expense, this employer will be better served the next time, when it is a high-level front office employee instead of a part-time stadium employee. In employment law, consistency is key, and to be consistent, someone always has to be first.

## Tweeting away your job

(Originally published at [www.ohioemployerlawblog.com/2010/04/tweeting-away-your-job.html](http://www.ohioemployerlawblog.com/2010/04/tweeting-away-your-job.html))

Before yesterday, former major league pitcher Mike Bacsik was likely most famous for giving up Barry Bonds 756th homer. This morning, he is perhaps more well known for the racially insensitive tweet that has cost him his sports radio hosting gig in Dallas.

According to the *Dallas Morning News*, Bacsik said he drunkenly tweeted, “Congrats to all the dirty mexicans in San Antonio” after watching the Spurs beat the Mavs on Sunday night. To his benefit, Bacsik at least realizes his mistake. He has removed the offensive tweet, and replaced it with the following apology on this Twitter account.



ESPN.com quotes Bacsik’s words of wisdom for all employees:

When you tweet like I did, you can’t see the sarcasm. It’s not a good joke. You can’t tell if it was pure hate or sarcasm. I never got to say anything. My tweets were talking for me. When you tweet like that, it’s not a playful, harmless thing. It’s not what it was meant to be.

A disciplined or terminated employee may not be as understanding or remorseful as Bacsik. So that employees understand your expectations about responsible social networking, it is best to have a

policy. That policy should spell out to employees that what they post online is public, that anything in cyberspace can be used as grounds for discipline or termination, and that there are consequences for posting anything that negatively reflects on your business.

### **A textbook example of Facebook firing**

*(Originally published at [www.ohioemployerlawblog.com/2010/05/textbook-example-of-facebook-firing.html](http://www.ohioemployerlawblog.com/2010/05/textbook-example-of-facebook-firing.html))*

I spent the summer between my junior and senior years of high school bussing tables in a nursing home dining room. Not the world's most glamour job, but it paid \$8 an hour, which in 1989 was a lot of money. Needless to say, we had our fair share of difficult people to deal with. One of my co-workers would retaliate by spitting in the resident's food. Had he been caught by management, there is no doubt he would have been fired.

Flash forward 21 years – social media is the new spitting. Unlike spitting, however, social media is public, and much easier to discover. When a waitress at a Charlotte restaurant was stiffed on a tip from a difficult table, she took her grievance to Facebook, “Thanks for eating at Brixx, you cheap piece of ---- camper.” Two days later, her managers fired her for violating company policies against speaking disparagingly about customers and casting the restaurant in a negative light on social networks.

There are three important lessons to take away from this tale that is becoming all too common.

Your employees are on Facebook, Twitter, blogs, and myriad other websites, saying things both good and bad about your business. Your business needs to harness the good and discourage the bad.

If an employee makes disparaging comments about your business on the Internet, you are within your rights as an employer to fire that employee.

But, you are selling your business short if you don't have a policy that warns employees of the potential punishments for illegitimate

and irresponsible uses of social media, as well as instructs them about legitimate and responsible uses.

### **Employees' social networking continues to confound employers**

*(Originally published at [www.ohioemployerlawblog.com/2009/07/employees-social-networking-continues.html](http://www.ohioemployerlawblog.com/2009/07/employees-social-networking-continues.html))*

Let's suppose that you learn that a group of employees have created an on-line group that's sole purpose is to provide a forum for other employees to bash your company. Do you have the right to require the employees to provide the password to enable you access the forum and its members? According to one federal court in New Jersey, the answer is no.

According to Law.com, a federal jury has awarded \$15,000 to two restaurant employees terminated for criticizing their employer on MySpace. The jury determined that by requiring the employees to divulge their passwords, the employer violated the Stored Communications Act, a federal law that extends liability to parties that exceed authorization to access electronic communications.

This area of the law is decidedly gray. The question for you, as an employer, to ask yourself before you undertake a gray-area employment practice is whether you want to foot the legal bill to prove its legality if a lawsuit is filed. In the case discussed above, the restaurant did not have to access the on-line forum for grounds to terminate the two employees who administered it. A manager had reliable information that the two at-will employees were acting unprofessionally by flaming management. While the damages to be paid were low, the attorneys' fees expended by the employer to defend its practice were certainly significantly higher. Companies should consider letting others push the legal envelope and only adopt tried and tested employment policies and practices that clearly pass legal muster.

## The Social Media Policy

### Employer electronic monitoring survey illustrates the importance of clearly defined policies

(Originally published at [www.ohioemployerlawblog.com/2008/02/employer-electronic-monitoring-survey.html](http://www.ohioemployerlawblog.com/2008/02/employer-electronic-monitoring-survey.html))

The Electronic Discovery Navigator is reporting that according to the 2007 *Electronic Monitoring & Surveillance Survey from American Management Association (AMA) and The ePolicy Institute*, more than half of all employers have fired an employee for e-mail or internet abuse. According to the report:

The 28% of employers that have fired an employee for e-mail misuse cited the following reasons:

- i Violation of any company policy (64%)
- i Inappropriate or offensive language (62%)
- i Excessive personal use (26%)
- i Breach of confidentiality rules (22%)
- i Other (12%)

The 30% of employers that have fired an employee for internet abuse cited the following reasons:

- i Viewing, downloading, or uploading inappropriate/offensive content (84%)
- i Violation of any company policy (48%)
- i Excessive personal use (34%)
- i Other (9%)

The stat that really caught my eye is that of the 65% of companies that use software to block connections to websites they deem inappropriate for work, 18% prevent employees from visiting blogs. And, it's not only the reading of blogs that is getting employees in trouble. Both Ernie the Attorney and John Phillips' Word on Employment Law are reporting on a CNN producer fired for having a blog that CNN deemed to be unfriendly towards it. CNN has a policy in its handbook that prohibits employees from writing for any non-CNN outlet without network approval, and terminated the employee for his off-work musings.

Technology in today's workplace comes in too many forms to keep track. It's no longer just enough to have a policy that covers e-mail and internet access. Workplace technology is not going to get any less complicated, and it is important to have policies in place that keep up with the changes. Policies should also cover blackberries and other PDAs, cell phones, and even blogs. Companies have to be careful, however, not to overreach and be too draconian in what they try to accomplish with these policies. If you intend to hold employees accountable for what they do on their private free time (whether it's blogging, smoking, or any other lawful activity), it's best to have those expectations out in the open so that everyone is operating under the same ground rules, and people will have less of a reason to gripe if there is some adverse action taken.

### **Drafting an appropriate social networking policy**

*(Originally published at  
[www.ohioemployerlawblog.com/2009/01/drafting-appropriate-social-networking.html](http://www.ohioemployerlawblog.com/2009/01/drafting-appropriate-social-networking.html))*

According to a recent report published by the Pew Internet & American Life Project, the percentage of adults who use social networking sights such as MySpace, Facebook, and LinkedIn has more than quadrupled in the past four years – from 8% in 2005 to 35% in 2008. By age, the stats break down as follows:

- i 18 – 24: 75%
- i 25 – 34: 57%
- i 35 – 44: 30%
- i 45 – 54: 19%
- i 55 – 64: 10%
- i 65 & over: 7%

For American businesses, these numbers mean that a large quantity of workers have profiles on any number of social networking sights (yours truly included). They also mean that if your internet or technology policy does not cover the appropriate use of social networking and blogging you are leaving yourself potentially exposed for abuse, embarrassment, and potential liability.

Let me offer a few thoughts on putting together a policy to cover employees' use of social networking.

1. A blanket prohibition does not make sense. I am not a fan of draconian policies. They cause more harm than good. They are bad for morale, drive away quality employees, beg for violations, and hamstring employers into making personnel decision they might not otherwise want to make when the policy is violated. If the reality is that a large chunk of employees are social networking, employers should embrace this medium within reason.
2. Employees need to understand that with the ability to use social networking comes responsibility. If a profile can link someone to their place of employment, the employee cannot post anything that could potentially embarrass or otherwise reflect poorly on his or her employer. This policy is one of common sense. Posting where you went to college is acceptable, posting pictures of yourself drunk while in college is not.
3. Use while at work should be governed by a company's general internet protocol. If a company permits limited personal use at work (which most should), then the same ability should be extended to employees' social networking activities.

These types of policies are governed by one guiding principle – treat employees like adults and assume that they will return the favor until they prove otherwise.

### **Drafting a social networking policy: 7 considerations**

*(Originally published at [www.ohioemployerlawblog.com/2009/06/drafting-social-networking-policy-7.html](http://www.ohioemployerlawblog.com/2009/06/drafting-social-networking-policy-7.html))*

I could draft a perfect social networking policy using only a few words: “Be mature, be ethical, and think before you type.”  
Ultimately, you may decide that such brevity is what you want for

you business. For the sake of completeness, though, I offer seven thoughts to consider when drafting a social networking policy.

1. *How far do you want to reach?* Social networking presents two concerns for employers – how employees are spending their time at work, and how employees are portraying your company online when they are not at work. Any social networking policy must address both types of online use.
2. *Do you want to permit social networking at work, at all?* It is not realistic to ban all social networking at work. For one thing, you will lose the benefit of business-related networking, such as LinkedIn. Without turning off internet access or blocking certain sites, a blanket ban is also hard to monitor and enforce.
3. *If you prohibit social networking, how will you monitor it?* Turning off internet access, installing software to block certain sites, or monitoring employees' use and disciplining offenders are all possibilities, depending on how aggressive you want to be and how much time you want to spend watching what your employees do online.
4. *If you permit employees to social network at work, do you want to limit it to work-related conduct, or permit limited personal use?* How you answer this question depends on how you balance productivity versus marketing return.
5. *Do you want employees to identify with your business when networking online?* Because this blog is affiliated with my law firm, Kohrman Jackson & Krantz, I am cognizant that everything I write reflects on my partners and my business. Employees should be made aware that if they post as an employee of your company, the company will hold them responsible for any negative portrayals. Or, you could simply require that employees not affiliate with your business and lose the networking and marketing potential Web 2.0 offers.

6. *How do you define “appropriate business behavior?”* Employees need to understand that what they post online is public, and they have no privacy rights in what they put out for the world to see. Anything in cyberspace can be used as grounds to discipline an employee, no matter whether the employee wrote it from work or outside of work. There should be consequences for any information that negatively reflects on your business.
  
7. *How will social networking intersect with your broader harassment, technology, and confidentiality policies?* Employment policies do not work in a vacuum. Employees’ online presence, depending on what they are posting, can violate any number of other corporate policies. Drafting a social networking policy is an excellent opportunity to revisit, update, and fine-tune other policies.

### **Companies are banning social networking. Should you?**

*(Originally published at [www.ohioemployerlawblog.com/2009/10/companies-are-banning-social-networking.html](http://www.ohioemployerlawblog.com/2009/10/companies-are-banning-social-networking.html))*

According to a recent survey by Robert Half Technology, more than half of employers completely prohibit their employees from visiting social networking sites during working time. The complete results are as follows:

- i Prohibited completely: 54%
- i Permitted for business purposes only: 19%
- i Permitted for limited personal use: 16%
- i Permitted for any type of personal use: 10%
- i Don’t know/no answer: 1%

I’ve been answering a lot of questions lately on social networking. It does not seem realistic to totally ban all social networking at work. To effectively implement a total prohibition you must either turn off internet access, install software to block certain sites, or monitor employees’ use and discipline offenders. These options, though, stifle business-related productivity, are expensive, or are time consuming. Do you really want all employees not to be able to access the internet

for any purpose? Do you have the manpower to dedicate to around-the-clock monitoring of employees' online activity?

The better option is to allow limited personal social networking during business hours. If you treat employees respectfully and professionally, in most cases they will return the courtesy. This is not to suggest that you act naively. You also need to have a social networking policy to cover those circumstances when employees abuse the privilege through excessive use or inappropriate postings.

### **Is it wrong to “friend” your boss on Facebook?**

*(Originally published at [www.ohioemployerlawblog.com/2010/03/is-it-wrong-to-friend-your-boss-on.html](http://www.ohioemployerlawblog.com/2010/03/is-it-wrong-to-friend-your-boss-on.html))*

Mashable reports on a recent survey conducted by Liberty Mutual's Responsibility Project, in which 56% of Americans reported that “it's ‘irresponsible’ to friend your boss on Facebook, while 62% of bosses agree it's wrong to friend an employee.” These numbers simply beg the question – what does your social media policy say about this issue? Here's five suggestions:

1. Anything goes. Any employee can friend any other employee regarding of rank or position.
2. Supervisors are prohibited from friending direct reports, but employees can friend their supervisors (who can choose whether to accept the request).
3. Supervisors and their reports cannot be Facebook friends, regardless of who initiates the request.
4. Employees are only permitted to be Facebook friends with their peers. No one can friend anyone higher or lower on the org chart.

5. Employees are expressly prohibited from being Facebook friends with any co-workers, regardless of position.

The option you choose has a lot more to do with your corporate culture than what is legal or illegal. Your choice, however, will impact certain legal issues, such as harassment liability. Regardless of which option you choose, you should choose one to incorporate into your social media policy.

### **Is LinkedIn a risk for employers?**

(Originally published at [www.ohioemployerlawblog.com/2009/07/is-linkedin-risk-for-employers.html](http://www.ohioemployerlawblog.com/2009/07/is-linkedin-risk-for-employers.html))

One of the more interesting features of LinkedIn is the ability to recommend your connections. In fact, LinkedIn will prod you to recommend others to further complete your profile. For example, my LinkedIn profile is 90% complete, and it tells me I can get to 95% if I recommend another person. Most successful professionals share two personality traits that will cause them to strive for that 100% goal – overachieving and type-A personalities.

In the *National Law Journal*, however, Tresa Baldas makes an excellent point about the legal risks posed by LinkedIn recommendations. Let's say, for example, a manager provides one of his subordinates a glowing LinkedIn recommendation. If that employee is later fired, the odds are pretty high that the employee will try to use that recommendation as evidence of pretext in a later discrimination suit.

Social media provides a gold mine of information to use in employment lawsuits. Employees' Facebook pages, YouTube videos, and blogs are all fertile ground for discovering useful information to use against an employee. If employers are going to swim in these waters, they need to be equally mindful that what they write about an employee can also be used against the employer. When drafting a social media policy, consider these risks and decide whether an outright ban on LinkedIn recommendations is best for your organization.

## Legal Risks

### **Does your social networking policy violate federal labor laws?**

*(Originally published at [www.ohioemployerlawblog.com/2010/11/does-your-social-networking-policy.html](http://www.ohioemployerlawblog.com/2010/11/does-your-social-networking-policy.html))*

It was only a matter of time before the NLRB inserted itself into the intersection of social networking and employment relations. It has a Twitter account. Now, it has issued its first complaint challenging an employer's social networking policy.

The NLRB has issued a complaint against a company that fired an employee after posting negative comments about her supervisor on her personal Facebook page. The Blog of Legal Times reports that the NLRB not only alleges that the employer illegally fired the employee for the posting, but that the company "maintained and enforced an overly broad blogging and Internet posting policy."

An NLRB investigation found that the Facebook postings were "protected concerted activity," and that the company's blogging and Internet posting policy contained unlawful provisions, including one that barred employees from making disparaging remarks when discussing the company or supervisors and another that prohibited employees from depicting the company in any way over the Internet without company permission.

"Such provisions constitute interference with employees in the exercise of their right to engage in protected concerted activity," the NLRB found.

This case could have far reaching implications for all employers—not just those that are collectively bargained. If the NLRB concludes that a singular posting on a personal website constitutes protected concerted activity, then it will be nearly impossible for an employer to regulate off-the-clock Internet activity.

## **Employees aren't the only ones who have to watch what they post: Social media as retaliation**

*(Originally published at [www.ohioemployerlawblog.com/2011/01/employees-arent-only-ones-who-have-to.html](http://www.ohioemployerlawblog.com/2011/01/employees-arent-only-ones-who-have-to.html))*

Employers are also at risk for the reckless use of social media. The EEOC recently filed a complaint alleging that a manager used a company's Facebook page to post threatening messages in retaliation for a prior harassment complaint.

It is becoming increasingly clear that communication is communication, whether spoken, in writing, in an email, in a text message, or posted on a social media website such as Facebook. Consistently, courts are ignoring the vessel used to communicate the message. If a message is retaliatory, it will be treated the same, whether told to an employee or posted on a Facebook page.

Other than retaliation, what are some of the other legal risks should employers be aware of concerning social media?

- i Harassment
- i Defamation
- i Disclosure of confidential or proprietary information
- i Commentary on on-going litigation

How can employers guard against these risks? Proactive training. Businesses that fail to properly train all employees about the risks of the reckless use of social media are acting recklessly themselves.

## **GINA and Social Media**

*(Originally published at*

<http://www.ohioemployerlawblog.com/2010/11/5-most-interesting-things-about-gina.html>)

Late last year, the EEOC published its long-awaited regulations to the employment provisions of GINA, the Genetic Information Nondiscrimination Act. According to the EEOC, GINA has 4 stated purposes:

1. To prohibit the use of genetic information in employment decisions;
2. To restrict employers and others from requesting, requiring, or purchasing genetic information;
3. To require that employers maintain genetic information as a confidential medical record, with strict limits on disclosure; and
4. To provide remedies for individuals whose genetic information is acquired, used, or disclosed in violation of the Act.

Interestingly, GINA has an exception for genetic information inadvertently learned via social media. GINA's prohibition against the request of genetic information about an employee or family member includes Internet searches in a way that is likely to result in obtaining genetic information, even if the information is publicly available. However, if an employer "inadvertently learns genetic information from a social media platform which he or she was given permission to access by the creator of the profile at issue" (such as an employee who posts family medical history on his Facebook wall, and his supervisor, with whom he is a Facebook friend, sees it), GINA has not been violated. Employers are similarly protected for genetic information employees inadvertently disclose during casual "water cooler" conversations.

## Social Media and Litigation

### Discovery of social networks in employment disputes

(Originally published at [www.ohioemployerlawblog.com/2010/05/do-you-know-discovery-of-social.html](http://www.ohioemployerlawblog.com/2010/05/do-you-know-discovery-of-social.html))

I've long preached that employees should not enjoy an expectation of privacy in information they voluntarily place on the Internet, including social networks like Facebook. What they make available for the others to see should be fair game for employers to use in making employment decisions. According to one federal court in Indiana, it is also fair game for employers to use this information in defending against discrimination lawsuits. Because there are so few cases discussing this developing issues of the discoverability of social networking information, this case is helpful in defining the scope of these issues.

*EEOC v. Simply Storage Management* (S.D. Ind. 5/11/10) concerns two employees' sexual harassment claims, and in particular their claims of depression, stress, and other psychiatric disorders stemming from the harassment. In discovery, Simply Storage sought the following information from the claimants' social networking pages on Facebook and MySpace:

- i All photographs or videos posted by the claimants or anyone on their behalf on Facebook or MySpace.
- i Electronic copies of the claimants' complete profiles on Facebook and MySpace (including all updates, changes, or modifications to their profiles) and all status updates, messages, wall comments, causes joined, groups joined, activity streams, blog entries, details, blurbs, comments, and applications (including, but not limited to, "How well do you know me" and the "Naughty Application").

The EEOC objected to the discovery on the grounds that the requests were not relevant, improperly infringed on the claimants' privacy, and would harass and embarrass the claimants. Simply Storage claimed that discovery of these matters was proper because the claimants put their emotional health at issue beyond that typically encountered with "garden variety emotional distress claims."

The court agreed with the employer and ordered the discovery. In doing so, it made four key observations about the discovery of social networking in discrimination cases.

1. Social networking content is not shielded from discovery merely because it is “locked” or protected as “private”.
2. However, all social networking content is not necessarily relevant or discoverable in all cases; the information must still be relevant to a claim or defense in the case. The court used the following example to illustrate this difference: “If a claimant sent a message to a friend saying she always looks forward to going to work, the person to whom she sent the message and the substance of the message are what should be considered to determine whether the message is relevant.... But the mere fact that the claimant has made a communication is not relevant because it is not probative of a claim or defense in this litigation.”
3. Allegations of depression, stress disorders, and similar injuries will manifest themselves in some social networking content. An examination of that content might reveal whether and when onset occurred, the degree of distress, and other stressors that could have produced the alleged emotional distress.
4. Because discovery is meant to be liberal, the producing party should err in favor of production if there is any doubt over the arguable relevance of social networking information.

The court also specifically addressed the employees’ privacy concerns:

The court agrees with the EEOC that broad discovery of the claimants’ SNS could reveal private information that may embarrass them. Other courts have observed, however, that this is the inevitable result of alleging these sorts of injuries. Further, the court finds that this concern is outweighed by the fact that the production here would be of information that the claimants have already shared with at least one other person through

private messages or a larger number of people through postings. As one judge observed, “Facebook is not used as a means by which account holders carry on monologues with themselves.”

In other words, if it is fit to share with your Facebook friends, it is fit to be disclosed in discovery (as long as it’s relevant). As these issues become more prevalent in litigation, these guideposts will become more fleshed out. In the meantime, consider including requests for social networking information in all employment disputes.

### **More on discovery of social networks: Subpoenas to websites proving to be difficult**

(Originally published at [www.ohioemployerlawblog.com/2010/06/more-on-discovery-of-social-networks.html](http://www.ohioemployerlawblog.com/2010/06/more-on-discovery-of-social-networks.html))

*EEOC v. Simply Storage Management* concerned discovery requests by an employer for a claimant’s social network pages. Rebuking any claims of an infringement of the plaintiff’s privacy, the court stated:

The production here would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through postings. As one judge observed, “Facebook is not used as a means by which account holders carry on monologues with themselves.”

In *Crispin v. Christian Audigier, Inc.* (C.D. Cal. 5/26/10), a different federal court confronted the issue of the discovery of social networks from the websites themselves via a subpoena. Most of the 37-page opinion deals with the technical issue of whether and to what extent third-party providers such as Facebook are covered by the Stored Communication Act. What is of interest, though, is the distinction drawn by the court based on privacy expectations and privacy settings.

Essentially, social networks offer three possible types of information:

1. Information made public via a social network—such as something posted on one’s Facebook wall or on Twitter).
2. Information not readily available to the general public via option privacy settings.
3. Private messages passed between users of the social networks, with the website used merely as a conduit to facilitate the private communications.

Only the first category may be discoverable via a subpoena, while the latter two may be worthy of protection by the provider:

With respect to webmail and private messaging, the court is satisfied that those forms of communications media are inherently private such that stored messages are not readily accessible to the general public.... Those portions of the ... subpoenas that sought private messaging are therefore quashed. With respect to the subpoenas seeking Facebook wall postings and MySpace comments, however, the court concludes that the evidentiary record ... is not sufficient to determine whether the subpoenas should be quashed. The only piece of evidence adduced was a Wikipedia article stating that Facebook permits wall messages to “be viewed by anyone with access to the user’s profile page” and that MySpace provides the “same” functionality. This information admits of two possibilities; either the general public had access to plaintiff’s Facebook wall and MySpace comments, or access was limited to a few.

What are the lessons to be learned from this case?

1. This case does not provide much in the way of relief. The prize isn’t information that is already publicly available, since you can just go to Facebook and get that information on your own. The prize is the private information to which you do not have access, and which this court suggests is protected from disclosure.

2. The Stored Communication Act is very technical, and makes it very difficult to obtain any stored information directly from a social network or Internet provider without the users written consent.
3. Provided that you are seeking information about a party to the litigation (for example, the plaintiff), you will be much better served simply asking for it in a Rule 34 document request. If the information is no longer accessible, a court can compel the party to sign a release so that you can seek the information directly from the website without having to worry about the Stored Communication Act. In other words, if the information had been requested directly from the party instead of trying to get it from the website, the Stored Communication Act is not an issue, and this case likely has a different result.

### **More on the lack of privacy in social media**

(Originally published at [www.ohioemployerlawblog.com/2010/09/do-you-know-more-on-lack-of-privacy-in.html](http://www.ohioemployerlawblog.com/2010/09/do-you-know-more-on-lack-of-privacy-in.html))

There are not (yet) many cases dealing with the discovery of litigants' social networking information. Thus, whenever a court addresses the issue, it becomes newsworthy.

*Romano v. Steelcase Inc.* (N.Y. 9/21/10) is a personal injury case. The defendant claimed that information the plaintiff posted on her Facebook and MySpace pages was inconsistent with her claim regarding the nature and extent of her injuries. The court disagreed with the plaintiff's argument that she had any expectation of privacy what she posted on social networking sites:

Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators

regarding privacy and social networking sites, given the millions of users, “[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking.”

It is becoming increasingly more difficult to convince courts that individuals have any privacy expectations in social networking information. Instead, these discovery disputes turn on issues of relevancy—whether the information bears on any issue in the case. In cases involving injuries (whether physical or emotional, and including employment cases), plaintiffs will have a very hard time shielding this type of information from discovery.

**Court compels production of social networking user names, logins, and passwords, and dispels any notions of personal privacy**

*(Originally published at [www.ohioemployerlawblog.com/2010/10/court-compels-production-of-social.html](http://www.ohioemployerlawblog.com/2010/10/court-compels-production-of-social.html))*

Social networking profiles and posts have become fertile ground for the formal discovery of information about litigants. One Pennsylvania trial court took this discovery one step further, and ordered the production of a plaintiff’s social networking user names and passwords.

In *McMillen v. Hummingbird Speedway, Inc.* (Pa. Ct. of Common Pleas 9/9/10), the plaintiff filed suit to recover damages for substantial injuries he allegedly sustained during a stock car race. The defendant asked in discovery for the names of any social networking sites to which the plaintiff belonged, along with users names, logins, passwords. The plaintiff objected, claiming that his Facebook and MySpace user names and login information were confidential. The trial court disagreed, and ordered the production: “Where there is an indication that a person’s social network sites contain information relevant to the prosecution or defense of a lawsuit, ... access to those sites should be freely granted.” It relied, in part, on Facebook’s terms and conditions, which the court concluded dispelled any notion that information one posts on Facebook is private:

Yet reading their terms and privacy policies should dispel any notion that information one chooses to share, even if only with one friend, will not be disclosed to anybody else.... Facebook users are thus put on notice that regardless of their subjective intentions when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion. Implicit in those disclaimers, moreover, is that whomever else a user may or may not share certain information with, Facebook's operators have access to every post....

The court also found that the relevancy of social networking information outweighed the potential of harm from the disclosure of that information.

Furthermore, whatever relational harm may be realized by social network computer site users is undoubtedly outweighed by the benefit of correctly disposing of litigation. As a general matter, a user knows that even if he attempts to communicate privately, his posts may be shared with strangers as a result of his friends' selected privacy settings. The Court thus sees little or no detriment to allowing that other strangers, i.e., litigants, may become privy to those communications through discovery....

Millions of people join Facebook, MySpace, and other social network sites, and as various news accounts have attested, more than a few use those sites indiscreetly.... When they do and their indiscretions are pertinent to issues raised in a lawsuit in which they have been named, the search for truth should prevail to bright to light relevant information that may not otherwise have been known.

In the *New York Times Magazine*, Walter Kirn made the following observation about the intersection between social networking and the loss of personal privacy:

As the Internet proves every day, it isn't some stern and monolithic Big Brother that we have to reckon with as

we go about our daily lives, it's a vast cohort of prankish Little Brothers equipped with devices that Orwell, writing 60 years ago, never dreamed of and who are loyal to no organized authority. The invasion of privacy—of others' privacy but also our own, as we turn our lenses on ourselves in the quest for attention by any means—has been democratized.

*As McMillen illustrates, by choosing to sacrifice our personal privacy through social interactions on social websites, we are also choosing to sacrifice our right to protect those interactions from discovery.*