

## **EMPLOYMENT LAW**

---

The Internet affects the relationships between employers and employees. E-mail communication has become commonplace as a fast and easy method of communication between employees, clients, and the public. This section covers the issues that businesses should be aware of with respect to employee use of the Internet. Guidelines are provided to protect a business from liability stemming from employee use of the Internet and e-mail.

### **DEFINITION OF AN EMPLOYEE**

To determine how the law of the Internet applies to employees, one must first determine whether an individual is an employee. There is not always an obvious answer to this question, and the issues can become complicated.

Basically, employees are a kind of agent. All employees are agents, but not all agents are employees. There are two essential characteristics that distinguish employees from agents. First, an employee must be a human being as compared to artificial or electronic agent. Second, an employer has more control over an employee than over an agent. An agent typically has its own facilities and is independent. Also, an agent's services usually are in the nature of a single transaction, and not part of a continuing relationship.

Employees are distinct from independent contractors. An independent contractor is not an employee, and therefore an employer's liability for independent contractors is much more limited than that for employees. A worker is not an independent contractor simply because they are called an independent contractor. An improper classification can be costly. The key in determining whether a worker is an independent contractor or an

employee is the degree of control a company exercises (or has a right to exercise) over the worker's performance of the work. The more control exercised, the more likely the worker will be considered an employee. The less control exercised, the more likely the worker is an independent contractor. The IRS Web site provides a helpful overview of how to determine whether a worker is an employee or independent contractor. See <http://www.irs.gov/plain/forms-pubs/pubs/p15204.html>.

## EMPLOYER LIABILITY

The ease at which e-mail is transmitted encourages informality and often reduces inhibitions. E-mail allows for the rapid dissemination of ideas, plans, and documents. Employees are frequently allowed unlimited access to e-mail and the Internet. This exposes the employer to many risks.

Employers can be subject to liability to third parties from actions of their employees. Such liability can arise from action of the employees done within the scope of their employment. An employer can be liable for sexual or racial harassment perpetrated or furthered by e-mail. Also, careless and defamatory e-mail may expose individuals and the company to litigation. Other problems for employers could arise where employees breach copyright laws by downloading information contained on other web sites. There are also risks that employees may disclose confidential company secrets to competitors or third parties.

The extent to which an employer is liable for employee conduct varies. Under the general concept of *respondeat superior*, an employer is liable for the damaged party's injuries if the employee's injurious actions occurred within the scope of the employee's employment. The scope-of-employment analysis does not lend itself to any simple definition, but courts traditionally apply the following factors:

- the time, place, and occasion of the act;
- the relationship between employer and employee;

- if the act is commonly done by employees;
- if the act departed from normal scope of work; and
- if the act was reasonably anticipated by the employer.

An employer cannot assume that it will escape liability merely because it does not know such action is occurring. A company will be liable if management-level employees knew, or in the exercise of reasonable care should have known about offensive conduct. See *Faragher v. City of Boca Raton*, 524 U.S. 775, (1998). Prompt action to remedy a hostile atmosphere may relieve the employer of liability, but there is no guarantee.

## **PRIVACY OF EMPLOYEE E-MAIL**

One method of reducing an employer's liability is to monitor or at least have the right to monitor employee e-mail. There are limitations to the extent an employer may monitor e-mail. Statutes have carved out exceptions to allow a company to monitor employee activity where there is a legitimate business purpose.

The Federal Electronic Communications Privacy Act of 1986 ("ECPA") 18 U.S.C. §§ 2510-2521, 2701-2709, 2711 generally prohibits the interception of electronic communications, including e-mail. However, three major exceptions to the ECPA may allow the interception of employee e-mail. First, an employer can monitor employee e-mail where the employee has consented to monitoring. This consent can either be express, where the employee actually agrees to the monitoring, or implied, where the employee continues to use the employer's e-mail system after being expressly informed that the employer intends to monitor e-mail. (See Privacy section in Commercial Transactions for discussion of ECPA and related federal privacy laws.)

The ECPA also allows the provider of electronic communication services to monitor communications when the monitoring is a necessary incident of the rendition of services or of the protection of the rights or property of the provider. This exception allows an

employer to monitor e-mail transmitted via an employer-provided system. Note that this exception would not apply to situations in which the employer simply provides the employee access to a commercial e-mail service.

Finally, the ECPA provides that the interception of electronic communication is lawful if it is for a legitimate business purpose. Courts have taken two separate approaches to this exception. Under the first approach, an employer may monitor e-mail where the employee has been informed of the monitoring and it is necessary to protect the employer's business interests. The second approach examines the content of the intercepted communication. Under this approach an employer may intercept business related e-mails but not personal e-mails. An e-mail message is considered business related e-mail if it is a message in which the employer has a legal interest or the interception is necessary to guard against the unauthorized use of the e-mail equipment.

A company will have a legal interest in an e-mail message when the message is either in pursuit of the employer's business or is a detriment to the employer's business. An employer that wishes to leave open the opportunity of monitoring employee e-mail messages would be well advised to inform its employees that it reserves the right to monitor e-mail messages. By informing employees, the employer will be in a stronger position to argue that its employees do not have a "reasonable expectation" of privacy in their e-mail messages and will thus avoid having to rely on the court's own notion of what privacy expectation is reasonable.

Courts dealing with these issues generally protect the company's interest when it is legitimate. Most courts have found that the interests of the company outweigh an employee's expectation of a right to privacy. It appears that an employer who wants to monitor employee e-mail can readily do so once that e-mail has been stored.

## **E-MAIL AND INTERNET USAGE POLICY**

The best solution to limiting an employer's liability is to establish an official e-mail usage policy. This policy should be carefully

conceived and disseminated to all employees. A physical copy should be given to employees and posted with other official legal notices to employees. Also, employees should acknowledge agreement with that policy.

The content of a company's e-mail and Internet policy depends on the type of business. Businesses with confidential information and trade secrets may want to have a stricter policy. The policy should be included in the employer's disciplinary code. The following is a list of issues that the policy should address:

- state that all e-mail correspondence is the property of the employer and employee e-mail is not considered private;
- state whether the company system can be used for reasonable private use or whether it is solely for business use. If connected to the Internet, state that it can only be used for business-related purposes;
- state that the employer reserves the right to monitor its e-mail system at its discretion in the ordinary course of business;
- state that the system must not be used to communicate highly sensitive, offensive, defamatory, or derogatory messages, which include, but is not limited to, messages that are inconsistent with the employer's policies concerning sexual harassment, equal employment opportunity, etc.; and
- state that all downloaded files from the Internet must be checked for possible computer viruses.

All personnel should use care when addressing e-mail messages to avoid inadvertent messages from being sent to the wrong address. This is especially crucial of confidential information. Development of a business/client address book listing all clients may reduce the tendency to inadvertently misspell an address. Businesses should also be cautioned not to use the "reply to all" function without first checking where the message could be sent. Proofreading an e-mail for accuracy and for the correct address

will also reduce the risk of sending out private, confidential or inappropriate information. A sample Internet Usage Policy can be found at the United States Patent and Trademark Office website at <http://www.uspto.gov/web/offices/com/sol/notices/fr990621.htm>. Though this guide may be used as a reference, businesses should tailor a usage policy to their company.

## **STORAGE OF E-MAIL**

All businesses should establish a policy for the storage of e-mail. E-mail does not disappear once it has been deleted. E-mail messages are typically stored in the company's backup system. Many casual yet potentially destructive messages sent over company networks and the Internet are stored in backup systems. If involved in litigation, discovery of computer data is available which includes the recovery of deleted e-mail messages and other information transmitted via the Internet or stored on a computer.

A company should establish procedures to control the distribution and deletion of e-mail. This will protect an organization from unexpected or inadvertent results in litigation. The following procedures should be considered:

- backup copies of e-mail should be physically separated from backups of the rest of the computer system. This allows e-mails to be deleted after a short period of time;
- any e-mail which the sender wants to retain should either be printed in hard copy format or else stored in the main backup system of the computer; and
- employees should be advised that e-mail will be deleted within a certain number of days.

## **EMPLOYMENT CONTRACTS AND NONCOMPETITION AGREEMENTS**

A written employment contract should be used to specify the rights and duties of both the employer and employee. Contracts clearly define all the terms and conditions of employment and

prevent future disputes. Employment contracts should be prepared with an understanding of how the law and Internet technology will affect the employer/employee relationship.

Many employers use written employment agreements with noncompetition covenants to protect trade secrets. Minnesota's noncompetition agreements are governed by case law, and, in this regard, Courts carefully look at the enforceability of such agreements in light of possible restraint of trade. Generally, for such agreements to be enforceable, there must also be adequate consideration. While non competition agreements are common, such arrangements are more prevalent among high-technology companies. It is essential for a company to include legally enforceable confidentiality obligations and to consider assignment and work-made-for-hire language concerning patents, copyrights and trade secrets. Minnesota also has a statutory requirement that employees be given notice of their rights to inventions created outside the scope of their employment without using any resources of their employer. See Minn. Stat. § 181.78, which provides as follows:

“Any provision in an employment agreement which provides that an employee shall assign or offer to assign any of the employee's rights in an invention to the employer shall not apply to an invention for which no equipment, supplies, facility or trade secret information of the employer was used and which was developed entirely on the employee's own time, and (1) which does not relate (a) directly to the business of the employer or (b) to the employer's actual or demonstrably anticipated research or development, or (2) which does not result from any work performed by the employee for the employer. Any provision that purports to apply to such an invention is to that extent against the public policy of this state and is to that extent void and unenforceable.

No employer shall require a provision made void and unenforceable by subdivision 1 as a condition of employment or continuing employment.

If an employment agreement entered into after August 1, 1977 contains a provision requiring the employee to assign or offer to assign any of the employee's rights in an invention to an employer, the employer must also, at the time the agreement is made, provide a written notification to the employee that the agreement does not apply to an invention for which no equipment, supplies, facility or trade secret information of the employer was used and which was developed entirely on the employee's own time, and (1) which does not relate (a) directly to the business of the employer or (b) to the employer's actual or demonstrably anticipated research or development, or (2) which does not result from any work performed by the employee for the employer".

### **Employee Laptops**

On March 8, 2006, the United States Court of Appeals (7th Circuit) determined that a person who is provided a laptop by a company and who uses a trace removal software tool to erase data, may be liable under the Computer Fraud and Abuse Act [18 U.S.C. § 1030] even without an employment agreement or corporate policy prohibiting the use of such programs. See International Airport Centers LLC et al v. Jacob Citrin.