Journal of Collective Bargaining in the Academy

Volume 0 *NCSCBHEP Proceedings 2011* Article 33

April 2011

The Developing Law Governing Employee and Employer Rights Relating to Use of Electronic Media Within and Outside the Workplace

Stuart W. Davidson Esq.
Willig, Williams & Davidson LLP

Amy L. Rosenberger Esq.
Willig, Williams & Davidson LLP

National Center for the Study of Collective Bargaining in Higher Education and the Professions
38th Annual National Conference

NEGOTIATIONS 103

COLLECTIVE BARGAINING IN THE BRAVE NEW WORLD:
Exploring the Impact Of Electronic Media On Negotiations, Protected Activity, And Privacy in the Modern Workplace

The Developing Law Governing Employee and Employer Rights Relating to Use of Electronic Media Within and Outside the Workplace

STUART W. DAVIDSON, ESQUIRE
AMY L. ROSENBERGER, ESQUIRE[1]
Willig, Williams & Davidson
1845 Walnut Street, 24th Floor
Philadelphia, PA 19103
www.wwdlaw.com

[1] The presenters gratefully acknowledge the assistance of their colleague, Lauren M. Hoye, Esquire, in preparing this paper.

Employees are using electronic media at an increasing rate to communicate with others both in and out of the workplace. While email, social networking sites, blogs, text messages, and online videos may seem to present new and complex challenges for employees and employers, the decisional law suggests that the key to understanding issues presented by electronic media use is to reason by analogy to more "traditional" means of communication. For example, an email string between two people or among a group may be viewed similarly to an in-person conversation; the former is just memorialized in writing. A comment posted on an employee's Facebook page may be treated like a verbal comment made by an employee to friends and coworkers. The same fundamental questions come up in the cases involving traditional or electronic communications: What was communicated? Who communicated it? When was it communicated? To whom was it communicated?

The purpose of this paper is to provide an overview of how the National Labor Relations Board ("NLRB" or "Board") and the courts are applying existing rules about employee communications and activity to electronic media. This paper focuses in particular on protected activity under the National Labor Relations Act ("NLRA"), issues of employee privacy rights, and First Amendment issues.

I. PROTECTED ACTIVITY UNDER THE NLRA

Often, the issue of protected concerted activity arises in the context of employee efforts to organize. However, the NLRA's protection extends beyond the context of representational activities, as is evident in the language of Section 7 of the NLRA, providing that employees shall possess "the right to self-organization . . . to engage in other concerted activities for the purpose of . . . mutual aid or protection." This right is enforceable under Section 8(a)(1) of the NLRA, which prohibits employers from interfering, restraining or coercing employees who exercise their rights under Section 7. At the intersection of protected activity and electronic media, several common misconceptions exist.

- **Myth #1: Employees are legally permitted under the NLRA to use employer email systems for union business.**
- **Reality: Employees have no statutory right of access to employer email systems for purposes of conducting union business.**

In Register Guard, 351 NLRB 1110 (2007), review granted in part and remanded, Guard Publishing Co. v. NLRB, 571 F.3d 53 (D.C. Cir. 2009), the Board held that employees have no statutory right under the NLRA to use an employer's email system for Section 7 matters. The Board explained that an employer has a "basic property right" to "regulate and restrict employee use of company property." 351 NLRB at 1114.

The Board upheld the discipline of a union member who used the employer's email system to disseminate union information. In the process, the Board created a standard for the discriminatory enforcement of email solicitation policies that essentially provides that to be unlawful, disparate treatment must involve communications "of a similar

character." Id. at 1118. Essentially, the Board concluded that an employer could restrict email pertaining to the union even if it allowed email for other uses, so long as the employer's prohibition was applied against solicitations for all groups and organizations. Therefore, the fact that employees in Register Guard had used the email system to send "personal," as opposed to "organizational," solicitations, including party invitations and baby announcements, did not impact whether the employer discriminated against the union member for using the email system to send an "organizational" union announcement. "[N]othing in the Act prohibits an employer from drawing lines based on a non-Section 7 basis." Id.

In July 2009, the Circuit Court for the District of Columbia rejected the Board's disparate treatment standard and remanded the case to the newly-constituted Board for articulation and application of an appropriate standard. See Guard Publishing Co. v. NLRB, 571 F.3d 53 (D.C. Cir. 2009). The court viewed the line drawn by the Board barring access to employer email based on the "organizational" purpose of the union as a "post hoc invention." Id. at 60. Further, the employer's own policy made no such distinction between "personal" solicitation and "organizational" solicitations.

Even if the Register-Guard rule survives in some form on remand, it does not restrict a union, once it becomes the employee representative, from bargaining for a contractual right to use employer email systems for union-related business. Unions have long bargained for the right to use employer property, including bulletin boards, mailboxes, and meeting rooms, to conduct union business or distribute union information.

It is worth noting, however, that using employer email systems for union business presents unique problems in that workplace email policies often expressly reserve to the employer the authority to monitor the content of employee emails. The result is that while unions may negotiate for the right to use employer email to conduct union business, they should be careful about using employer email to communicate about information that they wish to remain confidential. Indeed, unions that do successfully negotiate for use of employer email systems should treat employer email as they would other public forums, such as an employer bulletin board.

- **Myth #2: Under the NLRA, employees have a legal right to use social networking sites (i.e., Facebook, MySpace, Twitter, blogs, etc.) to vent about work.**
- **Reality: The NLRA protects communications regarding workplace issues through channels outside of the employment, so long as there is a direct nexus between the communications at hand and employment related concerns, and the comments are not egregious or reckless in nature.**

In a recent Board case (often referred to as "the Facebook Case"), an employee posted a series of disparaging remarks about her supervisor on her Facebook page. The employee's Facebook friends, including several of her coworkers, viewed and commented on her post, expressing their support and adding additional negative comments about the supervisor. The employer then discharged the employee.

The NLRB issued a complaint alleging that the employee was engaged in protected activity under Section 7 of the NLRA and that she had been fired in violation of Section 8 of the NLRA. The complaint also alleged (1) that the employer's rule regarding communications among employees, including online posting and blogging, was overly broad; and (2) that the employer violated the employee's rights when it refused to allow

her to have union representation during a meeting regarding her Facebook posts. The NLRB noted that the employer's policies prohibited employees from making disparaging remarks when discussing their employer or its supervisors, and from depicting their employer online without permission.

A settlement was reached in this case in February 2011. While the settlement agreement is confidential, the employer did agree (1) to revise its communications policies to ensure that they do not infringe upon employees' right to discuss their wages, hours, and working conditions; (2) not to discipline or discharge employees for engaging in those discussions; and (3) not to deny employee requests for union representation in the future. While the "Facebook case" resulted in settlement, what is clear is that the NLRB views employer policies interfering with employees' ability to talk about work on Facebook or other social media outlets as subject to scrutiny under the NLRA.

Note, however, that where the employer does not actually prohibit such disparaging comments, cautionary statements by management suggesting that employees be "careful" about what they post on social media outlets is not necessarily unlawful. In Salon/Spa at Boro, Inc., 2010 NLRB LEXIS 419, 356 NLRB No. 69 (2010), the Board held that an employer is permitted to advise its employees not to make "negative" comments about work on social media websites, so long as the employer's conduct is not coercive in nature. Where a manager made statements to employees warning them to be "careful" in their use of social networking media and where those statements were didactic, not coercive, in nature, there was no violation of Section 8(a).

In particular, the manager in Salon/Spa at Boro, Inc. reported to staff that "they needed to be kind and positive . . . there are a lot of other people reading their information, reading them that they may not even be aware that was reading what they were posting . . . So it's public." Id. The Board concluded that this warning was not referring to work in particular, but to life in general, and that the comments themselves could not be interpreted as intimidating or coercive. Rather, the Board held that the manager's comments (a) were meant to impress upon employees that their postings on social media websites were public and (b) that they should use judgment when making use of those websites. Because the purpose of the manager's comments was educational, not coercive, the Board held that they did not interfere with or restrain employees in their exercise of their statutory rights.

Likewise, when discussing work-related matters on social media outlets, employees must also bear in mind the duty of loyalty owed to the employer. Jefferson Standard, NLRB v. IBEW Local 1229, 346 U.S. 464 (1953), and its progeny govern allegations of disloyalty in employee communications. Under Jefferson Standard, as long as an employee's remarks relate to a labor dispute or workplace interests and are not egregious or reckless in nature, they are protected under the NLRA, even if widely publicized. In Stephens Media, LLC, 2011 NLRB Lexis 40, 356 NLRB No. 63 (2011), an Administrative Law Judge ("ALJ"), applying Jefferson Standard, held that an employee's comments on his blog regarding his former employer, a newspaper, did not rise to the level of disloyalty/disparagement when they were no more than a literary criticism of the employer's policies and there was no evidence that they were maliciously false.

In February, the full Board ruled that because these blog posts were made *after* the employee's unlawful discharge, the Jefferson Standard rule technically did not apply. The question was whether or not the employee should be denied reinstatement and/or back pay as a result of his post-discharge criticism of the employer. Recognizing that "employees who are unlawfully fired . . . often say unkind things about their former employers," the Board held that "[e]mployers who break the law should not be permitted to escape fully remedying the effects of their unlawful actions based on the victims' natural human reactions to the unlawful acts." As a result, the Board held that the standard adopted in 1969, in O'Daniel Oldsmobile, Inc., 179 NLRB 398 (1969), should apply. Under that standard, the question of whether an unlawfully discharged employee may be reinstated is whether the employee's conduct is "so flagrant as to render the employee unfit for further service . . . ."

Although the Board did not apply Jefferson Standard because the conduct in question in Stephens Media occurred after the employee was unlawfully discharged, the Board did not suggest that Jefferson Standard should not be applied to employee communications made via social media. The view that Jefferson Standard applies to posts made during employment is supported by an advisory opinion issued by the NLRB Office of General Counsel in December 2009. The advisory opinion recommended the dismissal of a complaint alleging that the employer's social media policy violated Section 7 of the NLRA. The policy prohibited employees from "disparag[ing] the company's or competitor's products, services, executive leadership, employees, strategy, and business prospects." The General Counsel was of the view that the policy could not reasonably be interpreted as prohibiting protected activity

because the activities set forth in the policy were not activities protected by Section 7. See 2009 NLRB GCM LEXIS 67 (Dec. 4, 2009).

Finally, just as in a more "traditional" context, to be unlawful, discipline for electronic media use must be issued in response to protected activity, and not for some other reason. In May 2010, the Office of General Counsel broached the issue of whether an employer violated Sections 8(a)(1) and (3) of the NLRA by disciplining employees based on Facebook postings. The opinion concluded that because the specific comments cited by the employer as the basis for the employees' discipline did not involve Section 7 concerns and were in no way related to the postings that did, the discipline did not violate the NLRA. See 2010 NLRB GCM LEXIS 51 (May 5, 2010). In particular, the employer became concerned about postings and comments on an employee's Facebook page suggesting that she, a nurse, and other employees may withhold care from hospital patients if they were personally offended by them. After reading these postings, the employer decided to suspend the employees.

Meanwhile, the employees had made other postings and sent emails regarding the terms and conditions of employment and ongoing labor disputes. For example, one of the employees had emailed union members regarding vehicle safety issues and disciplinary memos. One email contained the warning: "Remember, if . . . management lips are moving, they are lying." Because the discipline issued was based on the Facebook posts regarding withholding patient care, and not on the postings and emails regarding terms and conditions of the employment, the discipline was not violating the NLRA. In sum, the nurse's posts about withholding care, though arguably "work-related," were not protected because they did not "involve Section 7 concerns," in

contrast to her other communications. The underlying message of this opinion from the Office of General Counsel is that while communications pertaining to terms and conditions of employment – such as safety, discipline, or even distrust of employer communications – are protected, communications that are only peripherally related to work, but do not involve terms and conditions of employment, are not.

II. PRIVACY

For employees in the public sector, the Fourth Amendment, which prohibits unlawful searches and seizures, protects public employees' reasonable expectation of privacy in the workplace. The Fourth Amendment is only applicable, however, where the employer's conduct violates an "expectation of privacy that society is prepared to consider reasonable." O'Connor v. Ortega, 480 U.S. 709 (1987). At the intersection of privacy and electronic media, several common misconceptions exist:

- **Myth #3: A public employee has a reasonable expectation of privacy when it comes to technological equipment provided by his or her employer.**
- **Reality: A public employee may have a reasonable expectation of privacy when it comes to technological equipment provided by his or her employer, but it depends on the particular facts of the case.**

The "reasonableness" of an employee's expectation of privacy is determined on case-by-case basis. For example, in Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001), the Second Circuit Court of Appeals found that there was a reasonable expectation of privacy regarding a public employee's work computer where the employee occupied a private office and maintained exclusive use of the office, work computer, desk, and filing cabinet. Similarly, in U.S. v. Slanina, 283 F.3d 670 (5th Cir. 2002), cert. granted,

judgment vacated on other grounds and remanded, 537 U.S. 802 (2002), the Fifth Circuit held that a public employee had a reasonable expectation of privacy where the employee used a password protected computer in a locked office. While Slanina was a criminal case, the pornography recovered from the employee's computer was recovered in the course of a work investigation. The court, in determining whether the employee had a reasonable expectation of privacy on his work computer, assessed factors that would be relevant to the inquiry of whether any public employee has a reasonable expectation of privacy on her or his work computer: whether other employees had a key to the employee's office, whether the public employer had a regular need to access the employee's computer, whether the employer or the employee had purchased the computer, the lack of any employer policy preventing the storage of personal information on employer computers, and the fact that the employer never told its employees that their computer usage and internet access would be monitored.

However, in U.S. Barrows, 481 F.3d 1246 (10th Cir. 2007), also a criminal case, the court held that an employee who connected his personal computer to his employer's network without a password protecting his files had no reasonable expectation of privacy. The court explained that although this was a criminal case, the incident occurred in the workplace. Therefore, in its inquiry of whether the employee possessed a reasonable expectation of privacy in his work computer, the court took into account the employee's relationship to the item seized, whether the item was in the immediate control of the employee when it was seized, and whether the employee took actions to maintain his privacy in the item. Id. at 1248-49. Although the employee owned the computer, he had failed to password-protect it, turn it off when he left the room, or take

any other steps to prevent third party use. Accordingly, the court determined that the employee did not possess a reasonable expectation of privacy.

A public employer can create a reasonable expectation of privacy by notifying its employees that they can maintain private files on their computer. See, e.g., Haynes v. Office of the Attorney Gen., 298 F.Supp.2d 1154 (D. Kan. 2003); Maes v. Folberg, 504 F.Supp.2d 339 (N.D. Ill. 2007) (employee sufficiently pled that she had a reasonable expectation of privacy regarding files contained in her government-issued laptop computer because employer had no policies or procedures to suggest otherwise).

- **Myth #4: A warrantless search by a public employer is unconstitutional under the Fourth Amendment if the public employee has a reasonable expectation of privacy.**

- **Reality: When conducted for a "noninvestigatory, work-related purpose" or for the "investigation of work-related misconduct," a government employer's warrantless search is reasonable if it is "justified at its inception" and if "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of" the circumstances giving rise to the search.**

In City of Ontario v. Quon, 130 S. Ct. 2619 (2010), the employer, the City of Ontario, California, read employee text messages sent and received on an employer-issued pager, without obtaining a warrant. Without reaching the issue of whether the employee had a reasonable expectation of privacy in the messages, the Court found that the warrantless search did not violate the Fourth Amendment. In particular, the Court explained that there are "a few specifically established and well-delineated exceptions" to the general rule that warrantless searches are per se unreasonable under the Fourth Amendment. Id. at 2630. One of those exceptions is the "special needs" of the workplace.

The Court explained that the search was constitutional because:

- It was conducted for a noninvestigatory, work-related purpose or for the investigation of work-related misconduct;
- It was justified at its inception; and
- It was conducted according to measures that were reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search.

In particular, the search was justified at its inception because the employer needed to determine whether the character limit on the employer's text message contract with its wireless company was sufficient to meet the employer's needs. This was, according to the Court, a "legitimate work-related rationale." Id. at 2631. The employer, the Court explained, had a legitimate interest in determining whether it was paying for extensive personal communications, or whether employees were being forced to pay out of pocket for work-related expenses. As for the scope of the search, the Court held that reviewing the transcripts of the employee's text messages was reasonable because it was "an efficient and expedient way" to determine whether the particular employee's overages were the result of work-related or personal use. Id. Finally, because the employee was told that his text messages were subject to review and because his status as a law enforcement officer should have caused him to know that his use of the pager could be scrutinized, the search was not deemed by the Court to be excessively intrusive.

- **Myth #5: It is illegal for employers to use social media sites to gather information about potential employees.**

- **Reality: Employers may (and do) gather information from social media sites in the course of hiring, but they may not use that information to discriminate against potential employees.**

A January 2009 CareerBuilder.com survey reported that 45 percent of employers search social networking sites to screen job candidates. McCreary, John A., Symposium: Social Networking and Employment Law, 81 Pa. Bar. Assn. Quarterly 69, 70 (2010). Eighteen percent of employers found content on social networking sites that played a role in their decision whether to hire an applicant. The stated areas of concern by employers were:

- Provocative or inappropriate photos or information (53%)
- Content about drinking or drug use (44%)
- Content about an applicant's previous employer (35%)
- Content showing poor communication skills (29%)
- Content showing discrimination (26%)
- Content showing an applicant lied about her or his qualifications (24%)
- Content showing disclosure of confidential information from a prior employer (20%)

Id. at 70-71.

Employers who use information obtained from social networking sites in screening applicants should be cautious however, as other information obtained through such means may put them at risk for a discrimination claim. Under Title VII, it is not illegal for an employer to learn about the race, gender, disabled status, ethnicity, etc. of an applicant. However, Title VII requires that all applicants be give equal,

nondiscriminatory treatment in the hiring process. Therefore, if an employer learns of an applicant's protected status through the applicant's social media page, such knowledge could increase the risk of discrimination or the appearance of discrimination. Id. at 72; see also Michael S. Cohen, A Site (Un)Seen: Using Social Media in Hiring Decisions, The Legal Intelligencer, Dec. 22, 2010, at 7.

- **Myth #6: Non-public sector employees have no redress for invasion of privacy.**
- **Reality: Employer monitoring may give rise to a state common law action for invasion of privacy, under very limited circumstances.**

Most attempts by private sector employees to challenge employer searches of their email or other electronic data are unsuccessful. In Smyth v. Pillsbury Co., 914 F.Supp. 97 (E.D. Pa. 1996), for example, the court held that there was no reasonable expectation of privacy in email communications voluntarily made by an employee to his supervisor over the employer's email system. That was true even though the employer had assured its employees that their email messages would not be intercepted: "Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an email system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost." Id. at 101.

Common law invasion of privacy claims are not completely without potential for success, however. In United States v. Charbonneau, 979 F.Supp. 1177 (S.D. Ohio 1997), the court at least acknowledged that an employee had a limited reasonable expectation of privacy in personal emails sent via AOL. However, once those messages were shared in a public chat room, they lost any

semblance of privacy. The court, analogizing, to traditional means of communication, explained:

> E-mail transmission are not unlike other forms of modern communication. We can draw parallels from these other mediums. For example, if a sender of first-class mail seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause. However, once the letter is received and opened, the destiny of the letter then lies in the control of the recipient of the letter, not the sender, absent some legal privilege.
>
> Similarly, the maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others.
>
> Drawing from these parallels, we can say that the transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny.

Id. at 1184 (citing United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996)).

In Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (2010), the New Jersey Supreme Court held that an employee had a reasonable expectation of privacy over her attorney-client privileged communications. The court's ruling was supported in part by the fact that the employer's computer use policy was ambiguous and did not explicitly state that password-protected emails were subject to employer audit, and the fact that the employer had allowed employees to use their work computers for personal use.

- **Myth #7: Under the just cause standard, employees are free to engage in off-duty social media use without fear of reprisal by their employer.**

- **Reality: Under the just cause standard, off-duty social media use may result in discipline if an employer can show a "nexus" to the workplace or if an employee fails to take affirmative steps to safeguard the information.**[2]

In the arbitration context, arbitrators appear to apply traditional concepts of just cause to assess employees' use of electronic media. For example, arbitrators will consider whether other employees have been disciplined similarly for similar conduct, the exact nature of the employee's public employment (i.e., whether the grievant is a teacher or a firefighter, for example), whether the grievant took any measures to either mitigate or aggravate the particular harm, whether there is a sufficient nexus between the employee's conduct and the employee's work, and the extent to which the employer's ability to carry out its functions is affected by the employee's conduct.

In Phenix City Bd. of Educ., 125 Lab. Arb. Rep. 1473 (2009) (Baroni), the arbitrator sustained the discharge of a teacher after the school administration received an anonymous package from parents with printouts from a webpage containing nude pictures of the teacher. The arbitrator, holding the teacher to a higher standard because her important role as an educator, held that discharge was appropriate because of how easily accessible the websites containing the photos were, the fact that the teacher was nude or nearly nude in the photos, and the websites referenced explicit sexual acts.

In a somewhat similar vein, in Warren City Bd. of Educ., 124 Lab. Arb. Rep. 532 (2007) (Skulina), the arbitrator sustained the discharge of a teacher where the teacher's estranged wife posted nude photos of the teacher on social media sites and the photos

[2] Computer software now allows employers to track their employees' off-duty, personal posts made on social media networking sites. Employers can monitor employee activity through software that tracks particular key words and employee names. When the keyword is used by a tagged employee, the employer is alerted.

were discovered by parents, teachers, and the press. The arbitrator's decision was based in large part on the teacher's failure to take sufficient measures to prevent his estranged wife from making the photos public.

In contrast, however, L'Anse Creuse Pub. Schs., 125 Lab. Arb. Rep. 527 (2008) (Daniel), the arbitrator explained that there was an insufficient work nexus between internet pictures of teacher performing faux salacious acts and work as a teacher. As the arbitrator explained, "it did not directly involve either the school or her capacity to teach." Id. at 530. The arbitrator concluded that the employer would not have had just cause for terminating her employment.

In WMATA/Metro, 124 Lab. Arb. Rep. 972 (2007) (Evans), the arbitrator reduced the discharge of an employee who sent racist jokes via text message to coworkers to a suspension. The arbitrator found relevant that the text messages were sent inadvertently, that the grievant apologized for sending the messages, and that no other employee had been terminated for engaging in comparable conduct.

In Union Twp. Bd. of Trustees, 125 Lab. Arb. Rep. 1638 (2008) (Rosen), the arbitrator sustained the suspension of a firefighter who posted a demeaning rap song on the union's website. In sustaining the suspension, the arbitrator explained that "there is sufficient case law saying a public employee is not free to criticize publicly his employer over employment matters . . . there is sufficient case law for the proposition that internal harmony of a fire department may be adversely effected by a firefighter undermining supervisory authority by such adverse criticism." Id. at 1658.

In Shawnee County, 123 Lab. Arb. Rep. 1659 (2007) (Daly), the arbitrator sustained the grievance in a case where the employer viewed pictures of an employee online dancing at a bar and assumed that the employee had been dishonest about the reason for her tardiness to work. The arbitrator held that the employer failed to prove through the photos that the employee had lied about her reason for being late.

In Coca-Cola Bottling Co. of Ohio, 121 Lab. Arb. Rep. 1489 (2005) (Paolucci), the arbitrator denied the grievance of an employee whose prior conviction as a sex offender was registered on a state's public website. The arbitrator agreed that the publication undermined the company's image and could undermine public confidence in the employee's work.

- **Myth #8: Under the just cause standard, employers do not have a right to monitor employees' work emails and computer files or discipline employees for their misuse.**

- **Reality: Arbitrators typically hold that there is no right to privacy in work emails and computer files, and that employers may monitor employee computer use, especially where an employer has a reasonable belief that a violation of an employer policy is occurring.**

Arbitrators apply the traditional concepts of just cause and fairness to determine whether an employer has the right to discipline an employee for misconduct discovered as a result of monitoring an employee's computer use. In particular, arbitrators are interested in whether the employer notified its employees that their computer use would be subject to audit or whether monitoring was surreptitious.

For example, in PPG Indus. Inc., 113 Lab. Arb. Rep. 833 (1999) (Dichter), the arbitrator held that an employee had no reasonable expectation of privacy when using an individualized email password on company equipment. In PPG, the grievant sent sexual jokes over the employer's email system. Even though his email account was password-protected, the arbitrator determined that the employee had no reasonable expectation of privacy to his work emails: "The password prevents other employees from gaining access to material that they have no right to view. It does not protect the employee from the owners of the computer through its agents seeing anything that an employee might have in their files." Id.

Similarly, in Tesoro Ref. & Mktg. Co., 120 Lab. Arb. Rep. 1299 (2005) (Suntrup), the arbitrator permitted employer monitoring to ensure compliance with an employer policy prohibiting the storage of offensive materials on company computers. In particular, the employer had a policy providing: "It is not the Company's intent to strictly monitor the electronic information created and/or communicated by an employee using electronic media. However, the Company has the ability to trace and to monitor usage patterns and gateway activity to the Internet and reserves the right to do so." Id. at 1302.

In M T Detroit, Inc., 118 Lab. Arb. Rep. 1777 (2003) (Allen), the arbitrator sustained the discharge of an employee after the employer searched the employee's computer files after a tip from a chat room operator that the employee had posted racially offensive messages. The arbitrator disregarded the employee's argument that she did not know that her conduct on her employer's work computer would be traceable back to her employer, especially given the employer's disclaimer on the screen of her work

station computer warning her that her computer should only be used for work purposes and that the system was being monitored.

In an example of indirect monitoring of computer use, in Kuhlman Elec. Corp., 123 Lab. Arb. Rep. 257 (2006) (Nicholas), the arbitrator held that photographs of an employee viewing DVDs on his work computer obtained through a secretly installed camera were admissible at his arbitration. In particular, although the photos were obtained through a nonconsensual search, the methods employed to obtain the photos were was not "excessively shocking to the conscience of a reasonable person." Id. at 260. However, the arbitration reduced the discharge to a suspension because of the grievant's spotless work record and the employer's failure to prove lewd and indecent behavior for which it had fired the grievant.

Note, however, that in Beverage Marketing Inc., 120 Lab. Arb. Rep. 1388 (2005) (Fagan), the arbitrator reduced the discharge of an employee where the employer installed a secret GPS device without notice to the employee. The arbitrator, by his award, suggested that secret monitoring is generally not appropriate.

- **Myth #9: Federal and state electronic privacy statutes provides employees with a meaningful workplace right to privacy.**

- **Reality: Federal and state statutory privacy laws provide very little protection to employees.**

The federal Electronic Communications Privacy Act ("Act"), 18 U.S.C. § 2510 et seq., applies to both public and private employees. Title I of the Act makes it unlawful for an individual to intentionally intercept a "wire, oral or electronic communication." This does not include "electronic storage of any such communication." Title II of the Act limits access to electronically stored information, including computer files. There are two exceptions to the Act's protections. First, under the "consent exception," an employer policy that reserves the right to intercept, monitor, or access work emails and computer files will generally allow the employer to avoid liability under the Act. Second, the "provider exception" permits a person or entity providing a wire or electronic communications service to intercept or access electronically stored information.

Applying these rules, in Fraser v. Nationwide Mutual Insurance, 352 F.3d 107 (3d Cir. 2003), the U.S. Court of Appeals for the Third Circuit rejected an employee's claims under the Act based on an employer search of emails sent to and received by an independent insurance agent that were stored in employer's server. The Title I claim was rejected because the search did not constitute an "intercept" as it was not conduced contemporaneously with the transmission of the files. The Title II claim was also dismissed based on the provider exception. Similarly, in Bohach v. City of Reno, 932 F.Supp. 1232 (D. Nev. 1996), a trial court upheld the employer's access to employee text messages stored on employer's computer system because the employer was the "provider."

However, in Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001), the Sixth Circuit Court of Appeals ruled that an employer's surreptitious monitoring of phone numbers received on an employee's pager could constitute a violation of the Act. Likewise, where an employer's purported authorization to access the employee's MySpace account is coerced, a violation may be found. See Pietrylo v. Hillstone Restaurant Group d/b/a Houston's, No. 06-05754, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009).

Note that additional protections may be available under state law. A few states have laws that restrict an employer's monitoring of employee email and internet use without advance notice, and others have established statutes relating particularly to off-duty conduct. For example:

- California: Cal. Lab. Code § 96(k): gives authority to the labor commissioner to hear claims for loss of wages as a result of an adverse action for lawful conduct occurring during nonworking hours.
- Connecticut: Conn. Gen. Stat. § 31-48(d): compels employers to give notice to employees prior to monitoring of email or internet use; limits the restriction where an employer has a reasonable belief that an employee is engaging in unlawful conduct or conduct that violates work rules.
- Colorado: C.R.S. § 24-34-402.5(l): provides protection to employees, but only where the employee's conduct has no connection to the employer's business concern.
- Delaware: Del. Code Ann. Tit. 19, § 705: requires employers to provide notice to employees prior to monitoring email or internet use.
- New York: NY CLS Labor § 201-(d)(2)(a)-(c): makes it illegal for an employer to discriminate against an employee because of an employee's legal recreational activities outside work hours, but no protection is provided to employees where there is a material conflict of interest.

III. FIRST AMENDMENT

Because of the First Amendment, public entities and employers face greater constraints than do private employers in their ability to respond to employees' use of electronic media. A public employee's speech is protected under the First Amendment if: (1) when uttering it, the public employee was speaking as a citizen, (2) the public employee was speaking on a matter of public concern, and (3) the government employer does not have an adequate justification for treating the employee differently than a member of the general public. Garcetti v. Ceballos, 547 U.S. 410, 418 (2006). At the intersection of free speech and social media, several common misconceptions exist:

- **Myth #10: Employees' speech on social media sites is protected under the First Amendment.**
- **Reality: Public employees receive limited protection under the First Amendment, while private employees have no First Amendment protection.**

The Supreme Court has provided the standard for the First Amendment rights of public employees in Garcetti v. Ceballos, 547 U.S. 410 (2006). If a public employee is not speaking as a citizen on a matter public concern, the employee has no First Amendment protection. If a public employee is speaking as a citizen on a matter of public concern, the employee's speech is protected as long as the public employer had no adequate justification for treating the employee differently from any other member of the public. This inquiry requires an analysis of the importance of the relationship between the public employee's speech and the employment itself. The public employer has greater discretion to limit speech when the limitations it imposes are directed at speech that has some potential to affect the government entity's operations.

Under Garcetti, when a public employee speaks "pursuant to his or her official duties," that speech is not protected, as it is not made "as a citizen." In practice, this typically means that employees who take their speech up the chain of command are not protected under the First Amendment, as that speech is a communication made "pursuant to official duties." See, e.g., Meyers v. County of Somerset, 293 Fed. Appx. 915 (3d Cir. 2008) (comments made to someone in the chain of command are made pursuant to employment duties and therefore are not made as a "citizen"); Meenan v. Harrison, 264 Fed. Appx. 146 (3d Cir. 2008) (plaintiff police officer's speech was not pursuant to his official duties where he went to a media outlet with his concerns about the sufficiency of another officer's investigation into a teacher's misconduct).

The same general principles apply when the speech in question is communicated through social media outlets. For instance, in Spanierman v. Hughes, 576 F.Supp.2d 292, 297 (D. Conn. 2008), the court held that there was no violation of the First Amendment rights of a teacher who communicated with his students on MySpace because his speech was not on a matter of public concern and it was disruptive to school activities. The same result was reached regarding MySpace postings on matters of private concern in Snyder v. Millersville University, No. 07-1660, 2008 U.S. Dist. LEXIS 97943, at *7 (E.D. Pa. Dec. 3, 2008). In Nickolas v. Fletcher, No. 06-00043, 2007 U.S. Dist. LEXIS 23843 (E.D. Ky. Mar. 30, 2007), the plaintiff challenged the State of Kentucky's decision to prohibit state employees from accessing blogs from state-owned computers. The court held that the prohibition did not violate the First Amendment because it was a reasonable restriction implemented in order to prevent employee inefficiency.

The amount of information regarding employee activity and opinions on and off the job that is publicly available on the internet has grown exponentially in recent years. While there are relatively few reported decisions regarding such claims at present, if news reports are any indication, one can expect increasing numbers of such claims in the near future. Examples of currently pending or recently settled claims follow:

- In Payne v. Barrow County School District, No. 09-3083-X (Barrow Cty. Sup. Ct. Oct. 15, 2009), a case currently being litigated in Georgia, a teacher sued her former employer, the Barrow County School District, after being forced to resign in what she alleges was a violation of her First Amendment rights. Payne alleges that she was forced to resign after the School District viewed pictures of her on her Facebook page drinking alcohol.

- In April 2010, Elizabeth Collins, a teacher at an all-girls private school in Villanova, Pennsylvania was fired after posting her thoughts on her blog about a student's presentation. The post, which did not identify the school or the student, was viewed by the student's parents, who complained to school administration. Though the school had no specific guidelines on blogging, in its termination letter to Collins, it stated that she had violated faculty policies and procedures, as well as the school's ethics code.

- In February 2011, public school teacher, Natalie Munroe, was suspended with pay after posting insulting comments about students and staff members on her personal blog. As of March 2011, Central Bucks (Pennsylvania) School District had not made a decision about Munroe's ongoing employment, but her lawyer has stated that he will file a First Amendment suit on her behalf if the School District terminates her employment.

- Also in February 2011, Hope Moffett, a teacher at Audenried High School in Philadelphia, Pennsylvania publicly criticized the Philadelphia School District's decision to convert Audenried into a charter school. She was subsequently removed from the classroom and the School District initiated termination proceedings. The Philadelphia Federation of Teachers, the union representing Moffett, filed a motion for preliminary injunction in early March 2011. The parties settled in March 2011 and Moffett returned to the classroom with a five day suspension, which remains subject to arbitration.