A LAWYER'S GUIDE TO THE TOP 13 SOCIAL MEDIA ISSUES

By

Sharon P. Stiller, Esq.

Introduction

For most people, including employees, a day does not go by without accessing a social media site.

Employees may frequent social media sites, even while at work. Social media sites include Facebook, Twitter, My Space, You Tube, LinkedIn, Foursquare and Plaxo. Other social media sites include Orkutin Brazil and India, QQin China, Skyrockin France, VKontaktein Russia, Cywoldin South Korea, and Muxlim, which focuses upon Muslim society. The methods of communicating vary from blogs, to wikis, to instant messaging (IM), text messaging, and use of sites such as ResearchGATE for scientists and researchers.

Businesses are also using social media extensively. They may use it to promote and market a business and to build their brand.

Kodak's Chief Marketing Officer explains it well in Kodak's *Guide to Social Networking*:

> *"Why do I take the time to use social media like Twitter and Facebook? Because in today's media landscape, it's vitally important to be where our customers are. Kodak has always embraced this marketing philosophy, and today that means being active in social media.*
>
> *"The exciting thing about social media is it offers the opportunity to engage in two-way conversations with your customers. What better way to know how to best serve your customers than to hear directly from them? Social media has enabled new ways to initiate conversations, respond to feedback and maintain an active dialogue with customers."*

http://www.kodak.com/US/images/en/corp/aboutKodak/onlineToday/Social_Media_9_8.pdf

Businesses also may use social media defensively by defending against potential negative communications about the business in the workplace.

In this context, the ease of utilizing social media and the speed at which items are posted greatly enhances the potential for damage. For example, in 2009, a Michigan mayor accidentally posted a link to sensitive employee information on this Twitter account. His pot linked to a report that had personal information on 65 city employees, including the Social Security numbers of six of those employees. The report also included information regarding wages and other garnishments.

Twitter is a service that allows users to send messages of up to 140 characters known as "tweets" to its web site and directly to interested users or "followers" who subscribe to get updates from a particular user. The City responded to the security breach by providing employees with a free subscription to an identity theft protection service.

What happens when technology collides with employer regulation of conduct at work or conduct that affects work or customers? This article explores some of the common issues.

Issue 1: Must an Employer monitor e-mail?

While it is unlikely that a court will require that an employer monitor e-mail, it is unwise not to monitor email. The reasons for doing so are many.

An employer cannot ignore harassment in the workplace or close its eyes to what is rampant. In 1997, for example, Chevron Oil Company paid $2.2 million to settle a sexual harassment lawsuit brought by female employees who alleged that the company had permitted employees to use its e-mail system to disseminate sexually offensive materials, including a message discussing the *"25 Reasons Beer is Better than Women."* In the author's own practice, it is common to find e-mails attached as "evidence" in many hostile environment lawsuits.

It is therefore important to be aware of what is happening at the workplace, and monitoring helps employers to accomplish this.

Moreover, if an employer is charged with knowledge of what is happening at the workplace, it will also be charged with obviating the inappropriate behavior, so effective monitoring is needed to create effective remediation. The New Jersey Superior Court has held that *"an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activity, lest it result in harm to innocent third-parties."* **Doe v. XYC Corp**., 382 N.J. Super. 122, 887 A.2d 156 (App. Div. 2005).

This, of course, means that if an employer takes on the duty of monitoring, it must actually do so, and then take prompt and effective remedial actions if inappropriate conduct is revealed.

Issue 2: Can employers monitor an employee's use of personal e-mail at work?

Employers can monitor work-related e-mail. While the Electronic Privacy Communications Act protects electronic communications from interception, it generally does not prevent an employer from intercepting e-mails or other electronic communications because the exceptions permit monitoring with consent, or by the provider of services, and permits intra company communications. In **Fraser v. Nationwide Mutual Ins. Co**., 352 F.3d 107 (3d Circ. 2003), the court rejected a defense that the employer had improperly intercepted e-mails.

It is a good idea for an employer to have a policy that e-mail is for work use only (although this is an oft-debated question) and permitting monitoring of all e-mails. Some employers go so far as to have a logon which provides that: *"I hereby consent that all information and communications may be monitored."*

The question becomes more difficult when an employee accesses personal e-mail at work. The pivotal issue is whether the employee has a reasonable expectation of privacy in the personal account, if used at work. Establishing a reasonable expectation of privacy has proved difficult for employees, particularly if an employer has a policy prohibiting the use of personal e-mail at work. See, e.g., **United Sates v. Hassoun**, 2007 W.L. 141151 (S.D. Fla. 2007) (in light of employer's written policies, employee had no reasonable expectation of privacy in his office computer); **Garrity v. John Hancock Mutual Life Ins. Co**., 2002 WL 974676 (D. Mass. 2002 (employee had no reasonable expectation of privacy, even though folders were marked personal). See also **U.S. v. Butler**, 151 F. Supp. 2d 82 (D. Me. 2001) (there was no reasonable expectation of privacy in a computer that was part of a university network system).

Nonetheless, some emails may be off limits no matter what, such as those emails between an employee and counsel. In **Stengart v. Loving Care Agency Inc.**, 201 N.J. 300, 990 A.2d 650 (N.J. 2010), the appeals court rules that a company that was sued by a former employee alleging sexual harassment and constructive discharge was not entitled to read and copy pre-suit emails that the employee exchanged with her attorneys through her personal email account while using a company computer. The emails were drafted on the Company's computer, and the Agency's email policy confirmed that there was no privacy in emails on the company computer.

Issue 3: Can an Employer monitor an employee's social media use?

Similar to monitoring e-mails, an employer can monitor an employee's social media use, so long as it does not violate any statute or ethics rule. Courts have upheld terminations resulting from an employer's monitoring of an employee's social media discussions.

But employers must be careful about surreptitious conduct. Employers and attorneys alike have suffered adverse consequences from surreptitiously monitoring social media use, when they have had to engage in subterfuge or duress in order to access the media.

Some state laws as well as the federal Stored Communications Act (SCA), 18 U.S.C. § 2701, prohibit intentionally accessing or exceeding authorization to access a facility in which an electronic communication is provided and thereby obtaining access to an electronic communication stored in the system.

In 2009, a Newark, New Jersey jury found that restaurant managers who surreptitiously monitored employees' postings in a MySpace gripe group violated state and federal laws protecting the privacy of Web communications. **Pietrylo v. Hillstone Restaurant Group**, 2009 WL 3128420 (D.N.J. 2009).

Two servers were fired for criticizing their employers in the postings. The jury found that the restaurant violated the SCA as well as the New Jersey Wiretapping and Electronic Surveillance Control Act, N.J. S.A. 2A:156A-27.

The postings called managers "stupid corporate fucks" and "dick suckers", among other things. However, a password was needed to enter the forum. Although the employer claimed that another employee consensually provided the password, the fired employees' attorney argued that the employee only gave up her password under duress.

The court found that sufficient evidence supported a finding that the managers violated the SCA by knowingly accessing a chat-group on a social media website without authorization. Evidence indicated that although the witness had provided her log-in information to her manager, she had not authorized access by the managers to the chat-group, she felt she had to give her password to the manager, she would not have given the information to other co-workers, and she felt she would get in trouble if she did not provide her password. Evidence demonstrated that the managers accessed the chat-group on several occasions, even though the chat-group was intended to be private and accessible only to invited members.

A recent decision from the U.S. Court of Appeals for the Fourth Circuit allowed punitive damages under the SCA, even absent a showing of actual damages where an employer had accessed an employee's personal email account after she left the company, without the employee's authorization. **VanAlstyne v. Elec. Scriptorium Ltd.**, 560 F.3d 199, 28 IER Cases 1441 (4th Cir. 2009);

A similar conclusion was reached by the Philadelphia Bar Association's Professional Guidance Committee, which issued an advisory opinion on the question of whether a lawyer could, within the bounds of the Rules of Professional Conduct, ask another person to contact a witness on Facebook or MySpace in order to "friend" them and gain access to the information on their personal profiles. The Committee found that the proposed conduct would violate ethical prohibitions against misconduct and requirements for truthfulness in statements to others. See **Philadelphia Bar Ass'n Professional Guidance Comm'ee Opn.** 2009-02 (March 2009).

Interestingly, more surreptitious conduct may be occurring than we realize. Apparently, surreptitiously operating government agencies can access social media as an investigatory tool. Recently, the Electronic Frontier Foundation, a San Francisco based civil liberties group, obtained a 33-page document demonstrating that the FBI was engaged in covert investigations on social media services

In addition to not gaining access surreptitiously, an employer cannot use information gathered from social media in order to screen out applicants based on a protected category. Also, an employer cannot violate statutory privileges in obtaining the e-mails, such as the attorney client privilege. **Stengart v. Loving Care Agency Inc**., supra, 201 N.J. 300, 990 A.2d 650 (N.J. 2010)

Issue 4: Can an employer terminate an employee because of social media content?

On May 3, 2010, syndicated newspapers published a column which read as follows:

> "Dear Abby:
>
> My wife was hired for an administrative position. On her first day of work, they called her into the human resources director's office and told her she was being "let go" because of her website.
>
> The site has photos of her when she worked as a model for a large department store. They are in no way provocative or overly revealing. Photos of our children are also on the site.
>
> The HR director told her that one of the other (internal) applicants had Googled her and had seen the site. An image so upset the other applicant that she made a formal complaint, which caused my wife's dismissal!
>
> We consulted a lawyer and contacted the local Equal Employment Opportunity Commission only to be told that North Carolina is an "at will" employment state and that the employer did nothing wrong. We feel their actions were wrong. Is there anything that can be done? – Yankee in Confederate County
>
> "Dear Yankee:
>
> I'm sorry, but the answer is no. In most states there is a presumption of "at will" employment unless you have a written contract to the contrary. However, the employer cannot terminate an employee for an illegal reason – such as age, religion, gender, sexual orientation or a disability. It does not appear from your letter that your wife was terminated for an illegal reason, but what happened stinks anyway."

Termination for this type of conduct is not uncommon. In fact, a survey by the American Management Association in 2006 reported that 26% of employers had terminated an employee for violating the employer's e-mail policies; this was a 9% increase of the 17% termination rate reported in 2001. As many as 34% of employers fired workers for excessive personal use of the Internet.

Here are some of the most recent cases permitting termination for internet, e-mail or social media content:

Marshall v. Mayor and Alderman of City of Savannah, 2010 WL 537852 (11th Cir. 2010) : The 11th Circuit upheld a district court decision that a probationary firefighter failed to plead a retaliation claim based on gender, when the fire bureau chiefs met with her to discuss reprimanding her for posting

official photographs of bureau employees on her personal internet pages along with scantily clad photographs of herself.

These photos included a picture of firefighters from the Department, which she obtained without permission from the city's web site. Marshall labeled this picture "Diversity." Another photograph, captioned "Fresh out of the shower," depicted her posing bare-shouldered. The other revealed Marshall's backside. According to the record, it apparently was difficult to tell what clothing, if any, she was wearing. She titled that picture, "I model too--this is from like my second shoot!"

The Department learned about Marshall's MySpace photographs from an anonymous caller in February 2007. The caller suggested that the social network account contained images that "may conflict" with the way the Department wanted to be portrayed. She was issued a written reprimand for violating Department policy, and then ultimately terminated for her "denial" of violation of the Fire Department's policy. She claimed that her termination violated her First Amendment right "to freely communicate on a completely personal basis where no real or imagined damage" to her employer had been demonstrated. The court determined that her "speech" in disseminating photographs on her MySpace page was not entitled to First Amendment protection. The 11th Circuit also pointed out that she did not demonstrate that male firefighters were treated differently, and she was fired for more than merely social network postings.

Pacenza v. IBM Corp., 2010 WL 346810 (2nd Circ. 2010): Summary judgment in favor of the employer was upheld, where the 54-year old employee who suffered from post- traumatic stress disorder, was fired purportedly because he violated company policies by accessing sexual materials on the internet while at work. The Court held that the employer's reason for termination was legitimate and non-discriminatory and was not shown to be pre-textual. The conduct was a clear violation of IBM's policies, and there was no showing that he was singled out or treated more harshly than similarly situated non-disabled employees.

Calandriello v. Tennessee Processing Center, LLC, 2009 WL 5170193 (M.D. Tenn. 2009): The Court dismissed a discrimination claim, finding a sufficient non-discriminatory reason for his termination based upon loss of confidence resulting from an allegedly bipolar employee's (1) admitted viewing of military and violent web sites (including ones providing news about serial killers) on his work computer; and (2) altering an inspirational poster to say that the image of a well known serial killer was inspirational. The employee had claimed that his use of the Internet did not violate company policy because he was "told by my supervisor to surf the internet when I had no project to work on" and other employees were constantly searching the Internet.

Cervantez v. KMGP Services Co. Inc, 349 Fed. Appx. 4 (5th Circ. 2009): The Court found that violation of the employer's computer use policy which prohibited access to pornographic sites, was a legitimate reason for discharge and that the employee failed to show that this was pre-textual. In language that may prove helpful in these types of cases, the Court noted that the fact that the logs produced by the employer were inconsistent did not prevent summary judgment, since actual innocence is irrelevant if the employer reasonably believed the proffered reason and acted in good faith.

County of Sacramento, 118 Lab. Arb. Rep. (BNA) 699, 702 (2003) (Riker, Arb.): In a union setting, the Court will consider the equities despite the employer's policy. In one case an employer promised an employee confidentiality when interviewing her as part of a sexual-harassment investigation. The employee disclosed that she had used an internal computer system to send sexually explicit messages to a co-worker. The interviewer stated that the information she provided would not "be reported to her supervisor or co-workers, unless there was a need to know." The arbitrator reasoned that the one-day-suspension of the employee should be reduced to a written reprimand, in part because it was based on her confidential disclosures.

Schools are not immune from these issues; in some respects, conduct is scrutinized even more when children are involved.

In **Snyder v. Millersville University et al**., Case No. 07-1660 (E.D. Pa. 2007), a student was denied an educational degree based on information that the school learned from the student's MySpace account. She posted an e-mail about the students she was student teaching and a supervising teacher, accompanied by a photo of herself in a pirate's cap holding a cup, and captioned with "drunken pirate." When she was rated unsatisfactory in her student teaching and denied a degree, she sued, claiming violation of her free speech rights among other claims. In another incident, it was reported that a Sociology professor was escorted off the campus of East Stroudsburg University. The Newspaper reported that in February, 2010 the associate professor had posted on her Facebook page, "Had a good day today, didn't want to kill even one student." Earlier, she had written, "Does anyone know where I can find a very discrete hitman, it's been that kind of day." Chronicle of Higher Education, 2/28/2010 .

In **A.B. v. State**, 863 N.E.2d 12212 (Ind. Ct. App) (Indiana Ct. App) a minor posted expletive filled comments on a MySpace page purportedly in the name of the middle school principal; when he was held as a juvenile, the court found that the comment was political speech aimed at the principal's policies and protected under the Indiana constitution. But in **Ladyshock v. Hermitagge School Dist**., 412 F. Supp. 2d 502 (W.D. Pa. 2006) and **J. S. v. Blue Mountain School Dist**, 2007 WL 954245 (M.D. Pa. 2007), where the students posted MySpace comments on pages purportedly in the names of the principals, the punishment was upheld.

The rules may be different for public employees, who enjoy a free speech right. See., e.g., **Richerson v. Beckon, 337 Fed. Appx**. 637 (9th Circ. 2009) (teacher disciplined for blogging about what it was like inside a school district; here transfer did not violate her First Amendment rights since the speech had a significantly deleterious effect).

Issue 5: Is it legally permissible to use the internet or social media to conduct background checks?

Employers commonly perform "Google" searches of applicants as part of the reference check process. A 2009 CareerBuilder survey found that 45% of employers report that they use social media

sites to research job candidates. It has been estimated that at least 50 million individuals in the U.S. maintain "blog" diaries of their daily activities and at least 100 million post profiles on social media sites. These sites are commonly used to check up on an applicant.

Why is it important to verify credentials? The answer is that it is remarkable how many employees lie about their credentials. In 2002 Bausch & Lomb's chief executive, Ronald Zarella, was found to have lied about having a master's degree in business administration from NYU. Kenneth Lonchar, finance chief of Veritas Software, resigned in 2002 after the company learned he misstated his educational credentials, including falsely claiming to hold an MBA from Stanford. Sandra Baldwin, president of the U.S. Olympic Committee, left office in 2002 after admitting she lied about having a Ph.D. in English (she never actually completed her dissertation). See White Lies on Resumes Raise Red Flags for Employers - Investing - Economy - SmartMoney.com http://www.smartmoney.com/investing/economy/white-lies-on-resumes-raise-red-flags-for-employers-21201/?hpadref=1#ixzz0nTJWEr6O

According to the 2009 Screening Index released by ADP, a human-resources and payroll provider, 46% of employment, education or credential reference checks conducted in 2008 revealed discrepancies. That's up from 41% in 2006.

Because information posted on the Internet is voluntary, employers generally are not restricted from accessing information. However, employers may not engage in misrepresentation or surreptitious means to gain entry to a site deemed to be private, as explained in more detail in the beginning of this article.

Some of the most common reasons for rejecting applicants based on Internet background checks are:

Candidate posted provocative or inappropriate photographs or information: 53%

Candidate posted content about drinking or using drugs: 44%

Candidate made derogatory statements about their previous employer, co-workers or clients; 35%

Candidate demonstrated poor communication skills: 29%

Candidate made discriminatory statements: 26%

Candidate lied about qualifications: 24%

Candidate shared information from a previous employer: 20%

On the other hand, some employees have been hired because of their online profiles. Some of the reasons include:

Candidate's profile demonstrated personality and a good fit: 50%

Candidate's profile supported the applicant's professional qualifications: 39%

Candidate was creative: 38%

Candidate showed solid communication skills: 35%

There are restrictions set forth under the Fair Credit Reporting Act , 15 U.S.C. § 1681 et seq. to obtaining background information without an employee's permission. The FCRA only applies when outside third parties are used to collect the information, and the provisions may readily be complied with by obtaining the employee's consent for a background check. In 2003, Congress passed the Fair and Accurate Credit Transactions Act ("FACT") which specifically excludes from the definition of consumer report an investigation of: (1) suspected misconduct relating to employment; and (2) compliance with federal, state or local laws and regulations or any preexisting written policies of the employer.

Along with complying with the Fair Credit Reporting Act, employers must always remember that just as they cannot negatively use information about a protected category related by the applicant, so, too, employers are prohibited form taking adverse action based upon a protected category learned through viewing social media.

Issue 6: Do laws controlling an employee's off-duty conduct impact upon an employer's ability to use social media, or to terminate for the content of an employee's social media? What about off-duty conduct laws or searches involving public employees? Does it matter if the employer's equipment is used?

Several states protect off-duty conduct. New York, for example, has a "lawful activities" law, which protects employees engaging in recreational or certain political activities off duty, while not using work equipment, or work property. See N.Y. Labor Law § 201-d. Other states with similar laws include California (Cal. Lab. Code §§ 96(k), 98.6; Illinois (820 Ill. Comp. Stat. § 55/1-120 (limited to use of lawful products); Minn. Stat. § 181.938 (limited to lawful consumable products); Wisc. Stat. § 111.321.

To date, it is unclear whether anyone has attempted to use these statutes to protect their off-duty communications. To provide protection, it will have to be found that use of social media constitutes a recreational or political activity, which is not much of a stretch. However, to the extent that the communication is made at work or involves work-related activities, it may not find protection under these laws.

There are also Fourth Amendment and free speech protections available to public employees. The parameters of some of the protections will soon be set by the United States Supreme Court when it decides the case of **City of Ontario v. Quon**, 130 S.Ct. 1011, 77 USLW 3619, 78 USLW 3011, 78

USLW 3356, 78 USLW 3359 (2009). The United States Supreme Court has granted certiorari to determine whether there is a reasonable expectation of privacy in sexually explicit personal text messages transmitted on pagers provided by the police department in connection with work. The employees claimed that acquiring transcripts of the messages constituted an unreasonable search in violation of the Fourth Amendment. Oral argument took place in April, 2010.

Issue 7: Can an employer regulate whether employees spend work time visiting social media sites?

A 2009 survey conducted by Deloitte LLP concludes that 55% of all employees visit social media sites at least once a week. However, only 20% of the employees admit visiting these sites during working hours.

Unless a state statute prohibits monitoring work time, there is no other impediment to an employer monitoring how much time employees spend on productive activities or on non-productive activities, such as visiting social media sites.

In addition, in some contexts, the employee's job duties may require visiting social media sites. For this reason, if the employer is using social media as part of its own marketing strategy, it will need to consider the need for employees to be involved in that strategy in developing an appropriate policy on usage.

Issue 8: Can an employer be held liable for an employee's conduct on a network?

The FTC has issued regulations that set forth strict regulations on employees' use of social media to discuss a product or service offered by an employer. 16 CFR § 255.1(d) (2009) The Guidelines provide that:

> *"Advertisers are subject to liability for false or unsubstantiated statements made through endorsements, or for failure to disclose material connections between themselves and their endorsers. Endorsers also may be liable for statements made in the course of their endorsements."*

Under these guidelines, an employee must disclose his or her relationship, each time s/he endorses an employer's product or service. A positive comment on Twitter or Facebook could be deemed to be an endorsement if it "reflects [the employee's] opinions, beliefs, or experiences" about the employer's product or service.

The guidelines apply to endorsements made using "new media" such as blogs

and social media sites, and FTC enforcement actions could be brought against a company whose employees comment on company products for services without disclosing the employment relationship.

The practical import, then, is that the employer should prohibit all communications about products or services or at least prohibit communications without the employer's approval and prior consent. In addition, the policy should require that if an employee makes any comment, the employee must disclose the employee's relationship with the employer. Last, the policy should provide that all employees must report any communications coming to their attention that violate the policy.

Similarly, the SEC in a guidance issued in 2008 (Release No. 34-58288 (August 1 2008) made it clear that a company employee "speaking" from a company interactive forum may never be deemed to be acting in an individual capacity, so that the company may be liable for all employee statements made in that capacity.

Issue 9: Can an employer restrain an employee or ex-employee from defaming the employer on a network?

`While an employer may validly terminate an employee for making derogatory comments about the employer on the internet (See **Varian Med. Sys., Inc. v. Delfino,** 113 Cal. App. 4th 272 (2003), rev'd on other grounds (holding that an employer may terminate an employee who posted derogatory comments about the company and company executives), **get up to date cases** the courts are loath to grant injunctions prohibiting employee speech in advance of the speech.

In **Ramos v. Madison Square Garden Corp**, 257 A.D.2d 492 (1st Dept. 1999), the court refused to grant an injunction against an employee's defamatory statements, on the ground that there is an adequate remedy at law (post-publication damages) and relief in the nature of prior restraint is disfavored. But see **Aguilar v. Avis Rent-A-Car System, Inc.**, 21 Cal. 4th 121 (Cal. 1999) (granting a limited workplace injunction prohibiting racial epithets in the workplace).

Issue 10: Can an employer obtain damages from a network site for disparaging comments made by an employee?

In general, the Communications Decency Act of 1996 ("CDA"), 47 U.S.C. § 230 et seq. provides immunity to operators of websites in most situations involving communications by third parties. In **Doe v. MySpace, Inc**., 474 F. Supp. 2d 843 (W. D. Tex. 2007), the court held that these immunity provisions insulated the network from liability for a negligence claim alleged by the victim of sexual abuse by an online predator.

Issue 11: Are there any special issues involved when employees illegally post trade secrets or confidential information?

Even in cases where an employee allegedly misappropriated trade secrets and was in danger of posting copyrighted material, the court found that enjoining the posting would violate the First Amendment as a prior restraint. **Ford Motor Co. v. Lane**, 67 F. Supp. 2d 745 (E.D. Mich. 1999). But there can be tremendous repercussions if employees or former employees post trade secrets or confidential information.

If employees post copyrighted material on an employer-operated blog and permission hasn't been given by the copyright owner nor is it a "fair use" under the Copyright Act, thereby exposing the employer to potential liability, the owner can request the removal of infringing content.

While there may be some common law protection, employers should have confidentiality agreements with employees, which should prohibit disseminating confidential information of the employer as well as the employer's clients or customers. Moreover, the agreement and/or policies should explicitly prohibit posting any confidential information on any Internet site, or removing or copying it.

Issue 12: Are there any special protections available or other considerations for union employees?

The NLRB has held that an employer does not violate the NLRA by having a policy prohibiting employees from using e-mail for non job-related solicitations. **The Guard Publishing Co. d/b/a The Register-Guard**, 351 NLRB No. 70 (12.16/2007). See, e.g., **City of Okmulgee**,124 Lab. Arb. Rep. (BNA) 423, 430 (2007) (Walker, Arb.) ; **Kuhlman Elec. Corp.**, 123 Lab. Arb. Rep. (BNA) 257, 262 (2006) (Nicholas, Arb.). (new policy on use of computers and internet is not contrary to CBA and does not materially, substantially, and significantly affect the terms and conditions of employment).; But see California Newspaper Partnerships, 350 N.L.R.B. No. 89 (Sept. 10, 2007) (employer must bargain with union over policy forbidding use of e-mail accounts to send messages about union affairs).

In **Konop v. Hawaiian Airlines**, 302 F.3d 868 (9th Circ. 2002) a pilot claimed he was wrongly disciplined and was critical of labor concessions on his blog. The Ninth Circuit Court of Appeals found that the content of the blog represented protected union activity and lacked the actual malice needed to make it defamatory.

Employees have been disciplined for conduct involving the internet, even though the employee is a union member. See, e.g., **Dep't of Veterans Affairs**, (Hoffman, Arb.) (supervisor observed grievant repeatedly using computer for non-work related matters and calling other employees over to view his computer or announcing news to them and so requested a review of his internet usage); **Dept. of Veterans Affairs**, (Petersen, Arb.) (e-mails evidencing a slowdown were discovered when someone alleged harassment and defamation; the arbitrator reduced the discharge to a written

reprimand because that was the penalty for a slowdown under the employer's progressive discipline policy); **Tesoro Ref. & Mktg. Co.**, 120 Lab. Arb. Rep. (BNA) 1299, 1303 (2005) (investigation where employee posted hate group poster with listed URL); **A.E. Staley Mft. Co.**,A.E., 119 Lab. Arb. Rep. (BNA) 1371 (2004) (Nathan, Arb.); **MT Detroit**, 118 Lab. Arb. Rep. (BNA) 1777 (2003) (Allen, Arb.) ("chat room" operator informed company that an employee had posted a message containing offensive racial language); **State of Minn**., 117 Lab. Arb. Rep. (BNA) 1569 (2002) (Neigh, Arb.) (extensive investigation of chain of pornographic e-mails and related computer use based on complaint from one employee that she viewed a naked woman on co-worker's
Computer screen).

The same issues arise in relation to union members' conduct when that conduct takes place through using electronic methods of communication. There may be secondary picketing issues if mass e-mails are sent to employees by others soliciting membership or support or if employees use e-mail to put economic pressure on a secondary employer to stop doing business with a primary employer.

Issue 13: Should employers have a policy? If so, what should it contain?

Of course, the best practice is to have a policy which addresses not only computer use, licensing and access to the internet, but also the new issues evolving concerning social media. However, it is not sufficient to simply have a policy. It is incumbent upon employers to have a policies that actually reflect what it does and to enforce their policies, as well as to train employees regularly about what is expected and what is prohibited. Policies related to these issues include a workplace anti-harassment policy (including using the computer, internet or social media), a computer and e-mail policy (including cell phones, if company issued, and prohibiting personal use of the computer at work), a social media policy prohibiting use of company logos, trademarks or names or making statements about the company except as authorized by the company, a confidentiality and trade secrets policy, a no solicitation, no distribution policy, and a noncompetition policy if enforceable in your jurisdiction. There is no one-size-fits-all policy for every employer, since, for example, an employer who is using social media as part of its own strategy will need to take that into account in developing appropriate policies.

Fundamental aspects of a policy depend on the organization, but should include:

1. Employees should be warned against any postings which contain:

a. Confidential information: Employees should be warned that they must keep the employer and customers' proprietary information confidential;

b. Discriminatory statements or sexual innuendos regarding anyone associated with the employer (including customers);

c. Defamatory or derogatory statements about anyone associated with the employer (including colleagues and customers);

d. Any illegal conduct using the computer or software; and

e. Endorsements of company products or services.

2. Policies should also warn:

a. Against using company logos, or other identifying marks without company permission;

b Making any reference to company services or products;

c. Adding any unlicensed software to the company's computer systems;

d. Adding any software to the company's computer system without company approval;

e. Accessing any personal or inappropriate sites from work, including but not limited to pornographic or dating sites;

f That all use of the computer during work may be monitored and there is no privacy right in any account or information accessed during work or from the work related computer;

g Requiring review of any material before it is posted on the employer's website;

h. Prohibiting copying other material to publish on the employer's website;

i. Requiring professionalism in all postings and publications; and

j. That all computer use may be monitored.

3. Employees should also be required to:

a. Provide all passwords for accounts used during work time to management;

b. Report all violations of company policy;

c. Obtain management approval before sharing any data; and

d. Obey all standards for linking.

4. Managers should be warned against any postings which contain:

a. An informal review of an employee such as recommending someone on LinkedIn or "friending" a subordinate on Facebook; and

b. Making any statements about colleagues on a social media site.

Conclusion

Social media is a powerful tool and it can be powerful weapon. We are just beginning to develop the rules of engagement governing conduct relating to social media. This article contains some of these rules but certainly more will develop, as we attempt to harness this powerful tool in a way that is fair to both employers and employees.