I. Issues Surrounding Email/Computer Monitoring and Searches of an Employee's Property

In recent years, employers have had to become concerned with protecting their legitimate business interests while making sure to acknowledge and not violate the privacy rights of their employees. This article focuses on email/computer monitoring and searches of an employee's property.

While it is by no means exhaustive, the attempt of this paper is to provide and introduction to, and an outline of, the various issues which arise with respect to these areas, and, provide practical insights beneficial to employers.

a. Email and Computer Monitoring

Most employers have a legitimate need to monitor their employees' usage of email and their computer, particularly the internet, while the employee is at work. Employers must protect their assets, monitor employee productivity, and ensure that employees do not engage in conduct - - such as harassing, offensive or violent conduct - - which may expose the employer to liability. But monitoring an employee's use of the email system and the internet must be done carefully to avoid infringing an employee's privacy rights.[1] Although privacy case law has tended to arise from he common law of the states, two federal statutes also affect an employer's ability to monitor its employees email and computer usage.

The National Labor Relations Act ("NLRA")[2] prohibits an employer from restraining or interfering with employees' right to engage in union activity or other protected concerted activity conducted for mutual aid or protection, even if the facility or company is a non-union work-site. Monitoring employees' on-line usage may chill them from organizing or engaging in union activity, and will violate the NLRA if only some,

---

[1] Spying on Employees: What You Can and Can't Do, HR Hero, June 2003.
[2] 29 U.S.C. §§ 157-158.

but not other, non-business uses of the computer are permitted or monitored. If the employer is already a unionized facility, it should bargain with the union over the installation and use of monitoring devices. But regardless of whether the employer is a unionized facility or not, it must have an objectionably reasonable basis and standard for monitoring email and computer usage.

The Electronic Communications Privacy Act of 1968 ("ECPA"),[3] commonly known as the Federal Wiretapping Act, governs the interception or acquisition of the contents of electronic communications, such as telephone calls or emails. But despite the general prohibitions of the ECPA, employers may generally monitor email and internet usage if the employee has consented to the monitoring.[4] Consent is usually obtained by having the employee execute an acknowledgment of a computer and internet usage policy which makes clear that searches may occur, and that the employee has no reasonable expectation of privacy in the data stored on the office computer, or in any other communication medium. The policy should also make it clear that computers are to be used only for business purposes, and it should strictly prohibit unauthorized use of email or the internet for any other purpose, including but not limited to, downloading pornographic, offensive, or harassing communications, copyrighted or trade secret information, or any other non-business related information. The policy should also prohibit any attempt to appropriate the employer's trade secrets or copyrighted information, or to disable or compromise the security of information contained in the company's computers. The employer should also make it clear that passwords are intended simply to prevent outsiders from obtaining access to information on the

[3] 18 U.S.C. § 2510 et. seq.
[4] 18 U.S.C. § 2511(2)(d).

employer's system, but are not an indication that the employee has any privacy rights in the contents on the computer. Requiring employees to disclose their passwords to management will further make that clear.[5]

To make sure the policy is taken seriously, it should also note that any violation can result in disciplinary action up to and including termination, and the employer must ensure that it is in fact enforcing the policy consistently. A sample computer and internet usage policy is attached as **Exhibit A** to this article.

New Jersey has an analogous statute to the ECPA. The New Jersey Wire Tapping and Electronic Control Act, prohibits third parties from gaining unauthorized access to, or disclosure of, emails.[6] However, there are two exceptions to the statute that morph the employee protections contained in the statute with regard to the employment context. The first exception allows for unauthorized access if the inspection was done in the normal course of business for business purposes or if the inspection was done to protect the employer's rights or property. The second exception applies to monitoring that is consented to by one of the parties to the communication.

In the State of New Jersey, the Supreme Court addressed the right to privacy surrounding email and internet use and discussed what notice the employer should provide to the employee.[7] Advance notice to employees that emails and internet use must be limited to business purposes goes in favor of employer intrusiveness. Advance notice to employees that the internet use and/or emails may be monitored and reviewed and lead to disciplinary action also negatively affects an employee's right to contest the employer

---

[5] See generally, Joseph G. Schmitt, Escaping the Privacy Bind: An Outline for Employers, Andrews Sex. Harassment Litig Rptr 12 (2001).
[6] N.J.S.A. 2A:156A-1, *et seq*.
[7] *See, e.g.* Hennessey v. Coastal Eagle Point Oil, 129 N.J. 81 (1992)

accessing such information. These notices were construed by the court as affecting the employees' legitimate expectations of privacy.

In Pennsylvania, an employee claimed that he was told that his emails were confidential and privileged. He further claimed that he did not know the employer was reviewing his emails. Nonetheless, the Court ruled that the employer could terminate the individual for transmitting inappropriate and unprofessional comments over the employer's internal email system.[8]

b. Searching an Employee's Property

Employers may also have a need to search employees' possessions, in order to determine whether company property has been appropriated. Most states provide a cause of action for intrusion upon seclusion under which an employee may sue for such searches if done unlawfully.[9] Determining the lawfulness of such a search is usually made with reference to a reasonableness standard which considers whether the search comports with the employer's usual practice or stated policy, or, whether it unreasonably exceeds the employee's expectations in that regard, and, a balancing of the employee's privacy interests against the risk which the employer seeks to prevent. Since the determination of whether a particular search violates an employee's privacy rights is highly factual, employers should always be careful to conduct any searches with uniform practices, not search more than is reasonably necessary to prevent the potential harm which gave rise to the search, and, inform its employees in writing of its policies on searching employee's property ahead of time, preferably at the commencement of

[8] Smyth v. Pillsbury Company, 914 F. Supp. 97, 98 (E.P.D. PA. 1996).

[9] Intrusion upon seclusion requires showing (a) an unauthorized intrusion or prying into plaintiff's seclusion, (b) the intrusion would be offensive or objectionable (c) the matter upon which the intrusion occurred was private and it (d) caused mental anguish or suffering. Restatement Second of Torts § 652B (1977).

employment. Employers may also make clear that staff who violate these policies will be disciplined, up to and including termination. At all times, employers should also be vigilant to ensure that their polices regarding searches do not target or tend to single out any protected group or individual person such that it may later be held to be discriminatory or retaliatory.

In the private employer context, The New Jersey Supreme Court has refused to apply constitutional search and seizure protections in the arena of conduct that is not sanctioned by the government.[10] In the public employer context, the United States Supreme Court has ruled that employer searches of employee office space to retrieve government property or investigate work related misconduct is justified, "where there are reasonable grounds for suspecting that a search will turn up evidence that the employee is guilty of work related misconduct."[11] The courts have ruled that this standard is lower than the protections offered by the probable cause standard in the criminal context which does not apply in the employment context. Under the Ortega analysis, the work place that is subject to search includes areas that are related to work and within the employer's control such as file cabinets, offices, desks, cafeterias, and hallways. Ortega*, supra,* 480 U.S. at 715-716. The scope of permissible employer search exists despite the fact that employees may have personal items in the specific area. Ortega*, supra* 480 U.S. at 716. However, closed luggage, handbags or locked briefcases may be outside of the scope of a permissible search, even though the employee may bring the item to work with them

[10] State v. Robinson, 86 N.J. Super. 308 (Law Div. 1965) and State v. Pohle, 1166 N.J. Super. 504 (App. Div.), *cert. den'd,* 81 N.J. 328 (1979).
[11] O'Connor v. Ortega, 480 U.S. 709 (1987). *Contra* State v. Ferrari*,* 136 N.J. Super. 61 (Law Div. 1975*)* (Government employer's search of employee's office and desk violated the Fourth Amendment; no New Jersey constitutional claim presented.); Gossmeyer v. McDonald, 128 F.3d 481, 490 (7th Cir. 1997); and Wasson v. Sonoma County Junior College District, 4 F. Supp. 2d 893, 905 (N.D. Ca. 1997).

everyday and leaves the item in the office. The propriety of the search surrounds the issue of the employee's legitimate expectation of the privacy in the workplace. This expectation is affected by actual office practices, procedures, legitimate regulations, or advance notices that certain areas are subject to search. The employee's interest is balanced against the public interest and the need for supervision, control, and the efficient operation of the workplace.[12]

[12] *See* Wasson v. Sonoma County Junior College District, 4 F. Supp. 2d 893, 905 (N.D. Ca. 1997).

EXHIBIT A
COMPUTER AND VOICE MAIL USE POLICY

GENERAL PROVISIONS

The Company maintains this policy for the purpose of controlling and ensuring the legal, appropriate and productive use of its computer and voice mail systems.

Each employee is responsible for the use of ABC Company's computer and voice mail systems, including, but not limited to, its e-mail and Internet system, in accordance with this policy. ABC Company reserves the right to modify this policy at any time, with or without prior notice.

The use by employees of the Company's computer and voice mail systems constitutes their consent to all the terms and conditions of this policy.

COMPANY'S PROPERTY

ABC Company's computer and voice mail systems are the Company's property and are provided for your use in carrying out Company business. The use of these systems for incidental and occasional personal purposes is prohibited.

All communications and information transmitted by, received from and created or stored in its systems (either through word processing programs, e-mail, the Internet, voice mail or any other way) are the Company's Records and the Company's Property.

NO EXPECTATION OF PRIVACY

The Company supplies computers, computer accounts, Internet accounts and voice mail to its employees to assist them in performing their job duties. *Employees should not have any privacy expectations on anything they create, store, send or receive in the Company systems. Employees must also be aware that the deletion of any e-mail message or file will not actually delete them from the system. All e-mail messages are stored in a central back-up system.*

The use of passwords or other security measures does not reduce in any way the right of the Company to control and access the materials in its systems, nor does it create any privacy right for the employees in the data contained in the computer systems and files.

Any password used by an employee must be disclosed to the Company upon request when the Company needs to access the files in the employee's absence, or for any other reason that the Company, in its discretion, considers appropriate.

The Company has the right to control any and all of the aspects of its computer systems, and the Company may exercise its right to control, access, retrieve and delete any material stored, created, received or sent through its computers or voice mail systems for any reason, without prior authorization or notice to any employee.

Confidentiality of E-mail and Voice mail Communications

Employees are not authorized to retrieve, read or listen to any e-mail or voice mail message that has not been sent to them.

Even though the Company has the right to retrieve, read, listen to and delete any information created, sent, received or stored in its systems, e-mail and voice mail messages must continue to be treated as confidential by the other employees, and accessed only by the recipient.

In order to prevent the disclosure of the content of a message to unauthorized persons, employees should avoid listening to voice mail messages and engaging in confidential phone conversations while they use the speaker function of the phone.

OFFENSIVE AND ILLEGAL MATERIAL

ABC Company's policies on equal opportunity employment, harassment, and retaliation are applied in their entirety to the Company's computer and voice mail systems, and any violation of these policies is grounds for disciplinary sanctions, up to and including termination.

Consequently, no e-mail or voice mail messages should be sent or received if they contain intimidating or offensive material, including, but not limited to, material discriminating on the basis of race, color, religion, sex, age, national origin, ethnicity, disability, marital status, war veteran status, political affiliation, sexual orientation, and any other category protected by law.

Likewise, any material that is fraudulent, harassing, embarrassing, sexually explicit, profane, obscene, intimidating, defamatory, illegal, inappropriate, offensive, copyright protected or subject to trademark protection may not be downloaded from the Internet, nor visualized or stored in the Company's computers.

Employees that find or receive these type of materials from other employees are responsible for informing the sender that they do not wish to receive said material, and informing their supervisor or the Human Resources manager of the incident.