WORKPLACE PRIVACY ISSUES:

POTENTIAL PITFALLS FOR UNWARY EMPLOYERS

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 paper focuses on three areas of concern to employers, and in which they must be most careful to guard against violating their employees' privacy rights: (1) email/computer monitoring and searches of an employee's property (2) reference and background checks, and (3) disclosure of an employee's health information and health testing. 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.

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

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.

---

[1] Spying on Employees: What You Can and Can't Do, HR Hero, June 2003.

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, 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 ("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

[2] 29 U.S.C. §§ 157-158.
[3] 18 U.S.C. § 2510 et. seq.
[4] 18 U.S.C. § 2511(2)(d).

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 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.

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.[6] 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

---

[5] See generally, Joseph G. Schmitt, Escaping the Privacy Bind: An Outline for Employers, Andrews Sex. Harassment Litig Rptr 12 (2001).

[6] 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).

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 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.

II. Reference and Background Checks

While employers have a legitimate need to ensure they hire the best possible candidates, reference and background checking methods which impermissibly disclose protected information or private facts can expose employers to civil litigation.[7] The degree and type of checking permissible will vary from position to position, but the same degree of checking for all applicants for the same position should be done to avoid actual or apparent discrimination, especially since background investigation processes which have the effect of denying employment to individuals in protected classes may be found to be discriminatory. For example, credit checks are usually considered unnecessary for employees who will not be handling money or other financial assets. Similarly, checking

[7] Most states have a cause of action for "public disclosure of private facts" or "false light." Improper reference and background checking may trigger liability under these causes of action.

on a qualification which is unrelated to the job position, but which the applicant has disclosed on their resume, will not always be considered to be necessary or reasonable and may be considered discriminatory.

Criminal back ground checks raise specific concerns since employers have to be aware of past criminal behavior in order to prevent violence in the work place for which they may be liable under a theory of negligent hiring. However, criminal background checks should only seek information about convictions and not arrests, and employers should assess and balance the job duties and scope of responsibility against the seriousness of the criminal behavior.

In addition, employers should take care to guard the information obtained by them while performing these checks. A clear privacy policy should advise the employee that the company will limit collection of employee information to that needed for business and legal purposes, protect the confidentiality of all personal information in employee records, and limit access to private records to staff members who have an authorized business need to know or to parties who have obtained a court order or subpoena for specified employee records.

Generally employers should take the following steps to ensure that they obtain relevant information, while minimizing the risk of violating an employee's privacy interests:

1. Have the employee fill out an application form which must be signed and attested to for accuracy. Do not allow employees to simply state "see resume." Include an acknowledgment that any falsification, material omission or misrepresentation may result

in failure to receive an offer of employment, or, if hired, may result in a dismissal from employment.

2. Determine what checks are necessary considering the responsibilities of the position, and do not automatically use the same checks for every position. Perform the same checks for everyone applying for the same position however, in order to prevent a finding that the checks were discriminatory or retaliatory.

3. Tell the employee ahead of time, in writing, which types of reference and background checks will be conducted in order to determine that they are qualified for the job and obtain written consent from the employee or applicant to perform all such checks.

4. If credit, motor vehicle and/or criminal checks are required for the position, ensure that the procedures outlined in the Fair Credit Reporting Act are followed, and the appropriate notices given. Also ensure that if an adverse action is taken based on information contained in a credit, motor vehicle and/or criminal report, the employee is notified and advised of his or her rights in accordance with the Act.

5. Document all attempts to check references and the information obtained.

6. Attempt to reach the employee's former supervisor rather than simply speak with the Human Resources department.

7. Do not seek protected information while checking references. You cannot seek information from a third party about which you could not ask the candidate directly.

8. Keep personnel files in the Human Resources department or under lock and key. Ensure that they are not left in a public place where anyone may have access to them. Make sure that computerized versions of these documents are password protected.

9. Do not disclose information in personnel files to everyone, even another management employee, unless that person has a business reason to know information contained in the files.

10. Uniformly and consistently discipline employees who violate procedures aimed at protecting employees' privacy rights.

Similarly, while giving references concerning current or former employees, employers should authorize only the Human Resource departments to give such references, and verify only factual data, unless a written authorization to do otherwise is received from the employee. A sample reference check policy is attached as **Exhibit B.**

III. Disclosure of Health Information and Employee Health Testing

Another area which raises significant privacy concerns is the disclosure of health information and health or drug and alcohol testing of employees. Because health information is information which most employees and the general public consider to be highly worthy of protection, and health testing is perhaps the most invasive area of employer inquiry, employers face significant penalties and risk substantial jury verdicts if they do not ensure that both their disclosure of health information, and their attempt to obtain such information, is done lawfully.

a. Disclosure of Health Information

The Health Insurance Portability and Accountability Act ("HIPAA") is intended to standardize health information coding and transmission and regulate individual health information privacy. It applies to all private sector health plans (including managed care organizations and Employee Retirement Security Act plans, but excluding certain small

self-administered health plans with fewer than 50 participants).[8] As a result of its application to health plans, most employers will have some HIPAA obligations, which will be dependent on how much health information an employer receives about employees while providing employee health benefits through health plans.

HIPAA has an expansive definition of "protected health information." It applies to oral or recorded information that is created or received by a health care provider or plan, and that relates to the past, present or future health or condition of an individual, the provision of health treatment to an individual, or payments for health treatments.[9] Thus even enrollment forms, claim forms and bills for medical treatment include protected health information.

Moreover, HIPAA imposes severe civil and criminal penalties for noncompliance, including fines up to $25,000 for multiple violations of the same standard in a calendar year and fines up to $250,000 and/or imprisonment for intentional violations.[10]

The following principles must be kept in mind in an attempt to become HIPAA compliant:

1. Individually identifiable health information should be used only for the individual's health care treatment and payment or for health plan operations.[11]

2. If health information is used for payment and plan operations, only minimally necessary information should be released.

---

[8] What Employers Need To Do Now to Comply with HIPAA's Privacy Rule, Employment/Labor Law Feature, ACCA Docket, March 2002.

[9] 42 U.S.C. § 1320d.

[10] Bert Lazar, Most Employers Need To Comply With HIPAA Health Care Privacy Regulations, 19 No. 1 e-commerce L. & Strategy 5 (2002).

[11] Most of these recommendations are contained in Hungry Hungry HIPAA-are you ready for the Beast?, Arkansas Employment Law Letter, HR Hero, June 2003.

3. Health information should not be used for hiring, firing or other personnel decisions.

4. Entities covered by HIPAA should preserve the security of health data by adopting written policies to protect the data and to track disclosures, train employees in privacy protection requirements, and provide disciplinary measures against employees who violate the policies.

5. Maintain documentation of all uses and disclosures of health information.

6. To the extent possible, erect a "firewall" between the people receiving or using such information and the other employees, and limit access to computerized health data, in order to reduce the possibility of unauthorized disclosures.

7. Designate a privacy official who will be responsible for implementing these procedures and ensuring HIPAA compliance.

8. Amend plan documents to account for the use of participant health information.

9. Revise third party agreements to require specific limitations on the use of participant health information and compliance with privacy procedures.

b. Health Testing

While employers may have legitimate reasons to perform health tests, such tests are likely to be the most invasive of all employment procedures, and most likely to give rise to privacy claims. As a result, employers need to be extremely vigilant to ensure that all such testing is necessary, and then, that it is properly carried out.

As a general matter, applicants should be offered a position first before being required to undergo medical testing, and the employer should pay for any such testing. Drug and alcohol testing may be performed if an offer is made, and an applicant may be

excluded from employment if tests reveal the current use of drugs or alcohol. An applicant may not be excluded based on a past history of drug or alcohol use however.[12] Once the person is hired as an actual employee, testing is allowed for business necessity, or in order to comply with other laws and regulations, for example Department of Transportation regulations governing truck drivers. A sample Drug and Alcohol Policy is attached as **Exhibit C**.

Regardless of the type of tests, the following principles should be kept in mind:

1. There must be a specific business-related reason for a test and the test must measure something specific and objective.

2. The use of any test results must be clearly identified, and the results of each test must be applied uniformly in hiring, firing or promotion decisions.

3. Do not give tests if the results will not be considered.

4. Keep all test results confidential, especially medical, psychological, and drug and alcohol testing, but make the results of the test available to the employee.

5. Make sure tests are performed by a licensed professional and are not more invasive than necessary to obtain valid test results.

---

[12] See, EEOC Enforcement Guidance on Disability Related Inquiries and Medical Information, July 2000. If you are a federal contractor, you must comply with the Drug Free Workplace Act of 1988. 41 U,S.C. § 701 et. seq. See also, Testing and Employee Privacy, 6 Andrews Employment Litig. Rptr 16 (2001).

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.

EXHIBIT B

POLICY GOVERNING GIVING OF REFERENCES RELATING TO CURRENT OR FORMER EMPLOYEES

POLICY

None of ABC Company's employees (except for those in the Human Resources department) can deliver a letter of reference or provide a statement of references by phone on behalf of any current or former employee.

Breach of this policy may be grounds for disciplinary measures, up to and including termination.

PROCESS FOR PROVIDING REFERENCES

All requests, in writing or by phone, related to ABC Company's current or former employees, shall be directed to Human Resources at *[insert address and phone number]*

Human Resources shall only verify the name of the employee, the date of employment, the position, department, and shall confirm salary information.

No other data or information shall be provided, unless the employee submits a written request to the Company or ABC Company is mandated by law to provide such additional information.

In the event that the employee submits a written request for a reference which seeks additional information than that outlined above, the letter must include an authorization to provide the specific information requested, and a statement that renders ABC Company harmless in the event of any liability related to the release of the specified information.

EXHIBIT C

DRUG AND ALCOHOL ABUSE POLICY

POLICY

ABC Company abides by all federal, state and local laws on drug and alcohol abuse.

For the purpose of complying with its policy against drug and alcohol abuse, except in instances prohibited by law, ABC Company approves and complies with the following practices:

- All applicants are subject to drug tests prior to being hired.

- Employees that violate ABC Company's policy and procedures against drug and alcohol abuse shall be subject to the application of disciplinary measures, up to and including termination.

- All employees are subject to random drug and alcohol tests to the extent permissible by law.

- It shall be understood that employees that use, lave possession of, are under the influence of, or are involved in the sale or purchase of, any substance covered by state or federal legislation on controlled substances, while they are on ABC Company's premises, doing business for ABC Company or operating ABC Company's equipment (including lunch breaks and rest breaks) are committing a violation of the Company's Policy on Drug and Alcohol Abuse and shall be subject to the application of disciplinary measures, up to and including termination.

- ABC Company does not have the obligation to provide rehabilitation services to any group of employees. However, to the extent possible, employees shall be informed of said services when they are available.

- ABC Company reserves the right to conduct searches in any place and without prior notice with relation to controlled substances or alcohol (which include personal items or employees' vehicles) on the Company's premises. ABC Company's employees must not consider their desks, lockers and personal items (such as briefcases and bags) as private items while they are on the Company's premises.

- ABC Company shall provide its full cooperation to federal, state and local authorities in matters related to the use, possession, sale or purchase of controlled substances by any person that it employs.

- ABC Company reserves the right to amend at any time its Drug and Alcohol Abuse Policy and ABC Company fully intends to abide by the terms of any

applicable laws regarding the maintenance of a Drug free workplace, including, to the extent applicable, the Drug-free Workplace Act of 1988.

PROHIBITED CONDUCT

The employees covered by ABC Company's Drug and Alcohol Abuse Policy shall not:

- use controlled substances without the authorization of a physician
- report to work or carry out functions that are critical to security while they have alcohol concentration level of 0.02 or above in their exhaled breath
- ingest alcohol or medications that can adversely affect their activity or common sense while they carry out work related functions
- work or operate a commercial automotive vehicle, or mass transportation vehicle, if they are in possession of alcoholic beverages, unless the latter are declared and transported as part of the dispatch
- carry out functions that are critical to security during the 4 hours following the ingestion of alcohol
- use or be in possession of alcoholic beverages while they are on the Company's premises, unless such use or possession is related to a social event sponsored by ABC Company and at which alcoholic beverages are served by ABC Company
- ingest alcohol during the eight hours following an accident, unless the employee has been subject to an alcohol detection test after the accident, or
- refuse to subject to a required drug or alcohol test.

TESTS

ABC Company fully cooperates with local, state and federal authorities with regard to laws and regulations on Drug and Alcohol Abuse.

In accordance with these regulations, ABC Company shall carry out, when necessary and in the cases allowed by law, specific tests on employees to determine current drug or alcohol use.

DISCIPLINARY MEASURES

Employees that violate or refuse to cooperate with the implementation of ABC Company's Policy against Drug and Alcohol Abuse shall be terminated immediately.

In accordance with the provisions of the Law on a Drug-free Workplace of 1988, disciplinary measures shall be taken against employees that have been prosecuted for a violation of criminal laws against drug use, which occurs on the Company's premises.

ADULTERATION OR REPLACEMENT OF TEST SPECIMENS

Adulteration is the alteration of or tampering with samples taken in drug detection tests.

Replacement consists in sending a sample obtained from another individual or a sample that does not show signs or clinical features associated with normal human fluids being tested in the place of a sample from an employee who is being tested.

In the event that it is determined that an employee's test sample has been adulterated or replaced in any form, these acts shall be considered a refusal to subject to a test and the employee shall be immediately terminated. Applicants that adulterate or replace their urine samples shall not be hired.

Any positive test result shall be reviewed by a licensed physician or other certified professional with knowledge and experience to interpret and evaluate such results.