INTERNATIONAL MUNICIPAL LAWYERS ASSOCIATION



Work Session VIII: Employment Law

Title:

"Sherlock Holmes in the 21st Century Workplace"
Monitoring and Surveillance of Public Employees in an Electronic Age

By

Presenter: Attorney Daniel D. Crean
Presenter's Title: Education & Training Manager
Presenter's Office: New Hampshire Public Risk Management Exchange
Concord, New Hampshire

© 2007 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 2007 Annual Conference, held October 28-31, 2007 in Nashville, Tennessee. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

"Sherlock Holmes in the 21st Century Workplace" Monitoring and Surveillance of Public Employees in an Electronic Age

By Attorney Daniel D. Crean

[Note: This paper examines selected issues associated with monitoring and surveillance in the public sector workplace. After a brief overview of workplace privacy in general and Constitutional protections applicable to the public sector, the paper focuses on monitoring and surveillance through electronic means, including email, phone and fax, video cameras, and newer forms of surveillance, including GPS and electronic toll monitoring. The focus on these technological formats is not intended to minimize the need to analyze and consider issues arising with respect to more traditional forms of surveillance.]

I. An Overview of Employment Monitoring and Surveillance: The Basics **Who, What, Why, Where, When and How.**

A. Purposes, Locations, and Methods. Employer perception of the need to monitor the workplace has increased along with the reality that workforce conduct has led to losses. Data from a variety of sources indicate that employee actions account for losses in such numbers that, today, those figures can no longer be treated as merely a cost of doing business.[1] The possibility of loss due to employee theft has been joined by losses attributable to fraud,[2] time wasting[3] and, now, workplace harassment, sexual and otherwise, particularly through the use of email and downloading from Internet sites. Liability to harassed employees has led employers to become more vigilant about workplace conduct. In turn, that vigilance has led to pressure to expand observation of employees beyond the days of "management by walking around."

The loss-prevention focus of traditional methods of employee surveillance generally utilized direct observation. Except for those instances such as the search for abuse of leave time, most observation occurred in connection with employee conduct during the workday. Some surveillance did occur outside the workplace when issues involved matters such as validity of workers compensation injuries. As technology has made its way into the workplace, opportunities for employee "mischief" have increased dramatically. Employers, particularly in the

---

[1] In 2001, employees stole $15.243 billion in inventory. In a 2002 report, nine of ten employer-respondents indicated they had been victims of computer crime. The two most expensive categories of theft were intellectual property ($170,827,000) and financial fraud ($115,753,000). An estimated 70-80 percent of computer crime is committed by employees against their employer. Source: Lane, *The Naked Employee*, American Management Association, 2003, at 12 -13.

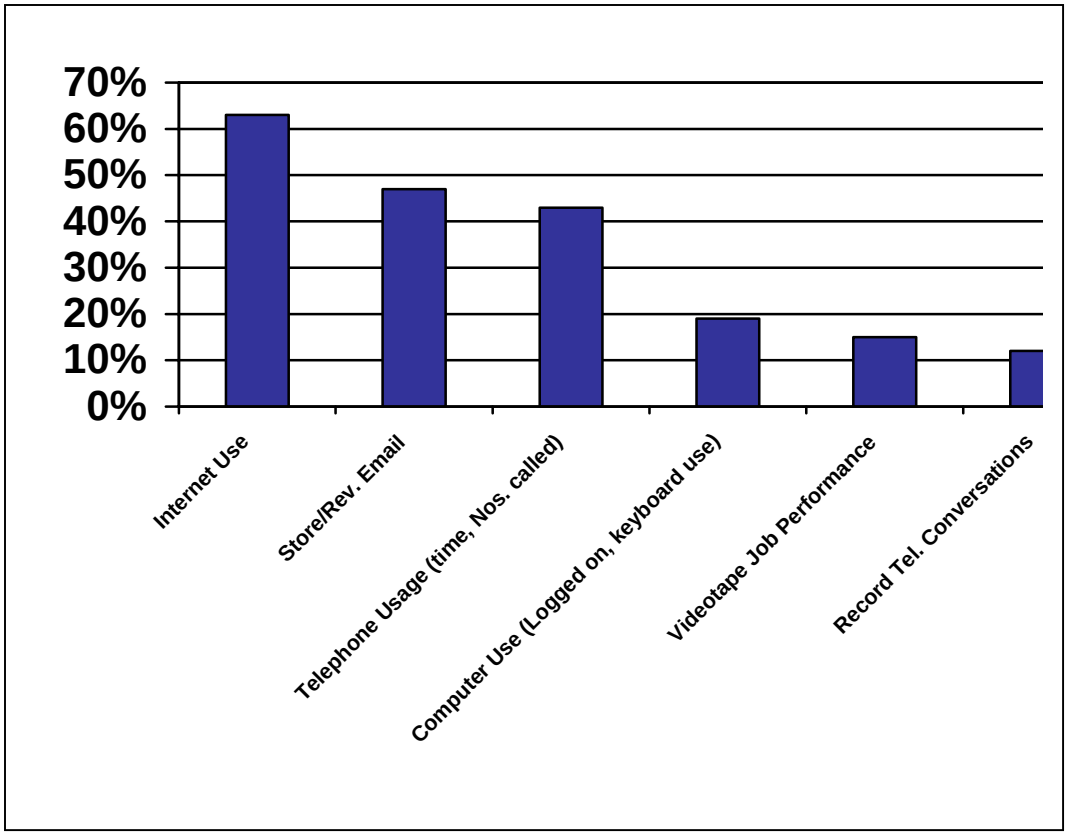
[2] The use of private detectives to observe the actions of employees "out" on workers' compensation has evolved to include observation of employees claiming the need for reasonable accommodation under the Americans with Disabilities Act and employees seeking to use the Family and Medical Leave Act.

[3] Apreo, the maker of *Anti-Game* software, claims that playing of workplace computer games costs employers more than $50 billion per year. *Ibid.* at 15.

private sector, responded to this conduct by implementing methods to observe and monitor employees' use of technology. (See Table 1.)

The formerly very limited "personal use" of technology in the workplace has expanded from occasional contact with home via the telephone ("Could you pick up a loaf of bread on the

Table 1. Private Sector Employee Monitoring
Source: Appleby Spaulding & Keegan, 2001 CBSNews.com



way home?") to widespread use of email[4] for both business and personal use and of the Internet to "chat," make travel reservations, participate in sports pools or fantasy leagues, "blog," and other less "benign" diversions.[5]

[4] As of May 2007, average American workers handled 142 emails per day (700 per week, 35,000 per year). By some estimates, that is expected to grow to 57,000 annually by 2010. Of course, not all of those emails are personal, unrelated to work. There can be no denying, though, that casual, non-business use of email is substantial and rising. Even business-related emails, though, can be the source of problems through actions such as inadvertently hitting "reply to all" or hitting "send" before the brain is fully engaged.

[5] Recently, a radio advertisement for a health provider touted the use of its website to access medical records and contact medical providers noting that it was no longer necessary to worry about time spent on personal phone calls from the office – to which one might respond: Is not working time spent on personal email as much of a concern to employers? Such seems to be the perception of computer communication.

Additionally, email and electronic documents can become a "mother lode" of evidence in litigation. With the relatively new federal electronic document discovery rules[6] (and existing and forthcoming state rules), employers need to (a) understand how employees use email and electronic documents, (b) establish procedures and policies regarding retention, storage, and deletion of email and electronic documents, and (c) create workable and cost-effective means of retrieving and producing email and electronic documents.[7]

In the public sector, employers also must address requirements of right-to-know or freedom-of-information laws with regard to retention of, and public access to, electronic communications and records. When records include confidential information, such as personnel files, employers must be prepared to separate information accordingly.

These actual and potential exposures have led employers to adopt a variety of methods to observe employee conduct. As discussed in more detail below, employee monitoring and surveillance appear to be more prevalent in the private sector. Yet, concerns about employer practices are not limited to the private sector. Indeed, public sector employers must address the additional Constitutional protections available for public sector employees.

B. The Rise of Concern with Employee Privacy.[8] Along with increased employer vigilance have come complaints about the scope of monitoring and surveillance and its intrusion on areas previously viewed by employees as being "personal turf." Complaints and concerns are not limited to employees and their unions (who have asserted that monitoring is a term and condition of employment over which bargaining must occur). Civil liberties and privacy advocates abound and employment practice lawyers regularly post articles on their websites about employer infringement of privacy (and, of course, their successes in obtaining redress for such injustices).[9]

Over time, limits arose with regard to direct observation of employees or searches of their "personal space." For example, restroom or dressing area monitoring simply went too far. Similarly, warrantless searches of employee briefcases were acknowledged as violating private space, while searching a desk drawer was a more questionable act. For reasons that would seem to defy logic, employees and privacy advocates assert that email and use of public computer systems to access Internet sites should be as protected from employer view as these other areas where employees may have developed expectations of privacy.

---

[6] *F.R.C.P. Rule 34*, et al.

[7] Morgan Stanley reportedly agreed to pay $15 million to settle charges by federal securities regulators that it failed to produce emails in several investigations, *Wall Street Journal*, March 26, 2007, at R10.

[8] Readers may wish to review an article entitled *Privacy and Governmental Workplace Monitoring* which I wrote for IMLA's Municipal Lawyer, Vol. 45, No. 2, March/April 2004.

[9] On July 30, 2007, a Google® search for the words "workplace privacy" returned in 0.15 seconds with 52,400,000 hits.

To place all of this in context, this paper now will review briefly the evolution of privacy in the workplace and Constitutional and statutory limitations on employer monitoring. It will then seek to apply the principles of workplace monitoring in a more conventional sense to the techniques and concerns of the public workplace in a technological era.

II. Privacy in the Workplace.

In 1931, George Bernard Shaw is said to have remarked about the United States:

> *An American has no sense of privacy. He does not know what it means. There is no such thing in this country.*[10]

Yet, the "Right to Privacy" as a formal legal concept is not novel. It predates Mr. Shaw's assessment, as privacy entered the popular American vocabulary when Attorneys Samuel Warren and Louis Brandeis authored an article for the HARVARD LAW REVIEW in 1890 entitled *The Right to Privacy*, which urged creation of privacy as a right to be protected by law.[11] After invasion of privacy gained acceptance in tort law,[12] notions of individual privacy found protection through court decisions,[13] express Constitutional provisions in some states, and legislation, though such protections often applied in limited contexts.[14]

Privacy as a primary legal concept has not developed uniformly or universally nor has it proceeded without controversy. By and large, though, privacy is now an accepted part of American jurisprudence. Indeed, many jurisdictions have extended individual privacy beyond residential environments so that it extends to workplaces in both the public and private sectors. Accordingly, a number of rules, created by both court decision and legislative enactment, have since sought to establish a definable line between legitimate employer interests and employee privacy.[15] In some instances, legislation has been enacted in response to perceived incursions on privacy in general; in others, legislation arose

---

[10] BARTLETT'S FAMILIAR QUOTATIONS 571 (16th Ed. 1992).

[11] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). See also
THE NAKED EMPLOYEE, *supra*, at 9.

[12] The Restatement of Torts contains four categories of invasion of privacy: (1) intrusion upon seclusion, (2) appropriation of identity, (3) disclosure of private facts, and (4) publicity that places another in a false light. McNulty, *Who is Watching Your Keystrokes?* II J. HIGH TECH. L 101 (2002) at 125.

[13] Though no provision of the Federal Constitution expressly protects individual privacy, the United States Supreme Court has long accorded privacy the status of Constitutional protection, e.g., *Katz v. U.S.*, 389 U.S. 347 (1967).

[14] The bedroom, for example. See *Griswold v. Connecticut*, 381 U.S. 479 (1965).

[15] According to McNulty's article (cited at note 9), as of 2002, twenty-five states have statutes or provisions within their state constitutions protecting the right to privacy.

in response to specific workplace practices that were seen to adversely affect employee privacy.

It is readily evident, therefore, that privacy rights impose at least some degree of restriction on employers generally, and public employers in particular, as to their ability to monitor employees. The statistics on employee surveillance and monitoring, at least in the private sector, suggest that employee privacy protections may not deter monitoring as much as might be expected.

While statistics on private sector practices are readily available[16], the paucity of information on employee surveillance and monitoring practices in the public sector is notable. Opportunity for wrongdoing, wasteful and unproductive pastimes, and similar conduct would not seem to differ markedly between private and public sectors, though potential for monetary losses might be perceived as being higher in the private sector. However, with the increase in public sector losses attributable to employee conduct, public sector employers can be expected to follow their private counterparts in expanding workplace monitoring. Given the ongoing and increasing issue of workplace harassment, public employers can be expected to become more vigilant to guard against improper conduct. The expansion of computer usage and Internet access in government workplaces similarly will engender the need for greater oversight.

The intersection of general privacy protection in the workplace with Constitutional protections in the public workplace makes it essential for public employers to proceed with caution. While caution must be exercised, employers must avoid an ostrich approach (head in the sand) to employee conduct that demonstrably exposes employers – and taxpayers – to financial loss.

III. Statutory Protections for Privacy.

Legislation protecting privacy can take several forms. It may arise in protections from specific actions such as wiretapping or eavesdropping that is not aimed directly at the workplace, but might be applied therein. Laws designed to protect personal information such as financial or medical information also have been enacted on both the federal and state levels, and some of these extend their reach to employers as well as the compilers and creators of the information such as credit agencies and medical providers.

The "good news" for public employers is that one hurdle for effective monitoring of employee electronic communications applicable to the private sector does not apply to local government employees. That hurdle is the Federal Electronic Communications Privacy Act.[17] Employers must be wary, though, of

---

[16] In 1999 the percentage of employers who electronically monitored their workers was 67%. Just two years later, in 2001, this number had increased to 78%. By 2003, 92% of employers were conducting some form of workplace monitoring. *Privacy Under Siege: Electronic Monitoring in the Workplace*, National Workrights Institute, copy available at www.workrights.org.

[17] 25 U.S.C. §2510, *et seq.*

state laws that may impose similar restrictions on employer monitoring of employee email and other communications such as blogging. Although each state law must be analyzed on its own, one possibly useful tool is to understand the difference between monitoring and intercepting. The former concept involves looking at records of communications (e.g., stored email, even email in transient, temporary storage) while the latter entails action that occurs contemporaneously or in close proximity to the actual communication (e.g., interception of email in transit). That latter type of action is more likely to bring employer action within the ambit of wiretapping and similar laws, at least according to some judicial analyses.[18]

IV. Constitutional Rights in the Public Workplace.

As noted above, the public employment arena must be examined from the additional perspective that the employer is deemed to be an arm of the state. Therefore, public employees are accorded additional protections based on the Bill of Rights to the United States Constitution. Of course, these first ten amendments seek to protect individuals from an over-intrusive government, and those protections apply to state and local governments by virtue of the Fourteenth Amendment. Public entities as employers do not lose their status as governmental entities. Hence, public employees have been found to have additional protections beyond the rights of workplace privacy that may exist for both public and private employees. Among these rights are those of freedom of speech, religion, and assembly afforded by the First Amendment and protections from unreasonable searches and searches established under the Fourth Amendment. Several state constitutions provide similar protections from governmental intrusion, but the materials for this session will focus generally on federal concerns.

Constitutional protections constitute a floor – a minimal level of protection. Statutes such as the federal anti-discrimination laws[19] restrict employer actions to control the workplace. State legislatures have enacted similar laws and some have broader reach than federal laws.[20] In addition, all states have enacted whistleblower protection laws that may protect employees from adverse consequences for speaking out on matters of public concern where constitutional protections may not exist.[21]

---

[18] E.g, *U.S. v. Councilman*, 245 F. Supp. 2d 319 (D. Mass 2003), overruled by First Circuit Court of appeals, after rehearing, see __ F. 3d __ (1st Cir. # 03-1383, August 11, 2005).

[19] Examples include the Civil Rights Act, the Americans with Disabilities Act, and the Age Discrimination in Employment Act. Federal law also regulates lie detector tests for employees, but that law does not apply to local government employees. Although religion and creed are two of the criteria protected under federal law, those issues are addressed only tangentially in these materials.

[20] New Hampshire's human rights law (NH RSA 354-A), for example, does not limit age protection to those over 40 as does federal law and includes sexual preference as a protected classification.

[21] Those interested in further reading on Whistleblower protection may wish to read *Whistleblowing in the Public Sector Workplace: From Snitch to Saint?* published in IMLA's magazine, MUNICIPAL LAWYER, vol. 47, No. 3, May/June 2003.

The modern day formulation of a governmental employer's ability to search an employee's workplace arises primarily from *O'Connor v. Ortega*,[22] after which standards regarding a governmental employer's workplace search are generally governed by two considerations:

- The employee's reasonable expectation of privacy; and
- Whether the search was reasonable under the circumstances.

Perhaps foremost in consideration of such an expectation is the existence of search-authorizing regulations, while two other major factors are the particular area searched[23] and the nature of the governmental workplace.[24] These standards apply to searches conducted for both non-investigatory purposes and investigation of employee misconduct.

With regard to workplace searches, relevant factors in determining the validity of a search include:

- Abandonment of privacy protection (such as tossing items in trash), though decisions narrowly construe an employee's actions;
- Property rights – generally the deciding factor relates not to any property or possessory interest in property but, rather, is decided on expectation of privacy factors;
- Existence, absence and clarity of search-authorizing policies or regulations;
- Purpose of the search – criminal or civil in nature; and
- Special factors, including nature of the workplace (e.g., medical, law enforcement).

Several state court rulings on this subject may be seen as being more restrictive of employee rights than federal court rulings, as they inquire also as to whether the privacy right being asserted is one that society, as a whole, is prepared to recognize as reasonable.[25] As a general rule, employees will bear the burden of demonstrating a reasonable expectation of privacy. Governmental employers may enhance their status considerably through adoption and implementation of policies realistically defining limited privacy expectations in the workplace.

Workplace systems and areas where policy adoption can assist in limiting employee claims of privacy expectations include: computer systems, telephone

---

[22] 480 U.S. 709 (1987). The employee, a psychiatrist, was found to have had a reasonable expectation of privacy in his office, desk, and file cabinet as those were not shared spaces, had been exclusively his for 17 years, contained personal items, and no personnel policies had been adopted regarding workplace privacy.

[23] An employee cubicle accessible by others is deemed a less intrusive place to search than one that looks into an employee's purse, coat, or even one's desk drawer.

[24] *Warrantless Search by Government Employers of Employee's Workplace Locker, Desk and the Like, as a Violation of Fourth Amendment Privacy Rights – Federal Cases*, 91 ALR Fed 226.

[25] *Employee Expectations of Privacy in the Workplace*, 18 ALR 6th 1.

systems, limited personal areas, work-related use of employee personal systems such as a home computer, and generation and retention of employment-related business records.

Workplace monitoring also may be viewed as a term or condition of employment. As such, and depending on jurisdictional laws, employer actions, such as installing video cameras, may be subject to collective bargaining.[26]

It is fair to conclude, therefore, that public employee privacy and employer monitoring practices will be a source of continuing and expanding conflict. This paper now discusses those conflicts with emphasis on constitutional issues as they relate to surveillance and monitoring in this era of electronic communication, data generation and retention, and word processing.

V. "Techno-Monitoring."

This segment provides some suggested considerations for employee monitoring involving the use of technology. In many instances, the private sector is already using at least some forms of these actions to varying degrees.[27] The public sector, perhaps due to search and seizure and First Amendment concerns, has been less prone to adopt some of these monitoring techniques. As losses from unproductive time, harassment, software piracy, copyright violation, and theft can be expected to continue to rise in the public sector, monitoring in the public sector likely will spread into areas previously visited, to a large extent, only in the private sector. The more traditional monitoring involving phone and fax communication has already been joined in many instances by surveillance of email and instant messaging. Video cameras, too, might be expanded beyond the public access areas of public offices where they made their appearance in response to violence directed at local officials and employees. As public employee use of mobile communications increases, so, too, might the perceived need to track employee locations through GPS monitoring.

A. The Eye. No, this is not some sophisticated hybrid computer search program. It is simply the human eyeball. Along the same lines as employees who access "adult" sites from work, some employees think nothing of downloading games, sending jokes, blogging, and even accessing their own personal websites using a workplace computer. "Careful" employees may label these cites so as to disguise them for inquiring eyes, while others seem oblivious to the notion that employer systems and working time ought not be used for personal pursuits. Assuming that an employer has adopted even a very basic policy announcing that computers are not the personal domain of employees, a simple "glance" at the employee's video screen desktop or computer directories would hardly constitute an invasion of privacy or unjustified search.

---

[26] E.g., *Brewers and Maltsters, Local Union No. 6 v. NLRB and Anheuser-Busch, Inc.*, 414 F.3d 36 (2005).

[27] See Table 1, *supra*.

Consider, though, an employer's potential dilemma when an employer has created a folder marked personal or confidential or with some other identification indicative of an intent that the file is private. If an employer has no computer use policy regarding such actions, the employee may have a legitimate expectation of privacy in that folder that would be violated by an unannounced search conducted without consent or a search warrant. Another issue arises once it is discovered that a folder contains personal information. An extensive policy (positively stating that employees who seek privacy in communications should not use the employer's communication systems) could deflect at least some of the challenges to employer surveillance of "personal" communications in the workplace.

B. Computer Searches. Basic searches can involve key words, file extensions, (".jpg" for photos; ".exe" for programs). Such searches should easily be able to turn up improper data and programs without running afoul of privacy or improper search concerns. More sophisticated software, such as *Anti-Game* (note 3), can monitor in greater depth and from remote locations.[28]

On a related front is the technique sometimes called computer forensics, referring to the common false belief that the ubiquitous trash can (aka recycle bin) actually removes a file from the computer. Much like a medical examiner, a computer forensics specialist can examine supposedly dead files and unearth the proverbial smoking gun. Of course, this type of evidence lies at much of the current debate and concern over federal and state electronic discovery rules as noted above. In addition, hidden data (sometimes called metadata) is observable (sometimes with very little effort) in electronic documents. Imprudently transmitted documents have been the source of financial losses in several instances.

Computer forensics is not necessarily brain surgery, although it can be viewed as looking into a computer's mental processing center and storage system. The difficulties lie primarily in sorting through the immense amount of data in the computer or system and eliminating irrelevant material. The emergence of new storage media including CDs, zip drives, flash drives, and external hard drives, of course, adds immense new storage space and users now have even less incentive to clean up hard drives and organize stored data. If adding on to a house were as easy as adding computer memory, we probably would never sort out "stuff" in our homes.

But, unlike household items, electronic storage is more durable. It remains in the computer until it is eventually overwritten or the hard drive is destroyed. The value of this data to employers and to opposing attorneys can be

[28] A 1997 U.S. Senate Bill proposed to enact "The Responsive Government Act" which would have required that all computer games be removed from government computers and prohibited governments from purchasing computers with pre-loaded games. The bill was attached to another senate bill but was removed by a committee of conference and did not become law.

huge. Accordingly, two new "professions" have arisen: one seeking to improve recovery or restoration of files (exemplified by "EnCase"), while the other seeks to permanently destroy data. (One program is called "Evidence Eliminator.) This latter category must be viewed in light of electronic records retention and discovery requirements in federal court and some state court rules, under the rules of professional conduct, and under public records laws.

Employer policies, therefore, should address not only usage of computer systems, but also the manner in which electronic documents and communications are stored, filed, organized, and retrieved.

C. Keystroke Monitoring. Keystroke monitoring has been around for a long time, at least since the time and motion studies pioneered by Frederick Taylor in the early 20th century. That form of monitoring, though, was aimed at speed. Today, computers can track not just speed but also content of what is typed, and, more significantly, can maintain records of dialog boxes and even take periodic snapshots of what is displayed on a computer screen.

According to *The Naked Employee*, one such program[29] "effectively record(s) every email (sent or unsent), Internet relay chat, or instant messenger session that takes place on the computer."[30] It can be configured for use with a webcam to take photos of the computer user, and its presence can be hidden effectively, as the program uses modules that change their names and the icons indicating that the program is operating. It can send information automatically on a regular basis or only when key words (e.g., pornography) are used. Another monitoring program[31] will detail the time an employee spends using applications, email and the Internet, and can be particularly useful in tracking, for example, telecommuters. According to *The Naked Employee*, legal barriers to the use of these monitoring programs do not exist under the Federal Electronic Communications Privacy Act, as the information collected is not "in transit" and employers argue that any privacy concerns of employees are outweighed by legitimate business concerns.[32]

E. Email. The sheer volume of employee email can make monitoring a nearly impossible dream. But, the costs and time incurred to monitor all email should not deter employers from announcing that they have the right to do so and that they will indeed do so as they see fit. A policy reserving the right to monitor can be made more effective by using sign-on or occasional "pop-up" reminders alerting employees that email in not private.

Even if an employer effectively alerts employees that email is not private, a concern may arise with regard to privacy rights of "outside" individuals with

---

[29] Called *Investigator* and available from WinWhatWhere.
[30] *The Naked Employee, supra,* at 128.
[31] *The Survey Suite* by Scalable Software.
[32] *The Naked Employee, supra,* at 129.

whom the employee is communicating.[33] Two defensive mechanisms may help to address those privacy concerns:

- Requiring employees who do communicate with others on personal matters to advise their contacts of the policy regarding monitoring (a variation of the "if you want privacy, don't use the employer's system" theme);
- Requiring the use of disclaimers in all email that the communication is subject to employer monitoring.

A key to success in this arena, though, is not just having such policy statements in place. Policy adoption must be accompanied by training and implementation. Employees can easily discern policies which are not enforced.

F. Internet Surfing.[34] Aside from wasted time, surfing can create real problems for employers. Just as one wonders at the continuing EEOC caseload involving sexual harassment claims, it seems that some employees will never understand the impropriety of accessing inappropriate websites using workplace computers.[35] Downloading inappropriate material onto a desktop or distributing it via internal email creates obvious exposures for environmental harassment claims.

But, even aside from these concerns, employers can face problems by employees attempting to use Internet content for positive purposes. The ease of copying material and reusing it internally or externally creates copyright exposures, not just for the employee but for the employer as well. Similarly, software applications may be downloaded and installed in a real effort to do a job better, but failure to obtain proper authorization or licensing creates another liability exposure for employers. Yet another concern arises with storage capacity in the system. Also, downloaded material may contain viruses or may otherwise harm or interfere with the employer's hardware and software.

These examples demonstrate that employee Internet access may create problems even when the employee's motivation is positive. Once again, employer vigilance is needed and monitoring may provide a degree of protection. That protection, though, may exist only after an incident causes damage. Thus, adoption of policies regarding Internet use, coupled with training and monitoring, will constitute a better protective arsenal.

---

[33] Justice Brandeis said "The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of persons at both ends of the line is invaded . . ." *Olmstead v. U.S.*, 277 U.S. 438 (1928) (Brandeis dissent at 478). The parallel to email interception deserves particular note.

[34] Generally, see *Expectation of Privacy in Internet Communications*, 92 ALR 5th 15; and Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 Business Lawyer #2, February 2002.

[35] In New Hampshire, for example, several assistant county attorneys were found to have accessed adult web sites using county computers. Several months ago, a Milwaukee newspaper reported that teacher had thousands of child pornographic pictures stored on a school computer.

G. Newer Forms of Surveillance. Telecommuting and mobile communications offer employers and employees opportunities to expand the workplace. While productivity may increase, opportunities for problems also increase. Employees working from home may not be "at home." Employers must decide if physical location is an issue, particularly if the employee has access to a network via their laptop or home computer. Using a home Internet connection may not be the safest protocol, but it is likely more secure than sitting in a coffee house, sipping a latte while using Wi-Fi access. For employers, knowing the location from which remote access is obtained can be a crucial loss prevention measure.

Cell phones are yet another device to keep in contact "24/7." Cell phone records may disclose information beyond time and location of persons called. They may well disclose the location of the user as well. Problems regarding privacy of personal communications will increase if an employer allows even limited personal use of an employer-provided cell phone in the same way that problems will exist when personal use is allowed of email or even conventional office phones.[36]

Employees who use employer-owned vehicles or who use their own vehicles for business purposes may find it convenient to stray from their appointed rounds. GPS equipped vehicles provide not only the ability to obtain directions. They also can transmit information about the location of vehicles. Employees whose whereabouts are tracked by a GPS system may not be aware that their employer is keeping an eye on them in this manner. Though case law or statutes do not appear to have addressed this form of surveillance as of yet, it can be expected that the validity of this form of monitoring will be governed by expectations of privacy and by the nature and extent of monitoring, particularly when the employee is "off the clock."

Employees who travel on business are perhaps more likely to use electronic toll payment devices such as EZ-Pass in the private sector. However, such devices may well be appropriate for public employees who work in areas with toll highways and who do not drive government vehicles that may be exempt from tolls. The review of toll payments may disclose information about wayward employees in much the same way as GPS devices. Similar concerns exist with regard to personal use of vehicles, though an employer certainly would justifiably be concerned if toll payments were being made for private trips.[37]

H. Fording the Castle Moat. The foregoing discussions of remote computer access, cell phone usage, and GPS and toll payment monitoring give rise to more general concerns with attempts to monitor employees outside the

[36] Employers and employees also should be mindful of the IRS' interest in treating as taxable benefits employer provided communications that may be used for personal purposes.

[37] Though relevance may be limited, one might take note of the recent disputes over access to toll records in divorce cases.

standard workplace. Indeed, one may question how long the phrase "standard workplace" will have meaning. As noted earlier, employers have sought to monitor employee conduct outside the workplace for workers compensation, ADA, and FMLA purposes. Privacy concerns are heightened when monitoring and surveillance extend to those areas, such as a person's residence, where privacy expectations are highest. In these instances, alerting an employee to the existence of surveillance will defeat the very purpose of monitoring the employee's activities. Covert surveillance can be the only effective means of uncovering inappropriate conduct.

The First Circuit addressed privacy concerns in a 2002 case.[38] A state trooper stated on his employment application that he did not use illegal drugs during the five-year period preceding his employment. While he was still in probationary status, a supervisor was given a videotape seized during a search that showed the trooper and others apparently smoking marijuana. He was interviewed and discharged. He challenged his termination, asserting, *inter alia*, that his termination resulted from a violation of the Massachusetts privacy law.[39] The Circuit Court had little problem finding that the privacy claim failed, as the conduct occurred in the presence of others and the defendants did not make or distribute the video – they merely watched it. More relevant to our present inquiry, though, the Court also ruled that in determining the reasonableness of an intrusion, an "employer's legitimate interest in determining the employees' effectiveness in their jobs should be balanced against the seriousness of the intrusion on the employees' privacy."

The New Hampshire Supreme Court had occasion to address the use of video surveillance of a classroom that was used in the prosecution of a school janitor for theft.[40] The Court rejected the challenge to the use of the video, holding that the defendant had no automatic standing under the New Hampshire Constitution's Search and Seizure limitations,[41] as he had no possessory interest in the classroom, the desk, or the money in the desk (that was alleged to have been stolen). Likewise, the defendant had no exclusive use and control over the classroom and he could not reasonably have an expectation of privacy in the classroom. On the other hand, the New Hampshire Court found (in a non-employment setting) that an individual could maintain an expectation of privacy in trash placed at curbside for refuse pick-up.[42]

---

[38] *Dasey v. Anderson, et als.*, 304 F.3d 148 (1st Cir. 2002).

[39] Mass. Gen. Laws ch. 214, §1B states that a person "shall have a right of action against unreasonable, substantial, or serious interference with his privacy" and protects people from "disclosure of facts . . . that are of a highly personal or intimate nature when there exists no legitimate, countervailing interest."

[40] *State v. McLellan*, 144 N.H. 602, 744 A.2d 611 (1999).

[41] N.H. Const., Pt. I, Art. 19.

[42] *State v. Goss*, 150 N.H. 46, 834 A.2d 316 (2003); see also *Reasonable Expectation of Privacy in Contents of Garbage in Trash Receptacle*, 62 ALR 5th 1.

As the workplace expands to include areas previously thought to be subject to possessory interests or under the exclusive use and control of individuals, tensions over employer needs to determine employee effectiveness, efficiency, and honesty can be expected to intensify.

E. Legal Considerations. Case law guidance on employee privacy and electronic surveillance, once sparse, is growing as might have been predicted given the rise in computer and other "modern" forms of workplace monitoring. In general, though, the public sector continues to be governed by *O'Connor v. Ortega* standards (reasonable expectation of privacy, reasonableness of search under the circumstances, scope and purpose of search in relation to workplace objectives). Private sector employers are not completely unfettered, as individual workplace privacy under common law or state statutes may limit the areas that may be searched or the extent and nature of searches. Of course, privacy and statutorily imposed limitations will apply to government employers in addition to Fourth Amendment considerations.

One factor then in determining the legality of surveillance undoubtedly will be the existence and contents of employer computer use policies and how they affect employee "reasonable expectations of privacy."

VI. Protections Afforded by Employer Policies.

Absent statutory changes that limit or expand employer/employee rights in the privacy arena, public employers perhaps are best advised to adopt and implement clear and comprehensive policies that will define and limit employee expectations of workplace privacy.

The appendix to this paper contains sample policies regarding (1) employee use of computers, email and Internet and (2) public employee blogging. Both of these policies were originally included in articles written for *Awareness in Action: The Journal of New Hampshire Public Risk Management*, a semi-annual periodical that is published by the New Hampshire Public Risk Management Exchange (Primex^3). For information on availability and subscriptions to the Journal please visit www.nhprimex.org and click on the publications link on the home page.

Appendices

Appendix A. Sample Employee Computer Use and Email Policy

[Note: This sample policy was adapted from a policy used by the former New Hampshire School Board Insurance Trust. It was included in an article entitled E-Government in New Hampshire printed in Issue #1 of the Primex^3 Journal of New Hampshire Public Risk Management, Awareness In Action.]

I. Introduction/Purpose Statements.

1. This policy governs access to and disclosure of electronic data composed, stored, sent or received by employees using the (Governmental Entity's) computer system. This policy is designed to protect the safety and security of the Entity's computer systems, including email and Internet use.

2. This policy is deemed to be a part of the Entity's personnel policies and will be enforced in accordance with the procedures stated in the personnel policies. Any violation of this policy will be deemed to be a violation of the personnel policies. Entity reserves the right to change this policy at any time.

3. All uses that are not otherwise permitted under this policy are prohibited.

II. Ownership and Control.

1. The computer hardware system, software and email system ("the system") are owned by Entity, and all messages or data composed, stored, sent or received using the system are and remain the property of Entity. Employee usage of the system is a revocable privilege provided for the purpose of facilitating performance of the employee's work. It is not the private property of any employee. For purposes of this policy, an employee's home computer, laptop or other equipment will be deemed to be part of the Entity's system to the extent that it uses the Entity's software or email system or is used for the performance of work for the Entity. Reasonable effort will be made to preserve an employee's privacy expectations with regard to such personal hardware, but it cannot be guaranteed. Employees who utilize their own hardware in this manner are conclusively deemed to understand this policy.

2. The computer system, including Internet access and the email system, is to be used for business purposes only. [Personal use is not authorized and shall not be conducted on the system, except with prior authorization.] or [Specify the limited nature of personal use allowed, indicating that employees should not expect any privacy in regard to such personal usage and that if employees seek privacy they should not use the Entity's system.]

3. The email system may not be used to solicit or proselytize for non-job-related purposes, including, but not limited to, use for commercial ventures, religious or political causes or outside organizations.

4. The transmission of any discriminatory, harassing or offensive material in any form, including electronic media, is prohibited. Material considered to be offensive and prohibited includes any message which contains sexual implications, racial slurs, gender-specific comments or any other comment that offensively addresses someone's age, gender, sexual orientation, religious or political belief, national origin, disability or other characteristic which is protected from discrimination by state or federal law.

5. The email system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information or similar materials without proper authorization.

6. Entity reserves, and may exercise without prior notice, the right to read, review, audit, intercept, access, or disclose any and all information on an

employee's computer system or messages created, received or sent over the email system for any purpose, even if coded or protected by password or other security device. Employees should not have any expectation of personal privacy with regard to their usage of the system. By using the Entity's computer system, software, email system and Internet access, the employee is deemed to have consented to this provision. Any employee who uses the system for any permitted personal communication shall advise the person with whom the employee is communicating of this monitoring policy and shall obtain that person's consent to the monitoring. Any employee who does not consent to this provision shall not be permitted such usage.

7. The confidentiality of any message or data should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. The use of passwords for security does not guarantee confidentiality, or that Entity will not retrieve it. All passwords must be disclosed to the computer systems administrator.

8. Any communications created, sent or retrieved using email may be read by individuals other than the intended recipient.

9. Notwithstanding Entity's right to retrieve and monitor any email messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any email that is not sent to them. Any exception to this policy must receive prior approval by the designated supervisor.

10. Entity has the authority to terminate or limit access to any program or hardware at any time.

11. Personal disks or data sources cannot be used on the system unless pre-approved by the computer systems administrator.

III. Confidentiality and Privacy.

1. Preservation of confidential and non-disclosure of private records is essential to the proper functioning of Entity. Employees shall read, understand and comply with this privacy and confidentiality policy.

2. All communications which are confidential shall not be disclosed intentionally, negligently or inadvertently. Confidential materials shall be handled and filed in accordance with the Entity's departmental directives.

3. Although employees have no expectation of privacy with regard to Entity's control of and access to the system, all employees shall treat other employees' workstations, computer files, email and data as personal and private to that other employee, except as required and appropriate for shared tasks or when appropriate to the employment context.

Acknowledgement of Receipt and Requirement to Comply. I acknowledge that I have read this policy, understand its provisions and agree to be bound by these provisions. I understand that all computer systems, telephonic and electronic communications systems and all information transmitted by, received from or stored in these systems is the property of Entity and that I have no expectation of privacy in connection with the use of the Entity's hardware, software, Internet

access and email. I also acknowledge that I have been given an adequate opportunity to consult with an attorney before signing this agreement and that I have received a copy of this agreement as signed by me.

Additional or Alternate Policy Language Examples.

Control/Ownership/Access. The computer systems are provided for Entity's governmental purposes only. Employees may not use the systems for personal use or for any offensive, unlawful or improper purpose, including but not limited to:

- Destruction or damage to equipment, software or data belonging to the Entity or others;
- Disruption or unauthorized use of accounts, access codes or identification numbers;
- Transmission of any unsolicited advertising, promotional materials or other forms of solicitation, including such activities as placing hypertext links to non-entity related web sites other than those requested or directly related to the functions of the Entity;
- Ignoring or disobeying policies and procedures established for specific network systems;
- Use of computer resources:
    - To send or store messages or materials with the intent to defraud, harass, defame or threaten others;
    - In ways which intentionally or unintentionally impede the computing activities of others (such activities include but are not limited to: disrupting another's use of computer resources, such as game playing; sending an excessive number of messages or emails; making or printing excessive copies of documents, files or programs; or introducing computer viruses of any type onto the computer resources);
    - That violates copyright, trademark or license agreements;
    - To violate another's privacy (including, but not limited to, accessing another user's account, identification number, password, electronic file, data or email; impersonation of any person or any communication under a false or unauthorized name);
    - For commercial purposes or personal financial gain; inappropriate mass mailing ("spamming"); tampering with any software protections or restrictions placed on computer applications or files; attempting to circumvent local or network system security measures; altering or attempting to alter system software or hardware configurations on either network systems or local computing devices; installing unauthorized software programs on entity-owned computing devices or network systems or using such programs;
    - To access adult-oriented sites that contain descriptions or depictions of a pornographic or offensive nature or that allow access to gambling facilities over the Internet.

Monitoring Usage. Entity reserves the right to monitor, access, change, delete, review or retrieve any information stored or transmitted on the system, including information which may have been deleted but still exists on the system.
Improper Usage. Any use of the system that violates the Entity's sexual harassment, anti-discrimination or other policies pertaining to respect for individuals and workplace conduct constitutes a violation of this policy.

Reporting Violations. Users are expected to report policy violations that they observe. Such reports should be made to a designated employee for investigation.

Appendix B. Sample Employee Blogging Policies
This sample Public Employee Blogging Policy was included in an article entitled Blogging in the Public Sector Workplace: Employee Right or Employee Bight that was printed in Issue #4 of the Primex[3] Journal of New Hampshire Public Risk Management, Awareness In Action.]

Preliminary Comment. The sample policy seeks to balance the exercise of public employee First Amendment rights of speech, religion or assembly with the requirements of the workplace. It is assumed that the employer has adopted email/computer use policies to establish ground rules for employee use of employer-provided email/computer systems. Employers who seek to adopt a blogging policy should be conversant with public employee First Amendment jurisprudence. Caution: This sample is not intended as legal guidance or advice. State law and practice may vary. As with any policy, specific legal guidance is recommended prior to adoption.

Why adopt a specific blogging 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 or personal website use accessed by use of the employer's system. Given the explosive growth of blogging and personal websites, employees, whether authorized or not, may use business computers for such personal activities. To the extent that general computer use policies or practices permit or tolerate any personal use, employers must consider how blogging fits into the equation. Policies may distinguish unacceptable blogging from electronic communication viewed as acceptable workplace communication or banter.

Even if personal use is prohibited or controlled, public employees may assert that blogging 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 blogging/website policy to limit employee expectation of privacy which continues 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 (with regard to matters such as sexual harassment or discrimination) and to protect employer confidentiality. In addition, particularly in the public sector, employment policies seek to maintain 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 or unauthorized representation.

Technology allows individuals to easily and anonymously make statements on virtually any topic, including their employment. Comments can be made electronically by email or by posting on a weblog or individual website and may be posted from the workplace or elsewhere. In many respects, electronically generated comments are not unlike any other speech made by an employee so that courts will apply standard First Amendment analysis to public employee electronic speech. Blogging, 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 such comments easier to trace. Discovery rules concerning defamation by blogging are evolving, but an employer's ability to use discovery can perhaps be facilitated by adopting a policy to limit privacy expectations for certain statements or conduct. Employees may consciously 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 straight-forward, once the message is sent electronically it can be altered as to identity of the source or its content. Employment blogging policies cannot prevent such actions but 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 blogging can be 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 the policy.

Scope and Approach of Policy. A blogging policy should be adopted in coordination with email and computer use policies and any other policies or practices governing any type of statements made by employees. Generally, though, a blogging policy might cover blogging that (a) involves the use of the employer's electronic computer system; (b) is conducted on company time or premises regardless of the system used; (c) is made by an employee in the course of performing duties as an employee; and (d) "private" blogging 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.[43]

Sample Policy Language

(1) Purpose and Intent. Employer acknowledges that the public and employees benefit from honest debate on matters of public interest. This policy, like the email and computer use policy, does not seek to censor public debate. However, Employer is justifiably concerned with the potential negative aspects of comment that may lead to liability, inefficiency, or adverse impact upon the workplace. This policy advises employees as to the nature of appropriate blogging that may affect the public, Employer and 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 name of individual(s)] for guidance].

(2) Scope. This policy applies to "blogging" in a broad sense including comments made to or by a public employee whether made by email, contribution to a weblog, or posting on a website (public or personal). This policy also applies to blogging statements made officially or unofficially in a public capacity and to statements made privately.

(3) General Guidance.

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

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

(2) May not blog during the workday or while on Employer's premises.

(3) May not blog 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.

(4) May not use the municipal website to engage in blogging.

---

[43] As an aside, some employers have begun to conduct background checks for prospective and even current employees for profiles or personal logs on networking sites or personally-owned sites. Such searches can be as simple as using a search engine or may involve a more in-depth comprehensive search. Given the nature of public employee speech rights, it may be advisable to at least alert employees to the possibility that such searches may occur. It is advisable, of course, that such searches be conducted ethically, based on job-related matters in accordance with First Amendment public employee speech principles.

(b) An employee must understand that blogging 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 blog, and Employer may read, review, monitor, or copy blogs. Employee further acknowledges that Employer may take all necessary steps to ascertain the identity of individual employees who engage in blogging, except for blogging that expressly constitutes non-work related blogging under this policy.

(c) Employee bloggers should follow these standards.

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

(2) Blogs may not disclose confidential or personal information about others.

(3) Unless authorized, blogs may not display images of Employer's property, equipment, apparel, or premises or of other employees.

(4) Bloggers must be wary of commentary about individuals and reputations.

(5) Unless prohibited by other policy provisions, blogs may mention facts regarding incidents or events involving Employer if the incident or event has first been reported through established media and the information is not confidential. Blogs may be used for purposes protected by state or federal law.

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

(7) Blogs may not be used for admission of or comment upon individual or Employer liability regarding any work-related matter. Employees shall use internal reporting mechanisms as set forth in [reference other policies]. [NOTE : Be wary of whistleblower laws].

(8) Bloggers should ensure that opinions are not capable of being seen as opinions of Employer or its officials or employees.

(9) Bloggers should not assume that anonymous blogging, or blogging conducted under a pseudonym, protects their identity from disclosure.

(4) Guidance for Non-Work-Related Blogging.

(a) Subject to the general guidelines and other policy provisions, individual bloggers acting on their own behalf, without identifying themselves as employees or in any way indicating their status as such, may make non-work-related blog 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-job related blogging as described in this paragraph by an employee of Employer who is identified as such shall conform to paragraph (5).

(5) Guidance for Non-Work Related-Blogging When Blogger Identified as Public Employee.

(a) When an employee engages in personal, non-job related blogging, 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 blogging.

(b) Accordingly, employee agrees that any such blogging shall clearly 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 blogging may constitute a basis for discipline, including termination, if it:

(1) Contains defamatory or false content,

(2) Creates an unreasonable adverse effect on the workplace;

(3) 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 blogging in the manner in which the blogging occurred; or

(4) 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 Blogging.

(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 by Constitutional guarantees of free speech, association, or 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 blogging is authorized by or represents Employer unless that is actually the case and the employee has expressly been authorized to make such statements.

(7) Guidance for Official Blogging. Blogging on behalf of Employer or as a representative or agent of Employer may be conducted only with specific written authorization of [identify individual]. The general guidelines and standards for official blogging require that the blog be specifically authorized, honest and candid, and confined to the authorized statement or topic, and conducted in the manner authorized.

About the Author
Attorney Daniel D. Crean
New Hampshire Public Risk Management Exchange (Primex[3]) Concord, NH

As Education and Training Manager, Dan's primary duties include design and implementation of educational risk management programs for local government entities. He also edits Awareness in Action: The Journal of New Hampshire Public Risk Management. Dan maintains a private municipal law practice, and teaches Land Use as an adjunct faculty member at Franklin Pierce Law Center in Concord, NH.

Dan has served multiple terms as chair of the NH Bar Association's Municipal and Governmental Law Section and currently chairs the NH Municipal Lawyers Association. He is IMLA's New

Hampshire State Chair and reporter for the IMLA Personnel Section. Several of his articles have appeared in Municipal Lawyer and the New Hampshire Bar Journal.

After completing a term as Selectman, Dan joined the Planning Board in the Town of Pembroke. He has served on many municipal, regional, and state boards and commissions. Dan has been President of the Yale Alumni Club of New Hampshire. In 1994, he co-founded the Granite State Symphony Orchestra for which he continues to write program notes. Dan also hosts a weekly classical music radio show for a local radio station.