

2012 Mid-Year Seminar
Personnel Section Meeting
April 22, 2012

Social Media & Electronic Communications and Employee Privacy – The Beat Goes On
Public Employer Compliance with Employee Privacy Rights & The Stored Communications Act

IMLA Personnel Section Chair, Daniel Crean, Pembroke, NH
Lisa Soronen, State & Local Legal Center

Local Government Employee Electronic Communication Privacy Rights
By Attorney Daniel D. Crean, Crean Law Office, Pembroke, NH

Crean Law Office
Pembroke, NH
creanlaw@comcast.net
www.creanlaw.com

N. H. Municipal Lawyers Association
Executive Director/General Counsel
nhmlaadmin@comcast.net
www.nhmla.org

©2012 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its Mid-Year Seminar held April 22-24, 2012, in Washington, D.N. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Local Government Employee Electronic Communication Privacy Rights

By Daniel D. Crean, Crean Law Office, Pembroke, NH
IMLA Personnel Section Chair

[Note: Portions of this paper are excerpted from materials provided during IMLA's Personnel Teleconference held on January 18, 2012.]

I. Public Employee Workplace Privacy (with a Brief Look at Public Employee Speech)

> "Imagine your deepest, darkest secret – a true, but deeply embarrassing, fact about yourself. Now suppose that you awake one morning to find this secret suddenly revealed to everyone you know, as well as dozens of strangers. Most of us would regard such a turn of events as a personal catastrophe. Given the unappealing nature of this scenario, and the ease with which juicy secrets can spread among people, one might expect that we would play our cards close to our vests, refusing to reveal these embarrassing details to anyone. Yet, it is likely that most readers have shared their most embarrassing details with other people: spouses, siblings, parents, best friends, clergy, psychiatrists, coworkers, or perhaps even strangers on Trans-Atlantic flights. Indeed, millions of Americans have shared their most intimate personal details with dozens of strangers, for example, by participating in a twelve-step group or seeking advice in an online chat room. By common parlance, we still consider these facts to be "secrets" even after we have revealed them to a handful of people. But do they remain secrets for the purposes of U.S. privacy law, such that a plaintiff can recover in tort against someone who discovers them through improper means or publishes them in a newspaper without her consent? If so, at what point does a fact "cross over" from being a "private matter" to a "public matter" whose widespread disclosure does not provide the plaintiff with a cause of action? Can something still be "private" if two people know about it? Five people?"[1]

An individual's right of privacy historically has involved considerations of both public disclosure of private facts and intrusion on seclusion.[2] Privacy rights also exist in the workplace, and concerns over privacy are magnified in the public sector workplace due to the public employer's status as an arm of government with respect to both First and Fourth Amendment protections and state constitutional equivalents.

A consistent, coherent body of law regarding the extent of privacy when individuals "choose" to share information with one or more persons has yet to be formulated. Courts, like legislatures and local government policy-makers, appear to be well behind technology in creating responses to the developed and evolving world of electronic communications and social media. While such a comprehensive legal approach does not appear to exist, there are bodies of fairly developed law that may provide guidance in looking at traditional rights in a technological age. Such a review may commence with the now fairly well-developed body of law regarding public employee speech and with the somewhat lesser-developed law of public employee privacy. Those reviews in turn may assist in setting a framework for guiding legal government attempts to create digital information management systems and policy.

A. Traditional Municipal Employee Speech Rights. Without going into great detail at this point, it is sufficient to summarize jurisprudence on the topic of public employee constitutional[3] speech

---

[1] Strahilevitz, "A Social Networks Theory of Privacy" American Law & Economics Association Annual Meetings, Year 2005, Paper 42, available at http://works.bepress.com/cgi/viewcontent.cgi?article=1019&context=james_grimmelmann.

[2] RESTATEMENT (SECOND) OF TORTS, § 652(D) (1977).

[3] Necessarily, these comments address only employee speech under the First Amendment. They do not address employee speech under state constitutions, though many states apply similar, if not identical, analysis. Also excluded from this discussion are state statutory provisions governing employee speech, such as whistleblower

rights and municipal employer rights by noting that local government employees (like state and federal employees) are protected to some degree when they are speaking on matters of public concern; but employers may take action, as employers, when speech has an unacceptable effect on the workplace.

The general rule, often described as the "*Pickering-Connick*"[4] rule, may be stated as follows:

> When speech by a public employee is involved, courts typically choreograph a three-step chaconne:
>
> 1. The first step is to determine whether the employee spoke as a citizen on a matter of public concern. . . .
> 2. The second step is to balance the employee's First Amendment interests against the interests of the government, as an employer, in providing effective and efficient services. . . .
> 3. At the third and final step, the employee must "show that the protected expression was a substantial or motivating factor in the adverse employment decision."[5] (formatting not in orginal)

To be encompassed under constitutional protection, employee speech also must address a matter of public concern, so that "mere" griping or simple dissatisfaction with work, e.g., a supervisor's attitude, is not protected speech. However, if the speech crosses an admittedly "movable" line, e.g., griping about a supervisor's conduct based on an illegal criterion such as age or gender, can arise to protected status. Similarly, statutes that protect employee conduct and speech, such as whistleblower protection or employee expression of the "right" of "full criticism,"[6] may limit employer controls.

U.S. Supreme Court and federal Circuit Court opinions have molded that basic rule into a set of principles and rules (which might be called *Pickering-Connick* "offspring") that may be summarized as follows:

- 1977: *Mt. Healthy City Board of Ed. v. Doyle*, 429 U.S. 274, confirmed that employers may use a defense based on non-speech related employee record;
- 1979: *Givhan v. School District*, 439 U.S. 410, First Amendment protects covered employee speech even if expressed privately and not broadcast publicly;
- 1976 & 1980: *Branti v. Finkel*, 445 U.S. 507; *Elrod v. Burns*, 427 U.S. 347, First Amendment protections do not apply to political, confidential, or policy-making positions.
- 1987: *Rankin v. McPherson*, 438 U.S. 378, employee speech may be cause for employment action if it has a detrimental impact on the work environment.

These earlier variations and refinements of the general rule were examined and further refined by *Garcetti*[7] and *City of Ontario*[8] which, respectively, noted that First Amendment protections may not extend to a public employee who is speaking as part of the employee's official duties, and that employers may adopt policies regarding electronic communications and discipline employees for violations. The latter case, importantly, also notes (a) that employer practices that conflict with an adopted policy may "trump" that policy and (b) employers may not have a "free hand" to obtain, review, and use all employee

---

protection statutes or those specifically protecting employee speech to a greater extent than the minimum protections afforded by the First Amendment, such as New Hampshire RSA chapter 98-E.

[4] The rule is named for the two U.S. Supreme Court cases that form the basis for current public employee speech doctrine: *Pickering v. Board of Education of Township High School District 205, Will County,* 391 U.S. 563 (1968), and C*onnick v. Myers,* 461 U.S. 138 (1983).

[5] *Foote v. Town of Bedford*, 642 F.3d 80 (2011).

[6] As protected by NH RSA 98-E:2.

[7] *Garcetti v. Ceballos,*547 U.S. 410 (2006).

[8] *City of Ontario v. Quon*, 660 U.S. __, 130 S.Ct. 2619 (2010).

electronic communications under the federal Stored Communications Act[9] (and, perhaps, under the employee privacy doctrine discussed in the next part of this paper).

B. Traditional Municipal Employee Privacy Rights. Here, it may be important to discuss federal and state interests separately. In last year's U.S. Supreme Court decision[10] involving employee workplace privacy, Justice Alito noted that the U.S. Supreme Court more than thirty years ago "referred broadly to a constitutional privacy interest in avoiding disclosure of personal matters. *Whalen* v. *Roe*, 429 U. S. 589, 599–600 (1977); *Nixo*n v. *Administrator of General Services*, 433 U. S. 425, 457 (1977)." At the outset, Alito premised his examination of the issues presented in the 2011 case as assuming (without deciding whether) the Constitution does in fact protect this interest. The *NASA* ruling focuses more specifically on applying this (presumed) Constitutional personal interest in the context of the case, and not on employee privacy more broadly stated, at least under federal jurisprudence.

While individual privacy became ingrained in common law jurisprudence during the twentieth century, its extension to the workplace, and public employment in particular, has been, and remains, an evolving development.[11] Workplace privacy protections may not be so widespread as to be considered fully commonplace, but some federal constitutional protection of employee privacy does exist under common law rights of privacy, at least where an employee may assert a reasonable expectation of privacy. The landmark case of *O'Connor v. Ortega*[12] extended Fourth Amendment privacy protection to the public workplace and allowed for a reasonable expectation of privacy in certain areas of the governmental workplace. However, that expectation of privacy is limited, as governmental employers may search or monitor to promote efficient operation and by adoption and implementation of limited and appropriate policies and practices. Yet, not all governmental actions will be upheld.

Thus, unless and until the Supreme Court actually reexamines *Ortega* and related cases, public employees may be presumed to have a federal constitutional right to be free from unreasonable searches of their persons, private personal property, and "private" areas of their workspaces under the Fourth Amendment. Usual formulations of this right to employment privacy often are derived from language used to describe the tort of invasion of privacy. (See text at footnote 2). As might be expected, the common law privacy elements most at issue in the workplace are those pertaining to intrusion on physical and mental solitude and public disclosure of private facts. Both of these interests may be seen as those that most often may be involved in employers seeking information about employee use of electronic communications and social media, as more fully discussed in section C of this paper.

States, either by common law or legislative enactment, may have created their own rules of privacy in general, and with respect to the workplace in particular. A detailed examination of such rules is beyond the scope of this paper and presentation. Practitioners are well advised to review state law and practices and then ensure that municipal policies and practices conform to them, and to recall that federal protections will constitute at least the minimum level of protection afforded to public employees.

For present purposes, it is sufficient to note that some practices likely will go beyond the limits of employer action (e.g., wholesale, unannounced searches that are little more than "fishing expeditions"). In addition, the scope of privacy and protections for employees may be affected, significantly, by the employer's creation of expectations of privacy. While a personnel policy cannot circumvent common law

---

[9] 18 U.S.C. § 2701, *et seq.* See materials for this session by Lisa Soronen.
[10] *NASA v. Nelson*, 562 U.S. __, 131 S.Ct. 746 (2011).
[11] For further information, please see the paper "*NASA v. Nelson: Dealing with Employee Privacy including Social Networking Privacy"* prepared for IMLA's 2011 Personnel Section Meeting at the Mid-Year Seminar, a copy of which may be obtained by contacting IMLA or this author.
[12] 480 U.S. 709 (1987).

or statutory protections, a clearly stated policy (and practices consistent with the policy) may limit employee expectations of workplace privacy, thereby enhancing the possibility that an employer's search of computer records or employee computer use would be deemed reasonable.

This paper includes a sample policy seeking to address employee expectations of privacy, particularly in the context of social media use. Naturally, any such policy should not be viewed as a "solution" that will apply in all workplaces or as being compliant with applicable jurisdictional privacy requirements. The goal of including a "sample" of this nature is to suggest areas that might be included in a public employer's policy and to note that some aspects of the policy might well be best stated as guidance for employee use of social media instead of employer-mandated directives.

C. Digital Information and Traditional Rights. As stated previously, court rulings and statutes generally do not yet address these traditional issues in the context of digital information and communications. These "shortcomings" are expressed in a variety of ways in terms of both incomplete guidance on handling electronic information and in incomplete or even "outdated" provisions. Similarly, state laws may conflict or at least may be uncertain with respect to how they "mesh" with federal laws such as the Stored Communications Act and the requirements to handle electronically stored information under federal court rules.

The difficulties that arise relate both to the nature of the media and the scope and speed with which they operate. *Facebook* did not exist when many, if not most, laws were written that now seek to govern the rights of employees and the data retention requirements associated with public records.[13]

Additional difficulties arise from the nature of electronic records and communications that creates "electronic footprints." Aside from the issue of retention and disclosure requirements, the traditional privacy and speech rights of public employees, in some way, will certainly address employer abilities to monitor use, obtain records of that use, and utilize that information in seeking to impose discipline or otherwise regulate employee communication in the workplace and, even more difficultly, outside the workplace, but in a manner that may be deemed to affect the workplace.

D. ESI, SCA & All That Jazz. The foregoing framework should be kept in mind as readers review the companion presentation prepared for this session by Lisa Soronen that addresses significant issues associated with the ability and duty to retrieve, search for, and retain Electronically Stored Information associated with public employment, along with the Stored Communications Act.

E. Social Media and Employee Communication – Policies and Controls. Notwithstanding the existence of employee rights in these areas, there are areas of conduct and communication by public employees that are legitimately subject to policy and control imposed by a local government employer. Likewise, it is evident that public employees retain protected rights of both speech and privacy – and those rights may extend to electronic communications such as social media, Internet access, email, and cellular phone uses.

Employer options with regard to exercising control and creating policy run the gamut from no control to outright prohibition of all such uses. Both extremes provide ample opportunity for liability and opportunities for challenge and litigation. The absence of policy subjects an employer to claims of

[13] Whether delineated as "Freedom of Information" or "Right-to-Know" laws, clear delineation of requirements to retain, organize, or provide access to electronic or digital information may be characterized most accurately as hazy. While statutes increasingly address retention and public access requirements associated with electronic documents and email, provisions directly addressing obligations with respect to employee social media or Internet use are, to be kind, in early stages of development.

arbitrary action and violation of both speech and privacy rights, particularly the latter by virtue of allowing employees to identify and formulate their own expectations of privacy.[14] Complete elimination of social media access in the workplace initially may be thought to enhance productivity, but further reflection would indicate that many employment tasks can be facilitated by legitimate Internet access and ease of email communication. In addition, reality suggests that an increasingly large segment of the workplace will not easily tolerate a workplace with such total restrictions.

The sample policy included here seeks to balance the exercise of public employee First Amendment rights of speech, religion or assembly and rights of workplace privacy with the requirements of the workplace. It is assumed that the employer will have adopted email/computer use policies to establish ground rules for employee use of employer-provided email/computer systems, including statements seeking to limit employee expectations of privacy in use of those systems. Employers who seek to adopt a social media use policy should be conversant with public employee First Amendment and privacy jurisprudence.

Why Adopt a Specific Social Media Policy? Workplace policies seek to govern conduct within the workplace, including those that govern use of email/computer systems. To some extent, those policies may effectively establish expectations and controls that apply to employee blogging, personal website and/or social media use accessed by use of the employer's system. Given the explosive growth of social media, employees, whether authorized or not, may use public workplace computers for personal activities.[15] To the extent that general computer use policies or practices permit or tolerate any personal use, employers must consider how social media use fits into the equation. Policies may distinguish unacceptable social media use from electronic communication viewed as acceptable workplace communication or unobjectionable "banter." Inclusion of social media guidance in a general computer use policy, while legally appropriate, may be insufficient to provide the degree of guidance needed to fully guide employees as to acceptable use and to provide useful defenses to challenges or other claims.

Even if personal use is prohibited or controlled, public employees may assert that social media comments about the workplace constitutes use for employment-related, not personal, purposes. Accordingly, and premised upon precedent involving public employee First Amendment and Fourth Amendment "privacy" rights, employers may wish to adopt a social media policy to limit employee expectations of privacy which continue to be the touchstone by which employer monitoring and control of employee behavior in the workplace may be measured, at least in this context.

Employee general conduct rules/policies often invoke common sense and accepted norms of behavior to address hostile environment issues (with regard to matters such as sexual harassment or discrimination) and to protect employer confidentiality. In addition, particularly in the public sector, employment policies are designed to maintain and enhance public confidence in, and respect for, government and its employees. Another focus is possible employer liability for statements made by employees that can lead to problems such as defamation, unauthorized representation, or disclosure of confidential information.

Technology allows individuals to make statements easily and anonymously on virtually any topic, including their employment. Comments can be made electronically by email or by posting on a weblog or individual website or any of the many social media sites. They may be posted from the workplace or

[14] As cited in parts A and B, employers may seek to narrow the boundaries of protections for employee conduct by establishing and enforcing policies that are designed to establish, identify, and communicate the extent of privacy that employees may legitimately expect in the workplace and in use of employer-furnished electronic communication devices.

[15] And for uses that are claimed, rightly or wrongly, to be associated with workplace functions.

elsewhere. In many respects, electronically-generated comments are not unlike any other speech made by an employee, so that courts likely will apply standard First and Fourth Amendment analysis[16] to public employee electronic speech. Social media use, though, is sufficiently different from "ordinary speech" that employers should consider establishing specific policies to address it.

Employees may assume they are protected by anonymity of electronic communication. Computer forensics can make comments easier to trace (so-called "electronic footprints"). Discovery rules involving social media defamation are evolving, but an employer's ability to use discovery perhaps can be facilitated by adopting a policy to limit privacy expectations for certain statements or conduct. Employers may be under a duty to ensure that records of electronic communications (including particularly ESI) are not deleted. The costs of recovering and producing ESI can be staggering and may be expected to be so in the absence of employer created guidance.

Employees consciously may identify themselves as public employees, may inadvertently disclose their status, or may consciously seek to avoid disclosing their identity and status. Even if an employee's message is straightforward, once the message is sent electronically, it can be altered as to identity of the source or its content. Employment social media policies cannot prevent such actions, but they **can** alert employees to the dangers inherent in electronic communication.

Keeping in mind that a public employer must respect employee rights and should avoid actions constituting (or perceived as) censorship, drawing a line between acceptable and unacceptable social media use is difficult. Whether employment is at-will or otherwise, public employers must be cognizant that discipline or dismissal for protected comment may lead not just to liability, but also to an unpleasant and unproductive work environment. Avoiding liability while guarding against unfettered negative commentary that adversely affects the workplace also justifies adopting a policy.

A social media policy should be adopted in coordination with email and computer use policies and any other policies or practices regarding other statements made by employees. Generally, though, a social media policy might cover:

(a) social media comments that involve the use of the employer's electronic computer system;

(b) social media comments that are conducted on company time or premises regardless of the system used;

(c) social media comments made by an employee in the course of performing duties as an employee; and

(d) "private" social media use that may expose the employer to liability or undue criticism, or that may adversely affect the workplace so as to constitute a potential for disruption or impair efficiency.

This latter criterion is derived from traditional public employee jurisprudence applying standard *Pickering*-*Connick* analysis, as discussed in part A of this paper.

A Sample Public Employee Social Media Policy Language

[The following sample policy, of course, should be adapted as appropriate to the needs and goals of the workplace. This sample language is **not** derived from any policy that has been reviewed by a court.]

(1) Purpose and Intent. Employer acknowledges that the public and employees may benefit from reasoned discussion on matters of public interest. This policy, like the email and computer use policy, does not seek to censor public discussion. However, Employer is justifiably concerned with the potential negative aspects of comment that may lead to liability, inefficiency, disclosure of confidential

[16] A major difficulty in creating an acceptable policy lies in the reality that both courts and legislatures may be considered as not being up to date on electronic communications, social media use, and blogging.

information, or adverse impact upon the workplace. This policy seeks to guide and advise employees as to the nature of appropriate and inappropriate social media use that may affect the public, the Employer, or other employees. This policy must be read in conjunction with other applicable policies and requirements. Employees who are uncertain about the scope or applicability of this policy may contact [insert positions or name of individual(s)] for guidance.

(2) Scope. This policy applies to social media use in a broad sense, including comments made to or by a public employee, whether made by email, contribution to a weblog, posting on a website (public or personal), or postings or other statements made on social media sites such as "Facebook." This policy also applies to comments made officially or unofficially in a public capacity and to comments made privately as stated herein. It also includes communications made by other forms of electronic communication (such as texting, instant messaging) when such communications are, or may be, posted or otherwise distributed more widely than to a single recipient.

(3) General Guidance On Social Media Use.

(a) Unless specifically and expressly authorized by an individual position description or by [department head/administrator/other designee], an employee:

(i) May not use Employer's computer system (including workstations, lap tops, or any portion of the system, software, or email system) for social media purposes. This prohibition applies to all social media use of any format or kind, and includes social media use of an employee's personal computer using Employer's system whether remotely or in the workplace.

(ii) May not use social media during the workday or while on Employer's premises.

(iii) May not use social media in any manner or at any time in a manner that identifies the individual as an employee of Employer to create an appearance, whether intended or not, that the employee is speaking as a representative of, agent for, or in any way on behalf of Employer, or that casts Employer and public employees in an improper, unjustified negative light.

(iv) May not use the municipal website to engage in social media comment.

(b) An employee must understand that social media use of any kind transmits information electronically and that the content may be viewed by anyone at any time. Therefore, employees cannot have any expectation of privacy in any social media comment. Employer may read, review, monitor, or copy social media comments. Employees who use social media within the workplace, or use the Employer's system (if and when allowed), must advise persons with whom they communicate that the communications may be deemed public records or documents under state law or may otherwise have to be disclosed in some manner. Employee further acknowledges that Employer may take all necessary steps to ascertain the identity of individual employees who engage in social media use, except for such uses that expressly constitute acceptable, non-work-related uses under this policy.

(c) Social media use by employees, whether authorized work-related or non-work-related use, should follow these general guidelines.

(i) Comments may not be used for personal or sexual harassment, unfounded accusations, or to create or contribute to a hostile work environment.

(ii) Comments may not disclose confidential information or personal information about others.

(iii) Unless authorized, comments may not display images of Employer's property, logo, seal, or premises or information of or about other employees.

(iv) Social media users must be wary of commentary about individuals and reputations.

(v) Unless prohibited by other policy provisions, social media comments may mention facts regarding incidents or events involving Employer if (a) that information has been reported to Employer and (b) the incident or event first has been reported through established media and the information is not confidential or false.

(vi) Social media users must avoid any activity or conduct that unjustly reflects adversely upon Employer and other employees, including but not limited to, pornography or illegal acts.

(vii) Social media comments may not be used for admission of, or comment upon, individual or Employer liability regarding any work-related matter. Employees are advised to use internal reporting mechanisms as set forth in [reference other policies that provide a means of reporting issues or filing complaints]. **[*Note*: Be wary of whistleblower laws].**

(viii) Social media users should ensure that opinions they express or relay are not capable of being seen as opinions of Employer or its officials or employees unless expressly authorized.

(ix) Social media users should not assume that anonymous blogging, or blogging conducted under a pseudonym, protects their identity from disclosure.

(4) Guidance for Non-Work-Related Social Media Use. Subject to the general guidelines and other provisions of this policy and other Employer policies, individual social media users acting on their own behalf, without identifying themselves as employees or in any way indicating their status as such, may make non-work-related social media comments, without prior review or approval by employer, provided that such activity does not constitute defamation or misrepresent or distort facts in such manner that it may cause negative effects for Employer, officials, or employees. Non-work-related social media use, as described in this paragraph, by an employee of Employer who is identified as such, shall conform to paragraph (5). [Again, employers must be wary of whistleblower protection statutes and laws that may otherwise protect employer statements of complaint or criticism.]

(5) Guidance for Non-Work-Related Social Media Use When User is Identified as Public Employee.

(a) When an employee engages in personal, non-work-related social media use, but the employee is identified as an employee of Employer, Employer has an interest in protecting itself, the public, and other employees from potentially adverse effects of such use.

(b) Accordingly, any such use clearly shall indicate that the content, opinions, and statements are solely those of the employee and do not necessarily represent the views of Employer, other employees, or the public.

(c) Such use may constitute a basis for discipline, including termination, if it:

(i) Contains defamatory or false content;

(ii) Creates or adds to an unreasonable adverse effect on the workplace;

(iii) Is represented or appears to be made as part of the official duties of the employee unless the official duties of the employee include the authority to engage in social media use in the manner in which the use occurred; or

(iv) Otherwise exposes Employer to liability or adversely affects public officials, employees, the public, or the governmental entity without due cause.

(6) *Guidance for "Unofficial" Work-Related Social Media Use.*

(a) The rights of public employees in some instances to make statements that constitute legitimate public comment on matters of public concern may be protected to an extent by constitutional guarantees of free speech, association, and religion. Those rights, however, are not unlimited and are subject to control, depending on the employee's position and duties and the effect of the statements.

(b) An employee may not state, imply, or suggest that social media comments are authorized by or represent Employer unless that is actually the case and the employee expressly has been authorized to make such statements.

(7) Guidance for "Official" Social Media Use. Social media use on behalf of Employer or as a representative or agent of Employer may be conducted only with specific written authorization of [identify individual or position]. The general guidelines and standards for official social media use require

that the comment be specifically authorized, honest, candid, and confined to the authorized statement or topic, and conducted in the manner authorized.

F. A Scenario for Discussion. One might question at the outset how and why an employee's posting on one of the social media sites in common use might ever be considered to be "private." Thus, a discussion on the following scenario may be deemed of value:

Supervisor:	Did you read what that jerk, Carly Complainer, wrote about me on Facebook?
HR Director:	You mean the one where she posted a photo of you at the holiday party and said you were harassing everything in sight?
Supervisor:	That's the one – I may have had one too many trips to the punch bowl, but I never did anything to anyone that doesn't happen every day as we have a little fun with each other. If my wife ever sees that posting, I could be in real trouble; it's a good thing she isn't real good at using the computer.
HR Director:	Well, it's probably a good lesson for you to watch out for cameras.
Supervisor:	You mean that's your response - for **me** to watch out! What about doing something about Carly? I want her to be at least suspended, if not fired.

- What, if any, speech and privacy rights are involved in the scenario?
- How might the employer "document" Carly's actions?
- Is there any issue involved in the employer viewing, copying and saving the Facebook posting?
- Would adoption of a policy governing employee use of social media help or hurt the employer's ability to act in such a situation?