



Legal and Policy Issues - Privacy Concerns in the Workplace



Introduction – “Big Brother” Concerns

- 50+ years ago - George Orwell's *Nineteen Eight-Four*
- Orwell described a society of continuous surveillance by authorities.
- "Big Brother" has entered general usage and is often heard in workplaces to describe company monitoring and surveillance activities.
- Employees often believe employers have no legal right to invade what they regard as their right to privacy.
- For the most part, their belief is misplaced.



“Right of Privacy” in the Workplace?

- In the broad context, the “right of privacy” is an individual’s right to be free from intrusion into his or her private and personal matters.
- In the employment context, such rights are limited – some are clearly protected by statutory law (i.e., medical information, personally identifiable information which could enable identity theft, etc.); but others are “created” by common law development (invasion of privacy and infliction of emotional distress causes of action, or “torts”).
- From a technology context we have the ability to monitor our employee’s activities with a level of detail that we never could have imagined – The question is: When should we, if at all?



Sources of Privacy Protections

There are four primary sources of privacy rights:

- 1. The U.S. Constitution's Bill of Rights** and subsequent amendments as well as some state constitutions have been interpreted to provide privacy protections.
- 2. Federal laws** – The following are major federal laws that address specific aspects of privacy pertaining to employment:
 - **Americans with Disabilities Act (ADA)** – regulates use of medical information, maintenance of medical documents and access.
 - **Fair Credit Reporting Act (FCRA)** – restricts the use and requires disclosure of the contents of investigative consumer reports by employers.



Sources of Privacy Protections (cont'd)

- **Federal Wiretapping Act/Electronic Communications Privacy Act** – Prohibits the intentional interception or disclosure of any wire, oral or electronic communication where there is a reasonable expectation of privacy. There are two exceptions, however: 1) if one party consents to the monitoring; and 2) businesses are permitted to use equipment to monitor communications within the ordinary course of business.
- **Health Insurance Portability and Accountability Act (HIPPA)** – Regulates the use and disclosure of protected health information by employers with health plans.



Sources of Privacy Protections (cont'd)

3. State Laws – Some state laws restrict employer access to information and regulate employer conduct; in North Carolina, examples include:

- **North Carolina Financial Privacy Act – limits circumstances under which a person’s financial information may be disclosed, even to the government**
- **North Carolina Identify Theft Protection Act – enacts safeguards for personal identifying information and a mechanism for individuals to obtain judicial relief for unauthorized disclosure of such information**
- **North Carolina Electric Surveillance Act – forbids “interception” of communications unless one party to the conversation is aware and consents (means caller or recipient may record the other without the other’s knowledge)**
 - **“Interception” must be willful, and there are exceptions for employers for accessing calls on business phone equipment for business purposes**



Sources of Privacy Protections (cont'd)

4. Common law (Case Law) – Privacy causes of action recognized in NC (so far) include:

- **Unreasonable intrusion into the seclusion of the employee** – situations where the employee had a reasonable expectation of privacy, the employer's intrusion was offensive and not justified by business necessity. *Examples: non-HR or supervisory employees accessing another's personnel file; "hidden camera" surveillance of bathrooms, changing rooms and other areas where employee's have an expectation of privacy*
- **Unauthorized use of the employee's name or likeness for the benefit of the employer.** *Example: misappropriation of one's likeness, such as for use in promotional materials or testimonials, generally resolved by obtaining pre-use consent*
- **Privacy concerns also arise in context of infliction of emotional distress torts.** *Increasingly, a catch-all for suits alleging humiliation caused by accessing personal information (husband accessing wife's psychiatric records)*



Electronic Monitoring

1. Employers are increasingly able and willing to monitor employees, using:
 - Telephones
 - Computer usage.
 - Electronic mail (E-mail)
 - Location through GPS
 - Activities through video recording devices such as drive-cam or security cameras
2. If not abused for personal (or prurient) interests, employers generally enjoy such rights, particularly if the employer:
 - Gives notice or warning (through policy or other published notice, such as email or “pop-up” message)
 - Obtains consent (or declares it as a condition of using work equipment)



Electronic Monitoring

Computer Usage:

- Computer software programs now enable employers to monitor each employee's computer and file folders
- Can monitor Internet usage, and measure employees word processing or data entry speed by monitoring keystroke pace and volume
- Can keep track of the amount of time an employee spends away from the computer
- As the employer owns the computers and provides the Internet access, it may legally conduct this type of monitoring
- If these measures are implemented, suggested practice is to have a written policy stating employer's right to monitor computer equipment and usage and that employees should have no expectation of privacy when using it
- When this type of monitoring reveals behavior that is illegal and may place others at risk, the information may require additional action on the part of the employer. (Stalking behavior, child pornography, workplace violence – USGA example)



Electronic Monitoring

Electronic Mail (E-Mail):

- Employees should be advised that they enjoy no expectation of privacy in use of E-mail systems on company equipment, as the employer owns the systems and is allowed to review such contents
- Messages sent within the company as well as those that are from an employee's computer externally can be subject to monitoring
- Most employers allow employees to use e-mail for incidental personal use
- In cases where employers are exposed to personal information that may serve to embarrass or humiliate the employee, and that information does not implicate legitimate business interests (e.g., business ethics and goals, protection of proprietary/confidential information, violation of company policy), the employer's representatives should stop reading or reviewing such personal information and hold that information confidential
- When conducted in normal course of business, no apparent requirement to disclose to employee that such access occurred – but again, prior notice or policy always a good idea



Before you act, keep in mind.....

- Be consistent - What is acceptable for your favorite employee must be acceptable for your least favorite
- Specific request for monitoring or activity sweeps should be tied back to business necessity or for cause such as multiple complaints about inappropriate web surfing, unusual virus activity - these standards should be applied equally and vetted by HR and/or Legal
- The best protection is a well defined policy that explains the types of monitoring/surveillance the employer may utilize, and requires a signed acknowledgment by the employee that work and personal communication using company resources can and will be accessed if prompted by business necessity