Workshop: Negotiations 102 CLE Credit - Collective Bargaining in the Brave New World: Exploring the Continuing Impact of Electronic Media on Negotiations, Protected Activity, and Privacy in the Modern Workplace

Stuart Davidson
*Willig, Williams & Davidson*

Amy Rosenberger
*Willig, Williams & Davidson*

Follow this and additional works at: [https://thekeep.eiu.edu/jcba](https://thekeep.eiu.edu/jcba)

**Recommended Citation**


DOI: [https://doi.org/10.58188/1941-8043.1071](https://doi.org/10.58188/1941-8043.1071)

Available at: [https://thekeep.eiu.edu/jcba/vol0/iss7/20](https://thekeep.eiu.edu/jcba/vol0/iss7/20)
NEGOTIATIONS 102

COLLECTIVE BARGAINING IN THE BRAVE NEW WORLD:
Exploring the Continuing Impact of Electronic Media on Negotiations,
Protected Activity, and Privacy in the Modern Workplace

An Update On 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
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, who contributed significantly to 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, with just a few exceptions, the decisional law continues to suggest that the key to understanding issues presented by electronic media use is to reason by analogy to more “traditional” means of communication, even where the analogy may not seem to be a perfect fit. For example, an email string between two people or among a group, may be viewed similarly to an in-person conversation. 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 updated overview of how the National Labor Relations Board (“NLRB” or “Board”), the courts and arbitrators are applying existing rules about employee communications and activity to electronic media. While use of social media in general can raise a host of legal issues, this paper focuses in particular on protected activity under the National Labor Relations Act (“NLRA”), issues of employee privacy and free speech rights and just cause for discipline.

I. PROTECTED ACTIVITY UNDER THE NLRA

Section 7 of the NLRA provides that employees shall possess “the right to self-organization . . . and to engage in other concerted activities for the purpose of . . . mutual aid or protection.” This right is enforceable under Section 8(a)(1) and sometimes (3) of the NLRA, which prohibit employers from interfering, restraining or coercing employees who exercise their rights under Section 7, or from discriminating against employees because of their protected activity. These rights apply to workplaces where a union represents the employees, and to non-union workplaces. In recent years, the Board has addressed issues relating to both employee use of employer electronic media, as well as use of personal social media to engage in protected activity.

A. Use of Employer Electronic Systems for Union Activity

The Board has held that employees have no statutory right under the NLRA to use an employer’s email system for Section 7 matters.2 The Board explained that an employer has a “basic property right” to “regulate and restrict employee use of company property.” Thus, an employer may lawfully ban non-work-related use of its email systems, so long as it discriminate against Section 7 protected activity.3

---

2 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), on remand, 357 NLRB No. 27 (2011).
3 351 NLRB at 1114-1116.
employer in Register Guard had adopted a policy governing use of its communications systems, and that policy prohibited use of its systems “to solicit or proselytize for commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations.” The Board found this policy to be a lawful regulation of the employer’s property.\(^4\) However, after many years of litigation, the Board ultimately found in 2011 that the employer had violated the NLRA by discriminatorily enforcing its communications systems policy.\(^5\)

Despite the policy’s clear prohibition of non-job-related solicitations through the employer’s electronic communications systems, the employer had not disciplined employees who used its email system for personal solicitations such as party invitations, baby announcements, offers of sports tickets and requests for services such as dog-walking.\(^6\) But when an employee sent emails to coworkers over the employer’s email system seeking support for union activities, the employer disciplined her for violating the policy.\(^7\)

In 2007, the Board had initially held that the employer lawfully restricted email pertaining to the union even if it allowed email for other uses, because there was no evidence that other employees had used email for organizational, as opposed to personal solicitations.\(^8\) The union appealed that ruling and two years later the D.C. Circuit Court of Appeals rejected the Board’s reasoning and remanded the case to the Board.\(^9\) 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.”\(^10\) Further, the employer’s own policy made no such distinction between “personal” solicitation and “organizational” solicitations. In July, 2011, the Board ruled, based upon the District Court’s decision, that the employer had unlawfully discriminated against the employee who sent union-related emails when it did not enforce its policy against other employees sending non-job-related solicitations.\(^11\) Thus, for the time being at least, it appears that the Board will continue to apply its longstanding rules concerning discriminatory enforcement of otherwise lawful non-solicitation policies.

Of course, the mere fact that an employer may lawfully use work rules to restrict non-job-related use of its email and other systems (so long as it does not discriminate in enforcing its rules) does not prevent a union from seeking to bargain 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,

---

\(^4\) Id. at 1114.

\(^5\) Register Guard, 357 NLRB No. 27 (2011).

\(^6\) 351 NLRB at 1111, 1119.

\(^7\) Id. at 1111-1112.

\(^8\) Id. at 1119, 1120.

\(^9\) See Guard Publishing Co. v. NLRB, 571 F.3d 53 (D.C. Cir. 2009).

\(^10\) Id. at 60.

\(^11\) See Register Guard, 357 NLRB No. 27.
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.

B. Off-Duty Work-Related Communications Through Social Media

In early 2011, the NLRB’s settlement of an unfair labor practice charge contesting the firing of an American Medical Response employee for posting disparaging comments about a supervisor on Facebook received widespread media attention. After the employee asked for and was denied union representation in connection with an investigation of client complaints about her, she posted comments on her Facebook page insinuating that the employer allowed a psychiatric patient to be a supervisor. She also responded to coworker comments on her post. She was fired for allegedly violating an employer policy prohibiting disparagement of the company or its management. The Board issued a complaint alleging that the employer’s policy was overly broad because it prohibited off-duty communication among employees concerning wages, hours and working conditions.\(^\text{12}\) The case settled shortly thereafter.

Two months later, the Board was in the media spotlight again when it reportedly decided to pursue a charge against Thomson Reuters concerning the reprimand of a reporter over a Twitter posting. In that case, a supervisor invited employees to “tweet” about how to make Reuters “the best place to work.” But when an employee posted a message saying, “One way to make this the best place to work is to deal honestly with Guild\(^\text{13}\) members,” she was reprimanded. That case ultimately settled in late 2011.\(^\text{14}\)

Perhaps as a result of the press coverage of these two cases, an increasing number of charges have been filed alleging that employees were disciplined for engaging in protected activity on various social media outlets. Signaling an effort to develop a consistent approach to these cases, in April 2011 the Board’s Acting General Counsel, Lafe Solomon, instructed regional NLRB offices to submit all charges involving employee use of social media to the Office of General Counsel’s Division of Advice for a determination as to whether or not a complaint should be issued. Acting General Counsel Solomon has issued periodic memoranda summarizing the Division of Advice’s determinations in these cases, in an effort to provide guidance to parties and practitioners in this area. The cases addressed by the Division of Advice, and the


\(^{13}\) Employees in that case were represented by the Newspaper Guild of New York.

\(^{14}\) See Thomson Reuters, Advice Memo, 2-CA-39682 (Apr. 5, 2011).
Board to date address issues of alleged unlawful employee discipline for engaging in protected activity, employer surveillance of protected activity, and overbroad employer social media policies. For the most part, the Board has been applying existing law concerning protected activity in the social media world.

1. Protected Concerted Activity

The Board has long held that employee communications that amount to “concerted activity for mutual aid and protection” is protected under the NLRA, and so cannot be restricted by the employer. Protected concerted activity occurs where the employee acts “with or on the authority of other employees, and not solely by or on behalf of the employee himself”\(^\text{15}\) and “encompasses those circumstances where individual employees seek to initiate or to induce or prepare for group action.”\(^\text{16}\) The activity must relate to wages, hours or terms and conditions of employment. Thus, complaints about the performance of coworkers that adversely affect the employee’s working conditions are protected.\(^\text{17}\) However, where complaints about employee performance or the quality of service provided by the employer have only a tangential relationship to employee terms and conditions of employment the complaints are not protected.\(^\text{18}\) Protest of supervisory action is also protected.\(^\text{19}\) Although the most clear type of protected communications occur when the subject of discussion is collective action, employee discussion about shared concerns about terms and conditions of employment is protected even when “in its inception [it] involves only a speaker and a listener” because this is “an indispensable preliminary step to employee self-organization.”\(^\text{20}\)

Applying these rules, complaints over social media about a supervisor have been found to constitute protected concerted activity where coworkers respond to the posts and a discussion of the issue ensues.\(^\text{21}\) Similarly, Facebook posts about managerial marketing decisions that negatively impact employee commissions have been found protected where they grew out of prior concerted complaints to


\(^{16}\) Meyers II, 281 NLRB at 887.

\(^{17}\) Georgia Farm Bureau Mutual Ins. Cos., 333 NLRB 850, 850-51 (2001).


\(^{19}\) Datwyler Rubber & Plastics, Inc., 350 NLRB 669 (2007).

\(^{20}\) Meyers I, 268 NLRB at 494; Meyers II, 281 NLRB at 887.

management about the subject. A “Tweet” to the effect that the employer should deal fairly with the union has also been considered protected.

However, the guidance from the NLRB so far indicates that social media posts complaining about work-related matters will more likely be considered individual griping, rather than protected concerted activity, if no coworkers respond or express agreement, and if the employee does not discuss the posts with coworkers, or if the posts are not an attempt to initiate or prepare for group action. Also unprotected are posts that do not relate to wages, hours or terms and conditions of employment, such as: complaints about a coworker’s annoying personal habits, qualifications, alleged misconduct, tattling on coworkers or inadequate performance; complaints about customers; sarcastic and derisive posts regarding a city’s homicide rate and employees of a competitor news organization; statements of employees’ intent to withhold medical care from patients who offend them; and descriptions of a client/resident’s odd behavior.

Activity or communications that might otherwise be protected concerted activity for mutual aid and protection may lose that protection where it is so “opprobrious” as to lose the NLRA’s protection. In considering whether communication loses the protection, the Board considers the place and subject matter of the discussion, the nature of the employee’s “outburst” and whether the outburst was provoked by an employer unfair labor practice. Likewise, “[s]tatements are unprotected if they are maliciously untrue, i.e., if they are made with knowledge of their falsity or with reckless disregard for their truth or falsity.”

---

27 Public Service Credit Union, Advice Memo, 27-CA-21923 (Nov. 1, 2011).
29 MONOC, Advice Memo, 22-CA-29008 (May 5, 2010).
30 Martin House, Advice Memo, 34-CA-12950 (July 19, 2011).
32 Id.
Applying these rules, the Division of Advice recently concluded that Facebook comments complaining about a union’s representation of employees who contested the commenter’s promotion lost any protection it might otherwise have had because it also used offensive racial stereotypes which caused disruption in the workplace.\(^{33}\) In another case, the Division of Advice found that a post alleging employer fraud lost its protection when the employee refused to remove the post after she learned that in fact there was no fraud.\(^{34}\)

Generally, 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.\(^{35}\) General disparagement of the employer’s product or services by a current employee, however, is not protected and therefore the Division of Advice has opined that a social media policy prohibiting “disparagement of company’s or competitors’ products, services, executive leadership, employees, strategy and business prospects” was lawful, when read in its context which included prohibition of disclosing proprietary information and intellectual property such as product design, software, ideas and innovation, explicit sexual references, disparagement of any race, religion, gender, sexual orientation, disability or national origin and other comments which are clearly not protected under Section 7.\(^{36}\)

When it comes to post-dismissal comments by an unlawfully fired employee, however, the employer faces a somewhat higher burden. The employer in such a case may avoid a reinstatement remedy only if the employee engages in conduct so flagrant that it renders the employee unfit for further service.\(^{37}\) The Board recently applied this rule in a case involving post-discharge blog posts by a news reporter criticizing his former employer’s apparent refusal to support its own staff and failure to report accurately news of interest to the community. The NLRB rejected the employer’s claim that the employee was unfit for further service, noting that “employees who are unlawfully fired . . . often say unkind things about their former employers,” and “[e]mployers who break the law should not be permitted to escape fully remediying the effects of their unlawful actions based on the victims’ natural human reactions to the unlawful acts.”\(^{38}\)

2. **Surveillance of Protected Activity**

An employer may violate the NLRA if it engages in surveillance of protected activity, or creates the impression that it is doing so, because employees

\(^{33}\) Detroit Medical Center, Advice Memo, 7-CA-6682 (January 10, 2012).

\(^{34}\) TAW, Inc., Advice Memo, 26-CA-063082 (Nov. 22, 2011).

\(^{35}\) Jefferson Standard, NLRB v. IBEW Local 1229, 346 U.S. 464 (1953)

\(^{36}\) Sears Holdings (Roebucks), Advice Memo, 18-CA-19081 (Dec. 4, 2009).


\(^{38}\) Hawaii Tribune Herald, 356 NLRB No. 63 (2011)
should feel free to engage in protected activity “without the fear that members of management are peering over their shoulders.”\textsuperscript{39} However, an employer does not engage in unlawful surveillance where a member of management is invited to observe.\textsuperscript{40} An employer unlawfully creates an impression of surveillance where “the employee would reasonably assume from the [employer’s] statement that their union activities had been placed under surveillance.”\textsuperscript{41} In cases outside the social media/electronic communications setting, the Board has found this standard satisfied by employer statements indicating knowledge of protected activity that is not generally known, and does not reveal the source of its knowledge.\textsuperscript{42}

Early indications suggest that the application of the standard in cases involving an alleged impression of surveillance of electronic and social media may lead to a different conclusion. For example, the Board has held that no impression of surveillance was created where a supervisor told employees he knew about a message on a password-protected union website, because “we think that a reasonable employee would assume that [the supervisor] lawfully learned of [the] message exactly the way [he] did—through public dissemination by another website subscriber.”\textsuperscript{43} In light of this holding, the Division of Advice has found no unlawful surveillance where an employee limited access to his posts to those whom he had “friended” – because he did not “friend” the supervisor in question, the employee could not reasonably believe that the supervisor had access to surveil the posts.\textsuperscript{44} Of course, where the employer learns of the employee’s posts because the employee has “friended” a supervisor, the employee will be considered to have invited the observation, and so no unlawful surveillance will be found then, either.\textsuperscript{45} Where a coworker who has access to the post voluntarily shows the post to the employer, no surveillance will be found.\textsuperscript{46} It remains to be seen whether the Board will find unlawful surveillance where an employer or supervisor coerces a coworker to provide access to the employee’s posts.

\textsuperscript{39} Flexsteel Industries, 311 NLRB 257, 257 (1993).
\textsuperscript{40} Donaldson Bros. Ready Mix, Inc., 341 NLRB 958, 960-961 (1976).
\textsuperscript{41} Flexsteel Industries, 311 NLRB 257, 257 (1993).
\textsuperscript{42} Stevens Creek Chrysler Jeep Dodge, 353 NLRB 1294, 1296 (2009), aff’d 357 NLRB No. 57 (2001) (knowledge of union meeting and distribution of union cards); Avondale Industries, 329 NLRB 1064, 1065 (1999) (knowledge of employee’s support for union).
\textsuperscript{43} Frontier Telephone, 344 NLRB 1270, 1276 (2005).
\textsuperscript{44} Public Service Credit Union, Advice Memo, 27-CA-21923 (Nov. 1, 2011).
\textsuperscript{45} Buel, Inc., Advice Memo, 11-CA-22936 (July 28, 2011).
\textsuperscript{46} Intermountain Specialized Abuse Treatment Ctr., Advice Memo, 27-CA-65577 (Dec. 6, 2011); MONOC, Advice Memo 22-CA-29008 (May 5, 2010).
3. Social Media Policies

An employer violates the NLRA if it maintains a work rule that “would reasonably tend to chill employees in the exercise of their Section 7 rights.” A rule is unlawful if it explicitly restricts Section 7 protected activity. If the rule does not explicitly restrict Section 7 activity, it may still be found unlawful if one of three criteria is met: (a) employees reasonably would construe the rule to prohibit such activity; (b) the rule was issued in response to union activity; or (c) the rule has been applied to restrict protected activity. Rules that provide specific examples of clearly illegal or unprotected conduct are less likely to be considered unlawful, as they could not reasonably be construed to cover protected activity.

Applying these rules, broadly-worded social media policies that prohibit, without limitation, communication that is disrespectful, offensive, rude, discourteous or inappropriate; or that “may in any way violate, compromise, or disregard . . . the rights and reasonable expectations as to privacy or confidentiality or any person or entity” or disclose “confidential” or “sensitive” information; or that embarrasses, attacks, insults, disparages or harasses employees or agents of the employer; or which might damage the employer’s reputation or goodwill; or rules prohibiting employees from responding to inquiries from third parties concerning employees, would likely be considered unlawful, as employees could reasonably construe such rules to prohibit NLRA-protected communications. Likewise, a policy that prohibits employees from referencing personal information of coworkers, clients, partners or customers without their consent, could reasonably be construed to prohibit discussion of wages and other terms and conditions of employment. A rule prohibiting use of employer logos, photographs of an employer facility, equipment, brand or product without permission may reasonably be construed to prohibit posting of pictures of the employee carrying a picket sign in front of the employer’s premises, or wearing a t-shirt with the employer’s name or logo while peacefully handbilling or engaging in other protected activity. A broad “savings clause” stating that nothing in the policy should be construed to limit NLRA-protected rights or other lawful conduct will not be viewed as sufficient to save an otherwise improper work rule.

---

51 Giant Eagle, Inc., Advice Memo, 6-CA-37260 (June 22, 2011).
53 Giant Eagle, Inc., Advice Memo, 6-CA-37260 (June 22, 2011); Flagler Hospital, Advice Memo, 12-CA-27031 (May 10, 2011).
However, a rule that prohibits employees from “pressuring” coworkers to participate in social media communications was found lawful, because it “is sufficiently specific in its prohibition against pressuring co-employees and clearly applies only to harassing conduct. It cannot reasonably be interpreted to apply more broadly to restrict employees from attempting to ‘friend’ or otherwise contact their colleagues for the purposes of engaging in protected concerted or union activity.”

II. PRIVACY RIGHTS

A. Public Employees

For employees in the public sector, the Fourth Amendment, which prohibits unlawful searches and seizures, provides some protection 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.” A public employee may have a reasonable expectation of privacy when it comes to technological equipment provided by his or her employer, but the “reasonableness” of an employee’s expectation of privacy is determined on case-by-case basis.

For example, the Second Circuit Court of Appeals held 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, the Fifth Circuit has held that a public employee had a reasonable expectation of privacy where the employee used a password protected computer in a locked office. 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

54 Giant Eagle, Inc., Advice Memo, 6-CA-37260 (June 22, 2011).
56 Leventhal v. Knapek, 266 F.3d 64 (2d Cir. 2001).
57 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). (While Slanina was a criminal case, the pornography recovered from the employee’s computer was recovered in the course of a work investigation.)
monitored. A public employer may also create a reasonable expectation of privacy by notifying its employees that they can maintain private files on their computer.\footnote{See, e.g., \textit{Haynes v. Office of the Attorney Gen.}, 298 F.Supp.2d 1154 (D. Kan. 2003); \textit{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).}

On the other hand, where an employee connected his personal computer to his employer’s network without a password protecting his files, the Tenth Circuit Court of Appeals found that he had no reasonable expectation of privacy.\footnote{\textit{U.S. Barrows}, 481 F.3d 1246 (10th Cir. 2007).} 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.\footnote{\textit{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.

However, a reasonable expectation of privacy alone may not be sufficient to protect the public employee under the Fourth Amendment. In 2010, the U.S. Supreme Court addressed a case in which a municipal employer 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.\footnote{\textit{City of Ontario v. Quon}, 130 S. Ct. 2619 (2010).} 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.\footnote{\textit{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.

\footnote{\textit{Id.} at 1248-49.}
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.” Employees had been permitted to use the wireless system for personal communications, but had to pay for any amount which exceeded the contract amount negotiated with the wireless company. 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. 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.

B. Public and Private Sector Employees

1. Screening of Job Applicants

A January 2009 CareerBuilder.com survey reported that 45 percent of employers search social networking sites to screen job candidates. 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.

---

63 Id. at 2631.
64 Id.
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 given 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. 66

2. Common Law Invasion of Privacy Claims

Most attempts by private sector employees to challenge employer searches of their email or other electronic data are unsuccessful. For example, one 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. 67 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.” 68

Common law invasion of privacy claims are not completely without potential for success, however. At least one court has acknowledged that an employee had a limited reasonable expectation of privacy in personal emails sent via AOL. 69 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

68 Id. at 101.
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)).

The New Jersey Supreme Court made headlines in 2010 when it held that an employee had a reasonable expectation of privacy in her attorney-client privileged communications, even though they were conducted from her employer-issued computer. 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.

3. Arbitral Views of Employee Privacy in Employer Systems

Grievance arbitrators often hold that an employer has a right to monitor employee use of employer electronic equipment. 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.

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. For example, one arbitrator held that an employee had no reasonable expectation of privacy when using an individualized email password on company equipment. 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.”

Similarly, another 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.”

In another case, the employer searched an employee’s computer files after a tip from a chat room operator that the employee had posted racially offensive messages. In sustaining the employee’s dismissal, the arbitrator rejected 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, an 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 not “excessively shocking to the conscience of a reasonable person.” However, the arbitrator 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 another arbitrator reduced the discharge of an employee where the employer installed a secret GPS device without notice to the employee. The arbitrator suggested that secret monitoring is generally not appropriate.

4. Federal and State Electronic Privacy Laws

The federal Electronic Communications Privacy Act (“Act”), 18 U.S.C. § 2510 et seq., applies to both public and private sector 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, 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 conducted contemporaneously with the transmission of the files. The Title II claim was also dismissed based on the provider exception. Similarly, a federal trial court upheld the employer’s access to employee text messages stored on employer’s computer system because the employer was the “provider.”

However, 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.

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. § 31-48d: 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: 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.

---

78 Adams v. City of Battle Creek, 250 F.3d 980 (6th Cir. 2001).

III. FIRST AMENDMENT FREE SPEECH RIGHTS

Employees often believe that because of their constitutional right to freedom of speech under the First Amendment, they cannot be subject to employer discipline for what they say or do on-line. However, the First Amendment protects individuals from government infringement on the right to free speech, and so does not provide private sector employees with any protection against employer discipline. Even public employees enjoy only a limited protection from employment consequences as a result of their speech. The First Amendment protects a public employee from discipline or dismissal due to his or her speech only if: (1) 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.80

If a public employee is speaking as an employee, rather than as a citizen, or speaking about a personal employment related matter, rather than a matter public concern, the employee has no First Amendment protection from retaliation by the public employer. 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.

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.”81

81 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, one 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 in another case regarding MySpace postings on matters of private concern. The State of Kentucky’s decision to prohibit state employees from accessing blogs from state-owned computers, was held not to violate the First Amendment, because it was a reasonable restriction implemented in order to prevent employee inefficiency.

In a case involving a special education due process hearing officer who maintained a blog in which she discussed special education issues, a federal court dismissed her First Amendment claim, because the employee’s free speech interest was overridden by the employer’s interest in maintaining an impartial hearing process. The court held that there was sufficient evidence from which a jury could find that the hearing officer acted as a private citizen in maintaining the blog, and the parties did not dispute that the subject of the blog was a matter of public concern. However, in light of the employee’s employment as a hearing officer, the employer had an interest in ensuring that she maintained not only impartiality but also the appearance of impartiality. Her blog posed a legitimate threat to the efficient operation of the employer’s due process system, and so did not fall within the protection of the First Amendment.

Of course, in order to present a viable claim for violation of a public employee’s free speech rights, the employer must have taken some action against the employee as a result of his or her protected speech. A federal district court in Florida found that an employee satisfied the three-part test for First Amendment protection when he posted an internal office memo on his blog page, since he had obtained it through a lawful public records request, it dealt with a matter of public concern, and there was no evidence that the posting of the memo impacted the employer’s ability to carry out its functions efficiently. However, the court found that the employer would have suspended the employee regardless of this particular posting, because he also posted internal emails after he had been told that the investigation that was the subject of the emails was still under way and so the emails were confidential. Employer policy prohibited the disclosure of confidential materials, and that violations of the policy could warrant dismissal. Additionally, the employee violated the employer’s procurement policies and then misrepresented his actions to the employer. The court found, based

---

upon action taken against employees for similar misconduct, that the employer would have suspended the employee regardless of his First Amendment protected activity. \(^{87}\)

**IV. JUST CAUSE DETERMINATIONS**

Arbitrators generally apply traditional concepts of just cause to assess employees’ use of social media. Arbitrators will consider whether other employees have been disciplined similarly for similar conduct, the exact nature of the employee’s 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. Social media arises in grievance arbitration both where the electronic activity constitutes the alleged infraction, and where it merely provides evidence of another infraction, such as abuse of sick leave, harassment, and the like.

An example of the former situation is a case in which the arbitrator reduced to a suspension the discharge of a transit employee who sent racist jokes via text message to coworkers. 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. \(^{88}\) However, the suspension of a firefighter in another case who posted a demeaning rap song on the union’s website was upheld. 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.” \(^{89}\) In a similar case, an employee accessed non-work-related websites from the employer’s computer on work time, and printed out racist material. He inadvertently left a few pages of jammed in the printer, which were discovered by other employees. The arbitrator reduced the penalty in that case from a 20-day suspension to five days, in light of the fact that the employee did not intentionally leave the material for other employees to see. \(^{90}\)

The dismissal of a teacher was sustained where 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 of 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 that the websites

---

\(^{87}\) Id., 2009 U.S. Dist LEXIS 52257 at *38-*45.


referenced explicit sexual acts. In contrast, however, where there was an insufficient work nexus between internet pictures of teacher performing faux salacious acts and her work as a teacher, no just cause for discharge was found. As the arbitrator explained, “it did not directly involve either the school or her capacity to teach.”

A three-day suspension of a 21-year teacher for placing insensitive posts on his Facebook page alluding to a student’s excuse for late arrival to a performance was reduced to a reprimand. The arbitrator found it significant that the employee had a spotless discipline record, and that the posts were not made through employer email or communications systems, and were not intended to harass the student, who did not have access to the page. Also significant was the employer’s failure to establish that its anti-bullying policy was ever disseminated or posted.

A Head Start teacher who created a private Facebook “group” was fired, and her dismissal was upheld, because she posted comments that denigrated parents, students and staff in vulgar and profane terms, and included her endorsement of a “what appeared to be . . . racist threats toward a supervisor and threats toward” a coworker. The arbitrator determined that the employee’s conduct disrupted the team atmosphere that the employer sought to build, and violated the employer’s policies requiring respect for students and their families and against discriminatory conduct.

National origin-based harassment was found to justify the dismissal of an employee who posted derogatory information on his blog referring to his plant manager as a “German, green card terminator” and comparing him to Hitler.

An employee may even be disciplined because of information that is posted on the internet by someone else. For example, an arbitrator sustained the discharge of a teacher whose estranged wife posted nude photos of the teacher on social media sites and the photos 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. Another 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.

On the other hand, a termination was reduced to a 30-day suspension where an emergency room nurse posted on her Facebook page a photo showing

---

93 American Arbitration Association Award, reported at 2011 WL 1928139 (AAA) (Mazurak, 2011).
several $100 bills with the caption “The things you find on your patients with no jobs,” as well as a post stating that “[the employer] can GFY!!” The arbitrator found that the employer had failed to establish that the photo involved any actual patient, or that the employee herself had taken the photo. He found the second comment serious, but that the two incidents of misconduct did not warrant dismissal.98

In an example of a case in which the employee’s electronic activity provided evidence of another infraction, an 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, and sustained the grievance.99

An employee’s post-discharge posting on Facebook of a photo of the former employee burning his work attire provided the arbitrator with a basis to modify the remedy. The employee was reinstated without backpay, and with a warning concerning the Facebook posting. It was perhaps significant that in that case, the reason for the employee’s dismissal was his statement that he was “going to burn this f***ing place down.”100

V. CONCLUSION

Social media and other electronic forms of communication have significantly – perhaps irrevocably – changed our professional and social interactions in a very short period of time. When it comes to electronic communications that occur in or relate to the workplace, however, arbitral, administrative and judicial caselaw indicates that the “rules of the road” are slow to change. For the time being, at least, decisionmakers are applying existing principles that grew out of cases involving verbal or written communications before the advent of social media. As long as that is the case, employees and employers both would be well-advised to think before they post, monitor or promulgate social media policies.

98 American Arbitration Award, reported at 2010 WL 5583163 (AAA) (Lowe, 2010).
100 American Arbitration Association award, reported at 2011 WL 2099034 (AAA) (Doering, 2011).