E-mails and the Internet in the Workplace- New Threats to Employers

Matthew J. Giacobbe, Esq.
Scarinci & Hollenbeck, LLC

Topics to be Discussed

- Employee Productivity
- Employee Technology Misuse
- Policies and Monitoring
- Hostile work Environment
- Open Public Records Act
- Endangering the Municipal Network
- Technology Staff
- E-mail Disclaimers
- Privacy Interests

Employee Practices

- 61% of employees access personal e-mail at work.
- 41% use instant messaging.
- Danger Points
  - Indiscrete use of internet and e-mail
  - Inappropriate and illegal activities conducted online (pornography, gambling, etc.)
  - Hostile workplace issues, harassment, discrimination
  - Accidental disclosure of municipal information
  - Abuse of municipal resources

You provide Internet access to employees to hopefully allow them to be more productive.

- 70% of adult websites are hit between the hours of 9am and 5pm.
- Recent findings of a Vault.com survey:

  37.1% said they surf the Web “constantly” at work.

  31.9% said they surf a few times a day at work.

  21.3% said they surf a few times a week at work.

  9.7% said they never surf at work.

- Not only do employees surf sex sites but they also visit sports sites like espn.com, bid on eBay.com, trade stocks on etrade.com, shop online at avon.com or just send tasteless jokes to their co-workers.
- This type of misuse not only hurts employee job performance but increases threats to information security and drains valuable network and municipal resources.

Hostile Work Environment

- Receipt of pornographic e-mail may subject the employer to liability for harassment.

"the workplace is permeated with discriminatory intimidation, ridicule, and insult … that is sufficiently severe or pervasive to alter the conditions of the victim's employment and create an abusive work environment …."

Harris v. Forklift Systems, Inc., 510 U.S. 17 (1993)

Hostile Work Environment

- Sexual harassment/hostile work environment liability of employees can be direct or indirect.

  1. Direct liability occurs for example when a supervisor makes a habit of forwarding racially or sexually offensive email.

  2. Indirect liability occurs for example when the employer is on notice that its employees are receiving pornographic email. The employer will be liable for allowing such email into the workplace, as there are solutions the for these problems.

- The New Jersey Supreme Court in Blakey v. Continental Airlines, 164 N.J. 38 (June 2000), held the employer liable of a hostile work environment for items posted on a work related electronic bulletin. The employees were post defamatory and harassing messages and the employer had a duty for failing to monitor and prevent such inappropriate use of the bulletin.

Defenses to Sexual Harassment

An employer may establish an "affirmative defense" by showing it had a specific policy concerning e-mail and that it responded promptly to potential harassment and discrimination claims.

Internet and e-mail policies are essential for any municipality with e-mailing and online capabilities.

You've Got Mail

- Disclosure of e-mail due to the Open Public Records Act. (N.J.S.A. 47A:1-1 *et seq*.)
- A government record is a physical record that has a government purpose. Under OPRA a record may be any paper, written or printed book, document, drawing, map, plan, photograph, microfilm, data-processed or image processed document, information stored or maintained electronically or by sound recording.
- Meyers v. Borough of Fair Lawn, (decided December 8, 2005/ GRC Complaint 2005-127)

You've Got Mail

- Email created by municipalities employers/employees and agencies in the course of official business can be considered a type of government record. Email communication can be considered similar to paper based mail. The actual contents of the email will determine if it is a government record or not.
- Treat email as a one way communication. Limit discussion to two (2) members. The more governing members involved in an email communication will begin to open the Open Public Meetings Act; as a possible quorum will be making and discussing municipal decisions. **Have a NO FORWARDING RULE!!!**

Monitoring Employee Use

- Employee Privacy Rights?

  -Fourth Amendment protections

  -Private cause of action

  -Wiretapping laws

  -Finding things you wish you hadn't

  -Becoming the Internet police

- Before You Monitor

  -Notify employees

  -Set standards for what you plan to monitor

  -Decide who will review reports and what actions might be taken.

  -Use caution in your review

E-mail and Internet Monitoring

- Federal Rule: Electronic Communications Privacy Act ("ECPA") allows Internet and e-mail monitoring including real-time "interception" under following exceptions:

  -Consent; "ordinary course of business"; "service provider"

  -Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 107 (3rd Cir. 2003) confirmed that employers can access employee's "stored" electronic communications under ECPA.
- General State Rule: No reasonable expectation of privacy in employer supplied e-mail or workplace Internet use. (Smyth v. Pillsbury Co.)

Employees Privacy Interests

- An employee has no legitimate expectation of privacy in contents of his workplace computer where the employer has notified employees that their computer activities could be monitored. United States v. Simons
- No Fourth Amendment right to privacy!

E-mail Disclaimers

- A disclaimer doesn't make public information private or confidential.
- It might create false sense of security.
- The message loses importance when it’s “boiler plate.”

Computer Use Policies

See Attached Sample

- Who can use the municipal equipment
- When can a municipal employee use it
- Personal use of the Internet
- Personal use of the e-mail
- E-mail content and language
- E-mail attachments and links
- Spam and junk
- Instant messaging
- Software downloads or purchases
- Password management
- Where and how to save documents, e-mails, etc.
- Ramifications for policy violation
- Plans for monitoring employee computer use
- Privacy expectations