MANAGING THE ELECTRONIC WORKPLACE

by

Scott Warrick, JD, MLHR, CEQC, SHRM-SCP

Scott Warrick Human Resource Consulting, Coaching & Training Services
Scott Warrick Employment Law Services
(614) 738-8317 ♣ scott@scottwarrick.com ♣ WWW.SCOTTWARRICK.COM

Follow Scott's *HR CONSULTING & EMPLOYMENT LAW SERVICES* on FACEBOOK and LinkedIn

Table of Contents

MANAGING THE ELECTRONIC WORKPLACE

by

Scott Warrick, JD, MLHR, CEQC, SHRM-SCP

Scott Warrick Human Resource Consulting, Coaching & Training Services
Scott Warrick Employment Law Services
(614) 738-8317 ♣ scott@scottwarrick.com ♣ WWW.SCOTTWARRICK.COM

Follow Scott's *HR CONSULTING & EMPLOYMENT LAW SERVICES* on FACEBOOK and LinkedIn

I. THE FEDERAL WIRETAP ACT OF 1968: INTERCEPTING OR DISCLOSING EMPLOYEE COMMUNICATIONS (18 U.S.C. § 2510, et seq.)

A. Coverage

Title III of the Omnibus Crime Control and Safe Streets Act of 1968, or The Federal Wiretap Act ("FWTA") (18 U.S.C. § 2510 et seq.), as amended by Title I of the Electronic Communications Privacy Act ("ECPA") of 1986 (18 U.S.C. § 2701 et seq.) prohibits any person from:

1. Intercepting or recording any wire, oral or electronic communications through the use of any electronic, mechanical or other type of device as well as

2. Disclosing any information obtained in violation of the FWTA.

The FWTA does not apply when:

1. **The person intercepting the transmission is also a party to the communication,**

2. **When anyone who is a party to the communication has given their permission to have the transmission intercepted or has been placed on notice that this interception will take place or**

3. **The interception was done with a legitimate business reason.**

(Employers should also realize that every state also has laws that govern employee privacy rights in some way. Therefore, even if employers are in compliance with the FWTA and the ECPA, they should always check the laws of the state where they do business.)

B. Exceptions To The FWTA

1. Ordinary Course Of Business or Legitimate Business Reason Exception

The FWTA specifically prohibits **any person** from intercepting another individual's wire, oral or electronic communication through the use of an "electronic, mechanical, or other device." However, the FWTA does permit employers to intercept their employees' communications when such an interception is done in the **ordinary course of the employer's business** by means of equipment supplied to it by a provider of wire or electronic communications that is also used in the ordinary course of the employer's business.

The courts have therefore permitted employers to intercept their employees' communications at work whenever the employer has a "legitimate business interest" in the communication and this interception occurs in the ordinary course of the employer's business under the FWTA.

For instance, in Briggs v. American Air Filter, 630 F.2d 414 (5th Cir. 1980), the manager of American Air Filter's Atlanta office, William McClure, heard that Dan Roby, one of his employees, was supplying Phillip Briggs, one of American Air Filter's competitors, with confidential information. McClure then informed Roby that American Air Filter employees were prohibited from disclosing confidential information to its competitors.

Later, as Roby secluded himself in a private office at American Air Filter during working hours, McClure learned from a secretary that Roby may be on the phone supplying Briggs with confidential information. McClure then went to an extension phone and recorded part of Roby and Briggs' conversation. Neither Roby nor Briggs were aware of the fact that McClure was listening in or recording their conversation.

Roby and Briggs contended that McClure, and therefore American Air Filter, violated their rights under the FWTA by intercepting and recording their conversation. However, the Fifth Circuit held that McClure did not violate the FWTA by intercepting and recording Roby and Briggs' telephone conversation. The court reasoned that this conversation between Roby and Briggs was related to American Air Filter's business and was not of a personal nature. This fact was undisputed by either party.

Further, McClure had a very good basis for believing that Roby's conversation was related to American Air Filter's business since McClure knew Roby had been supplying confidential information to a competitor.

The court therefore held that since American Air Filter intercepted and recorded this conversation in the ordinary course of its business and that it had a legitimate business reason for doing so, which was to protect its confidential information from being distributed, it had not violated the FWTA. As a result, even though American Air Filter had not put either Briggs or Roby on notice that their conversation was subject to interception, no violation of the FWTA occurred.

2. Ordinary Course Of Business or Legitimate Business Reason Exception: Notice May Be Required Anyway

In Adams v. City of Battle Creek, a municipal corporation, and Kruithoff, an individual, No. 99-1543 (6th Cir. 2001), David Adams, an officer with the Battle Creek Police Department, was suspected of dealing illegal drugs. In order to investigate, a police supervisor tapped into Adams' pager, which was supplied by the Police Department, to see if he was in fact assisting drug dealers. As it turned out, Adams was not dealing in drugs, but he was also not placed on notice that these messages might be monitored. Adams sued both the City of Battle Creek and Jeffrey Kruithoff … personally.

Battle Creek and Kruithoff argued that under the Federal Wiretap Act, they were permitted to read the messages on Adams' pager without giving him any notice since the pager belonged to the City. As a result, reading the messages fell under the "ordinary course of business" exception to the law.

The 6th Circuit disagreed and found for Adams. The court reasoned that even under the "ordinary course of business" exception, notice must be provided before any monitoring any such communications.

Therefore, it is always best to place employees on notice before conducting any type of electronic surveillance in the workplace.

3. Ordinary Course Of Business Exception: FRAUD

In Konop v. Hawaiian Airlines, No. 99-55106 (9th Cir. 2001), Robert Konop, an employee of Hawaiian Airlines, set up his personal website for chatting with non-management co-workers. Konop issued passwords to those fellow employees who were given access to the website. However, in return for receiving a password to the site, members were required to promise not to give the password to anyone in management. Hawaiian Airlines convinced an employee to let it use his assigned password so the company could monitor the communications of its employees.

When Hawaiian Airlines then terminated Konop for the derogatory remarks made on his website. Konop sued the company under the Federal

Wiretap Act and the Stored Communications Act for illegally monitoring his communications.

The Ninth Circuit agreed with Konop and found the company's activities to be based on fraud and therefore illegal under the Federal Wiretap Act and the Stored Communications Act.

4. Ordinary Course Of Business Exception: Personal Phone Calls

Employers may intercept the communications of their employees, which most often involves the use of a telephone, when doing so is in the "ordinary course of business," as previously discussed. However, the ordinary course of business exception does not permit employers to monitor the personal conversations of their employees. Instead, employers are permitted to monitor the communication long enough to only determine the nature of the message but not its contents. (Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983)).

In other words, employers are permitted to monitor their employees' communications only long enough to determine if they are of a personal or business nature. Once the employer is able to reasonably determine that the employee's communication is personal, the employer must cease its monitoring immediately.

For instance, in Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992), Newell and Juanita Spears owned and operated a small store that adjoined their mobile home. The Spears had a telephone in their store that also had an extension line that ran into their residence.

When the Spears' store was burglarized one night, the Spears suspected that Sibbie Deal, one of their employees, was involved. In order to obtain evidence that might incriminate Deal, Newell Spears connected a recording device to the extension line that ran into their mobile. The recorder was installed in such a way that whenever anyone used the phone in the store, it would record the conversation automatically.

By recording and listening to Deals' telephone conversations, those that were both personal and business-related, it became clear that Deal was not involved in the burglary. However, the Spears did discover that Deal had been selling goods to her friends at cost. The Spears therefore fired Deal.

Further, the Spears also overheard Deals' "sexually provocative" conversations with Calvin Lucas concerning an extramarital affair they were having together and Deals' "partner-swapping" activities. Juanita Spears then repeated this information to others.

Both Deal and Lucas sued the Spears for violating their rights under the FWTA. In reaching its decision, the court reasoned that while Newell

Spears was well within his rights under the FWTA to intercept and record all of Deals' conversations that were business-related, the court also held that it was unlawful for him to intercept and record Deals' personal conversations, since such communications do not fall within the "ordinary course of an employer's business" exception.

Instead of recording every conversation made by Deal, Spears should have monitored her conversations only long enough to determine if they were of a business or personal nature. If the conversation was found to be personal, the monitoring must end. If it was found to be business-related, then the monitoring may continue.

Although the court found Newell Spears liable to Deal and Lucas under the FWTA for intercepting and recording their personal conversations, it also found Juanita Spears liable to both Deal and Lucas for repeating to others the personal information she heard on these tapes. Both Newell and Juanita Spears were therefore liable to both Deal and Lucas under the FWTA.

The difference between Briggs, and Deal is that in Deal, the Spears intercepted and recorded Deals' personal phone calls even though it was obvious that such calls were personal in nature and were not at all related to the Spears' business. In Briggs, the intercepted call was purely business-related.

5. Eliminating Employees' Reasonable Expectation Of Privacy

Employers are also permitted to intercept, monitor and record their employees' communications in the workplace whenever the employer has **clearly** obtained the employees' consent to do so. In order to be effective, the notice given to employees must clearly destroy any reasonable expectation of privacy they might have formerly enjoyed.

Some jurisdictions have held that this notification given to employees must be **very clear and that such notices will be strictly construed against the employer**. In fact, some courts have held that merely notifying employees that the employer is **able** to monitor their communications whenever it desires is **inadequate**. Rather, the employer must inform its employees that it **will be monitoring** their communications. (Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).

Therefore, such consent must come in the form of clearly putting the employees on notice that their communications **will be monitored by the employer…not simply that these communications may be monitored or that the employer reserves the right to monitor these communications.** If an employer clearly puts its employees on notice

that they enjoy no reasonable expectation of privacy in their workplace communications, and that the employer will be intercepting their communications at any time as it deems appropriate, then the employer may monitor its employees' communications and not be in violation of the FWTA.

6. Party To The Communication

Whenever an employer is actually a party to an employee's communication, the employer is able to intercept, monitor, and record the message. Whether the employer would want to disclose the communication depends on privacy laws, for instance, and the content of the message.

As a general rule, employers should only disclose information regarding their employees to those individuals who are on a need-to-know basis.

7. May An Employer Monitor the <u>Personal Communications</u> of Its Employees When The Employees Have Been Placed On Notice?

Even if an employer monitors an employee's communication in the ordinary course of its business based on a legitimately related business reason, the courts have tended not to allow employers to monitor their employees' personal communications. Instead, employers have been permitted to monitor their employees' communications **only long enough to discover whether the communication is personal or business-related**. Once it is determined that a communication is personal, the employer must immediately cease monitoring the communication.

Of course, **IF** the employer has a policy of "no personal communications" during ***<u>working time</u>***, the employer may then deal with the employee accordingly.

On the other hand, some courts have indicated that when an employer has clearly put its employees on notice that their communications will be and are monitored by the employer so that these employees enjoy no reasonable expectation of privacy in the messages they send or receive, then there is really no difference between a personal or a business-related communication. The employer may intercept, monitor and record them freely. However, many courts have not ruled on this issue as of yet.

As the best matter of course, many employers choose not to intercept or monitor the personal communications of their employers for many reasons. Actually, putting employees on clear notice that they enjoy no right to privacy in their personal workplace communications can be an employee relations nightmare.

Further, if an employer becomes privy to some very confidential

information regarding an employee as a result of monitoring personal communications, such as the employee is having an extra-marital affair, has become pregnant, or is HIV positive, the employer could face tremendous liability if such information would negligently "leak out." In practicality, the more interesting the information is, the greater the likelihood it will be passed onto others.

And finally, there is really no business reason to monitor the personal communications of employees. If an employee is making a personal communication in violation of company policy, the employer is permitted to determine the nature of the message, stop its monitoring once it is discovered that the call is personal in nature, and then deal with the employee accordingly. There is really no advantage to continuing to monitor an employee's communication once it is determined that the message is personal.

Therefore, many employers who have placed their employees on notice that their communications will be monitored do not continue to monitor these communications once the nature of the message is determined, even though they may be legally permitted to do so.

C. Does The FWTA Cover Cordless Telephone Communications?

Although the use of cordless telephones is becoming increasingly more common, the federal courts are split as to whether the FWTA protects communications.

In U.S. v. Hall, 488 F.2d 193 (9th Cir. 1973), Hall made a call on his car telephone in which he stated that he had in his possession marijuana and that he intended to distribute it. This message was intercepted and Hall was arrested. Hall claimed that intercepting his telephone call violated the FWTA.

The Ninth Circuit agreed with Hall and held that his telephone communications were covered technically under the FWTA.

However, the Ninth Circuit also held that Hall's oral communication **was not** covered by the FWTA, since he did not enjoy a reasonable expectation of privacy when using a cordless telephone. Under the FWTA, in order for an oral communication to be protected, the FWTA required that the individual enjoy a reasonable expectation of privacy in sending or receiving the message.

The court then reasoned that no reasonable expectation of privacy exists when a person uses a cordless phone since the person's message is sent out into the atmosphere where anyone can intercept it. The Ninth Circuit therefore held that oral messages sent over a cordless telephone are not covered by the FWTA.

In Tyler v. Berdot, 877 F.2d 705 (8th Cir. 1989), the Eighth Circuit agreed with the Ninth by also holding that no justifiable expectation of privacy exists when sending a message by way of a cordless telephone. However, contrary to the

Ninth Circuit's holding in Hall, the Eighth Circuit in Tyler court also held that no wire communications are involved in sending messages by way of cordless telephone. As a result, the Eight Circuit held that the FWTA does not protect communications sent by way of cordless telephones.

D. FWTA Summary

Consequently, under the FWTA, as amended, intercepting or disclosing an employee's communication in the workplace is illegal if:

1. **There is an interception of an employee communication by means of any electronic, mechanical or other device, and**

2. **The employee had no expectation that the wire or electronic communication was subject to interception, and the employee's expectation was reasonable under the given circumstances,**

3. **The person who intercepted the communication was not a party to it, and**

4. **The communication was not related to the employer's business.**

II. TITLE II OF THE EMPLOYEE COMMUNICATIONS PRIVACY ACT: MONITORING STORED COMMUNICATIONS (18 U.S.C. § 2701 et seq.)

A. Coverage

Once an electronic communication, such as an e-mail, has been received, it becomes a "stored" communication. As a result, since the FWTA only covers the "interception" and disclosure of intercepted communications, the FWTA does not protect employees' privacy rights regarding their stored e-mail messages. Therefore, if an employer wanted to go into an employee's computer terminal and read the employee's stored e-mails, the FWTA would not protect that employee's privacy rights, even if these e-mail messages were personal and not business-related.

To correct this gap in the law, Congress passed Title II of the Electronic Communications Privacy Act, or the "ECPA" (18 U.S.C. § 2701, et seq.). However, since the ECPA applies to communications that have already been received, the ECPA is also referred to as the "Stored Wire Act."

Therefore, whether monitoring another person's electronic communication falls under the FWTA or Title II of the ECPA depends on whether the message was intercepted "on route," wherein the FWTA would apply. On the other hand, if the message had already been received and was in "storage" when it was monitored, Title II of the ECPA would cover this communication.

Under Title II of the ECPA, even though employers are not permitted to retrieve the stored personal e-mail communications of their employees, the same exceptions that apply to the FWTA also apply to Title II of the ECPA.

B. Eliminating Employees' Reasonable Expectation Of Privacy

If employees are clearly put on notice that they enjoy no reasonable expectation of privacy in their stored e-mail communications, then just as under the FWTA, employers will be permitted to review these messages.

C. Ordinary Course Of Business Exception

Just as under the FWTA, the "ordinary course of business" exception also applies to the ECPA. Therefore, if an employer reviews the e-mail messages of its employees based upon a legitimate business reason without first notifying its employees that such monitoring will occur, then no violation of the ECPA will exist. Such monitoring may be permitted in order to allow employers to perform maintenance functions on their computer systems or to determine if employees are using their systems in prohibited ways.

In Bohach v. City of Reno, 932 F.Supp. 1232 (D. Nev. 1996), where the police department retrieved the electronic messages two officers were sending to one another, the court held that the police department did not violate the ECPA by retrieving these messages. Instead, the court reasoned since employees do not enjoy a reasonable expectation of privacy when sending such e-mail messages, and since these messages were stored on the employer's system, the police department was free to access these messages.

D. E-Mail Cases

In Bourke v. Nissan Motor Company, No. YC003979, Cal Sup. Ct., Los Angeles Cty. (1991), the employer terminated two employees who sent e-mail to one another that contained off-color jokes and criticized their supervisor. The court ruled that the employer was entitled to read the employees' e-mail because the company owned the system on which the message was stored.

In Smyth v. Pillsbury Company, 914 F. Supp 97 (E.D. Pa. 1996), when the employer discovered that an employee was sending "unprofessional" and "inappropriate" e-mail over the employer's system, he was terminated. The court held that unless the employer had given this employee some assurances that it would not monitor e-mail messages, reviewing the employee's e-mail did not violate the state's public policy regarding privacy rights.

In fact, the court reasoned that once an employee sends a message over an e-mail system, any reasonable expectation of privacy is lost. The court also held such monitoring is not a highly offensive or substantial invasion of an employee's privacy rights.

III. CONSIDERATIONS UNDER BOTH THE FWTA AND THE ECPA

A. "Affect Interstate Or Foreign Commerce" Requirement

Both the FWTA and the ECPA state that in order to have jurisdiction, the applicable communication must "affect interstate or foreign commerce."

Therefore, whenever a communication is sent via a public network (i.e., America On-Line, Prodigy, etc.), the message would clearly be covered by the FWTA or the ECPA respectively, since the message would be viewed as having entered and "affected interstate or foreign commerce."

However, if a communication is sent via an entirely internal system, the question arises whether the FWTA and the ECPA apply since it is questionable if the message did in fact "affect interstate or foreign commerce."

Of course, it can also be argued that when the employer purchased this equipment, it affected interstate or foreign commerce, which would place its employees under the protection of the FWTA and the ECPA. Still, this issue remains unresolved by the courts.

IV. OTHER STATES AND ELECTRONIC WORKPLACE LAWS AND/OR PRIVACY

Since many companies have employees in different states or conduct business in different states, they should also be aware of the fact that not only are they governed by the FTWA and ECPA, but each state also has their own privacy, wiretapping and electronic communication laws. Depending on which state a company is conducting business in, the rules could be very different.

States like Ohio mirror the FWTA and the ECPA.

However, Massachusetts' privacy law reads as follows:

"A person shall have a right against unreasonable, substantial or serious interference with his privacy."

Other states constitutions, such as Alabama, have provisions that are identical to the Fourth Amendment of the U.S. Constitution.

Further, some states include in their constitutions a guarantee of privacy. Some of these states include Alaska, Arizona, California, Florida, Illinois, Louisiana, Montana, South Carolina and Washington.

V. LIABILITY AND DAMAGES UNDER THE FWTA AND THE ECPA

Penalties under either the FWTA or the ECPA can run as high as the actual damage to the plaintiff, or the greater of $100 a day or $10,000 per offended individual. Also, since both laws apply to "any person," not only can employers be held liable for violating these laws, but both the employee and the individual with whom the employee was communicating under both the FWTA and Title II of the ECPA can also hold managers personally liable.

In Rodgers v. Wood, 910 F.2d 444 (7th Cir. 1990), the court held that the awarding of damages is mandatory. However, in Nalley v. Nalley, 53 F.3d 649 (4th Cir. 1995) the Fourth Circuit held that whether a court decides to award damages is discretionary.

Also, not only can an employer be held liable for violating the FWTA and the ECPA, but managers can be held personally liable as well. In Deal, the court ordered Newell and Juanita Spears to each pay $10, 000 to Sibbie Deal and another $10,000 to Calvin Lucas. Altogether, the Spears were ordered to pay $40,000 in damages.

A. General Guidelines: How Employers May Protect Themselves

Employers who decide to monitor their employees' communications should consider undertaking a few preliminary measures in order to protect themselves from incurring liability for such actions.

1. Employers should first adopt, implement and publicize an "Employee Communications Monitoring" or "Data Systems" policy, which may inform employees that:

    a) The employer owns all of the equipment throughout the workplace by which messages are created, sent and received. Every message transmitted through or stored in this equipment is therefore the property of the company, so the employer may intercept, retrieve, monitor and record every communication made and received on its various systems without first notifying its employees. The employer may also allow others to monitor employee communications as it deems appropriate, such as in the case of business necessity, for reasons related to safety, or under the order of subpoena, to mention a few.

    b) Employees should not expect any privacy in creating, sending, or receiving communications in the workplace, regardless of whether they have been assigned or use a password or security code. Further, employees should not expect any privacy even regarding those communications that have been deleted from the system, since messages may often be retrieved after being erased.

c) Employees are required to provide the employer's MIS manager their e-mail passwords.

d) The employer's telephone system may be used for personal matters, but not to excess, as determined by company management.

e) Employee communications are to never contain any offensive, harassing or discriminatory materials or messages, as determined by the employer.

f) Employees should not interpret the rights the employer has reserved for itself to intercept, retrieve and/or monitor their communications as granting them permission to intercept, retrieve and/or monitor the messages of their fellow employees.

Employees should also not interpret these rights reserved by the employer as constituting a waiver of their duty to keep confidential information secured, which may include such items as company trade secrets, financial information, copyrighted materials and other materials or information of the employer.

g) Any authorized or unauthorized projects developed with the employer's equipment or resources become the property of the employer, regardless of whether the product was developed during business hours.

h) Employees are prohibited from bringing any proprietary materials from any other employer into its workplace, and employees are forbidden from taking any proprietary materials belonging to the employer from its workplace without written permission.

i) Employees are to never disguise or conceal their identity when sending e-mail messages.

j) Employees are not permitted to engage in spamming.

k) Employees are to never download any data that may be copyrighted material.

l) Employees are not to forward chain mail.

m) Employees are not to forward e-mails to others without the permission of the sender.

n) Employees are to never send an encrypted message without permission from management. However, employees are to never

send trade secret or confidential information over the Internet without having first encrypted the message.

2. The employer's policy on this matter should be included in the company's employee handbook. This handbook then should be signed by every employee as having been read, understood and accepted as a condition of employment. Employees should also be informed that violating the employer's policy on these matters would subject the employees involved to the company's disciplinary policy, which includes possible termination.

3. Employers should also place on their computer screens a reminder telling employees every time they sign on that they enjoy no expectation of privacy in their communications and that the employer reserves the right to freely intercept, retrieve and monitor any messages on its system.

4. Employers should also adopt procedures that employees must follow whenever they download software or information from some outside source in order to protect its systems from viruses and access by unauthorized personnel.

5. Security measures that are able to reasonably protect the employer's confidential information and trade secrets should also be implemented.

6. Employers should also train their managers in how to properly monitor the communications of their employees. Managers must understand that in spite of the company's policy, they are still only permitted to monitor those communications that are in the ordinary course of business and are legitimately related to the employer's business. Personal communications should not be monitored.

   Therefore, once it is discovered that an employee is making a personal communication, the monitoring should end. The employee may then be dealt with accordingly if personal communications are forbidden or restricted.

7. Managers must also realize that if they do become aware of personal information due to monitoring an employee's personal messages, these managers should treat this information as being confidential and are permitted to disclose it only to those who are on a legitimate need to know basis.

B. Other Privacy Issues

1. Photographing Employees

Even though several states regulate the use of cameras by employers, an employer's right to photograph its employees in public places has generally been upheld. This situation often arises when an employee

claims some type of personal injury at work and the employer then tries to prove that the employee is not really injured by following the employee and photographing the employee's actions. Almost universally, whenever the employee is in public, such practices have been upheld.

However, photographing employees in the workplace without their knowledge has been met with mixed results. Therefore, as a general rule, it is maybe best to notify employees that they are being photographed if that is indeed the case.

2. Searching Employee Work Stations

As a general rule, if an employee enjoys a reasonable expectation of privacy at his workstation, locker, and so on, many states prohibit employers from searching such areas. Employees have been found to enjoy a reasonable expectation of privacy if they are able to secure their work areas from others, including the employer.

For instance, if an employee is able to lock his office, desk or locker, and the only person who holds the key to any of these areas is the employee, then a strong argument would exist that the employee enjoys a reasonable expectation of privacy in these areas.

Therefore, if an employer intends to search such areas, it should adopt a policy which clearly informs its employees that they should expect no right of privacy from the employer in any of their work stations, lockers, and so on, since such areas always remain the employer's property, irrespective of whether an employee has been permitted to secure such areas.

However, regardless of any properly adopted policy, searching an employee's non-work-related property, such as an employee's car or his home, have generally not been upheld.

3. The U.S. Constitution

In the public sector, it is well established that employees enjoy at least some right to privacy under the Fourth (prohibition against "unreasonable search and seizure") and Fourteenth Amendments (liberty right to privacy) of the U.S. Constitution.

In O'Connor v. Ortega, 480 U.S. 709 (1987), the U.S. Supreme Court held that public sector employees enjoy a reasonable expectation of privacy regarding their desks and files in their private work areas. However, in order for a "right to privacy" to exist in the workplace, the employee must have a subjective, although reasonable, expectation of privacy. Still, the Court held that "the operational realities of the workplace" might reduce or eliminate an employee's expectation of privacy. Therefore, an

expectation of privacy may become unreasonable based upon "actual office practices and procedures, or by legitimate regulation."

However, the Court also held that even if a right to privacy does exist, a public sector employer might still conduct a reasonable search without a warrant. The U.S. Supreme Court indicated that in such a situation, one must balance the employee's legitimate expectation of privacy and the employer's need for supervision, control, and efficiency in the workplace. If the latter prevails, then a "reasonable search," that is, one that is reasonable with regard to both the extent of the intrusion and the underlying reasons for the search, may be performed.

Therefore, again, if a public employer wants to be able to search its employees' work areas, the employer should be certain to remove any reasonable expectations of privacy by placing employees on notice that such searches may take place.

Still, the Ortega decision applies ***only*** to public sector employees, and most commentators believe that there is no right to privacy in the workplace for private sector employees based upon the U.S. Constitution. On the other hand, a few jurisdictions have found that a right to privacy does exist for private sector employees under the U.S. Constitution.

VI. UNDERSTANDING E-MAIL, THE INTERNET AND LIABILITY FOR EMPLOYERS

A. Encryption

Encryption is a method of sending digital messages in a scrambled format, or in "gibberish," in order to prevent unauthorized persons from gaining access to the entire message. Once the message is received, it can be decoded by anyone who has the proper key. Therefore, it is not enough to simply encrypt messages, but employees should be informed to NEVER release their code number to anyone.

The best encryption formats have two pass keys…one public, which may apply to employees of a certain department, division, geographic location, or so on, and one private, which is a code assigned to the employee specifically. These encryption systems, such as "Pretty Good Privacy" ("PGP") can be purchased on the open market and installed into a company's computer system.

However, the downside of using encryption technology is that it can also be used by employees to block the employer's access to employee messages and documents. Employees can also use this technology to hide their identity when sending e-mails.

Employers should therefore adopt a policy that forbids employees from using any form of encryption to hide their messages from the company, to send anonymous e-mails or to conceal documents from the company.

B. Intentional Misuse of E-Mail and the Internet

1. Spoofing

Employers should be aware of the fact that employees can send e-mails to one another, or even outside of the workplace using the employer's equipment, and make it appear as if the e-mail came from someone else. This process is referred to as "spoofing."

Although hiding one's identity as the author of an e-mail used to be difficult, this process has been made much easier with the advent of numerous "remailers" that can be found on the web. A "remailer" is a relay station that deletes the identity of the person sending the e-mail, gives the e-mail a new identity and then forwards the e-mail onto the desired location.

Therefore, if an employee wanted to send an anonymous e-mail to another person, or if the employee wanted to send a threatening e-mail to someone and put another person's name on it as the sender, this would be relatively easy. The employee would just send the e-mail to a remailer site on the web, the remailer would strip the employee's name and return address from the e-mail, the remailer could then place a new name and address on the e-mail, as instructed by the employee, and the remailer would forward the e-mail to the correct party.

Needless to say, the existence of such remailers on the web creates many issues for employers regarding illegal harassment, stalking, etc. Employers should therefore put into their policies a statement that forbids employees from hiding their identity when sending an e-mail. It may also be a good idea to inform employees that entering a remailer address on the web is a terminable offense. Employers should then track where their employees are going on the web.

2. Spamming

"Spamming" occurs when someone sends a mass e-mail to many individuals whom the sender does not know or have a relationship. Spamming is usually used as a way to market a vendor's product to potential customers.

Employers should include in their policies a prohibition against spamming without management approval since some states, such as Nevada, have made it illegal to engage in spamming.

3. Harassment

More and more, the electronic workplace is creating liability for employers due to the illegal messages that are sent and stored on the employer's equipment.

In Coniglio v. City of Berwyn, 2000 U.S. Dist. LEXIS 9841 (N.D. Ill July 12, 2000), a supervisor's computer screen faced the window where all of his employees and passersby could see what he was viewing. However, throughout the day, the supervisor would often view pornographic material, which was seen by anyone who went by his office. The court held that a jury may consider the supervisor's conduct helped to create a sexually hostile environment.

In Blakey v. Continental Airlines, NJSCt. 2000, Tammy Blakey was not only a commercial airline pilot for Continental, but she was the airline's first female captain to fly an Airbus aircraft. Shortly after assuming this role, she began complaining to management that her male counterparts were posting pornographic pictures and vulgar comments in her plane's cockpit. When Ms. Blakey felt her complaints were not taken seriously, she sued in federal court for sexual harassment.

While this suit was pending, Ms. Blakey's co-workers began posting a series of derogatory messages about her on an online bulletin board used by Continental's pilots and crew members. (Continental contracted with EDS to provide this online information system so its pilots can access flight schedules and assignments. As part of this service, EDS contracted with CompuServe to provide this online bulletin board. All pilots were required to access the EDS information site…but not the CompuServe site.)

Blakey filed another suit based on these electronic messages for retaliation and sexual harassment hostile environment.

The New Jersey Supreme Court found for Ms. Blakey. The court reasoned that this online bulletin board acts the same as a traditional employee bulletin board. As a result, these offensive comments posted by Continental employees did in fact contribute to Ms. Blakey's hostile environment and did serve as retaliatory acts. The court then held that Continental did not take appropriate steps to end the harassment once it became aware of it.

Ms. Blakey won $600,000.00 in her suit. She has now filed another suit based on defamation against Continental.

In Strauss v. Microsoft Corp., 814 F.Supp. 1186 (S.D.N.Y. 1993), a female employee sued Microsoft for sexual harassment discrimination. The female employee based her case partly on evidence that her supervisor sent e-mail messages to the entire staff that included "sexual innuendo referring to the male genitalia," they referred to women in offensive terms and one e-mail message contained a parody entitled, "A Girl's Guide to Condoms." The supervisor also referred to himself in e-mails as the "president of the amateur gynecology club."

In 1995, a female employee filed a $2,500,000.00 sexual harassment lawsuit against Calsonic International, Inc. based upon lewd e-mails that were frequently sent to her by a male co-worker.

In 1997, the Chevron Corporation was sued by four female employees claiming they were sexually harassed through the company's e-mail system. The case settled for $2,200,000.00.

Further, in Owens v. Morgan Stanley & Co., 74 Fair Emply. Prac. Cas. (BNA) 876 (S.D.N.Y. 1997), racist e-mails were circulated among white employees in the workplace. As a result, two black employees brought suit against their employer for $25,000,000.00 each, alleging a hostile work environment based upon race.

Further, in Owens v. Morgan Stanley & Co., 74 Fair Emply. Prac. Cas. (BNA) 876 (S.D.N.Y. 1997), racist e-mails were circulated among white employees in the workplace. As a result, two black employees brought suit against their employer for $25,000,000.00 each, alleging a hostile work environment based upon race.

a) Hate groups

Whenever someone brings up the subject of keeping employees out of harassing or discriminatory Websites, almost automatically the subject goes to pornography on the Internet. As a result, employers often place "guards" on their systems to prevent employees from going into pornographic Websites. However, just as dangerous for employers are Websites that are sponsored by hate groups and promote bigotry.

If an employer fails to monitor where its employees are going on the Internet, and if the employees are freely going into Websites sponsored by hate groups, then an argument can much more easily be made that an atmosphere of racial, religious or ethnic animus exists in the workplace.

It is also important for employers to remember that official hate groups exist everywhere. Such groups are not relegated to the southern part of the United States. In fact, according to the

Southern Poverty Law Center (SPLC) of Montgomery, Alabama (www.splcenter.org), an organization that tracks official hate groups across the entire U.S., there are approximately 460 active hate groups operating in the U.S. Such groups are categorized as Klan, Neo-Nazi, Skinhead, Christian Identity and Black Separatist, to mention a few.

The Center also identified over 400 patriot groups in existence across the entire U.S. (A "patriot group" is an organization that opposes the "New World Order" an advocates or adheres to extreme antigovernment doctrines.)

Therefore, with hundreds of hate and patriot groups scattered throughout the entire United States, north and south alike, employers should take active steps to keep such discriminatory activity out of their workplaces…both in hard format and via the electronic highway.

b) Electronic communications are never really gone

Employees must understand that drafting an e-mail or a document on a harddrive is infinitely more dangerous that drafting a hardcopy document. With a hardcopy, the paper can be shredded and the information destroyed. This is not the case with computer-generated documents.

Even if an employee "deletes" old e-mails and old documents drafted on a harddrive, they are never really gone. Somewhere on the harddrive, they still exist and may be easily retrieved by a data systems professional. Therefore, if these documents and e-mails contain evidence of illegal or harassing conduct or an atmosphere that permits such conduct to occur, they may be retrieved by plaintiff's counsel and used against the employer in court.

Therefore, employees should be instructed to never put any harassing or discriminatory comments into a computer-generated document, which includes e-mail.

c) Internet trails

Whenever an employee goes out onto the Internet, an electronic record is left behind in the employee's harddrive…and possibly on the company's mainframe system, depending on how the employer's computer systems are configured.

Specifically, "cookies" are left behind in the employee's computer system. These cookies record where the employee has been on the internet and leaves a trail back to that site so the employee can get

there even faster the next time he/she desires to visit that site again. As a result, if employees are going into pornographic websites or hate group websites, this information can be retrieved and used against the employer as evidence that it is allowing a sexually hostile or discriminatory atmosphere to exist.

Employees should also be aware of the fact that when they visit a website, the Webmaster may have inserted a "spider" program into the site. The "spider" then attaches to the electronic trail left by the employee and follows the employee back to his/her e-mail address. The Webmaster then has the capability to e-mail the employee with messages and advertisements.

The company's policy should therefore forbid employees from visiting any illegal, discriminatory (i.e., hate groups) or pornographic websites.

d) No Free Speech

Interestingly, in Urofsky v. Gilmore, 167 F.3d 191 (4th Cir. 1999) a public sector employee claimed that a Virginia state law prohibiting employees from accessing sexually explicit material over state-owned computer systems violated his right to free speech under the First Amendment of the Constitution.

However, the court held that the state's interest in banning sexual material from the workplace far outweighed public employees' right to express themselves on sexually explicit matters. Therefore, even in the public sector where employees have all the rights afforded under the Constitution, prohibiting employees from accessing certain websites has been found to be permissible.

e) Helping to ensure compliance

In order to help ensure that employees are not visiting these websites, employers should appoint a Data Systems Compliance Officer. This Compliance Officer should monitor where employees go on the Internet and confront those employees who go into forbidden sites.

It is also advisable to install screening software that prevents employees from visiting pornographic websites. Such programs will help keep employees out of pornographic websites, for instance.

The employer's Data Control Policy should also advise employees that their e-mail and Internet trails and data will be monitored by the Data Systems Compliance Officer and that no discriminatory,

harassing or illegal data should be accessed or written on these systems. This policy should also clearly state that all such information is the property of the employer. The employer may therefore distribute and publicize this information as it sees fit.

4. Employers' Duty To Monitor

Many employers have a moral problem searching through their employees' e-mails and voicemails looking for inappropriate messages or information. Such employers see this as an invasion of the employees' privacy…if not legally, then morally. Such employers make an excellent point from an employee relations perspective, so when they do reserve the right to examine the employees' messages, employers should still proceed with caution and not abuse this authority in order to avoid a relations nightmare.

However, the questions surrounding whether an employer should be examining its employees' electronic communications are long over. The clear trend in the courts is to place an obligation on employers to monitor and enforce their policies. The reasoning by the courts is that the employer controls the workplace and should therefore monitor and enforce its policies. (Baker v. Weyerhauser Company, 903 F.3d 1342 (10th Cir. 1990); Campbell v. Leaseway Customized Transportation Inc., 1992 WL 72073 (Minn. Ct. App. 1992)) As a result, simply adopting a policy and providing training is not good enough. Employers are required to monitor their work environments to see that their policies and the law are being upheld.

Therefore, the question as to whether an employer should monitor its employees and their communications has been answered in the affirmative by the courts. The only question to decide now is how each employer is going to accomplish this obligation of monitoring.

5. Erasing Internet Trails and Erasing Harddrive Data

In spite of whatever policies or monitoring procedures an employer might put into place, employees are going to visit pornographic websites, hate group websites and they are going to draft and receive offensive e-mails and computer generated documents.

More and more, plaintiff's attorneys are using a company's own e-mails and Internet trails against it in employment law suits to show that the employer allowed an illegal hostile environment to exist.

For instance, if employees send discriminatory or obscene e-mails to one another, or if employees go into pornographic or "hate group" websites, this data can be used against an employer. Specifically, if employees send such e-mails and go into such websites, it can be argued that the employer

allows a "sexually offensive" or a discriminatory atmosphere to exist in the workplace. This evidence may to used against employers when such lawsuits arise.

In order to protect themselves, companies are beginning to be more diligent about erasing these "trails" and deleting documents. Software can be installed that will erase these trails to Internet websites. Data systems professionals may also install programs that will routinely destroy those documents that employees think they have deleted. This way, if employees are going into forbidden websites or saying things in e-mails or electronic memos that are questionable in nature, this data cannot be used against the employer in the future.

Of course, employers should review this data before it is erased and see if employees are engaging in prohibited behavior. If so, appropriate disciplinary action should be taken before the data is erased.

Further, if an employer is going to erase such data, this practice should be placed on a regular schedule as part of its ordinary business procedures. It is illegal for a company to go into its company records and destroy them in anticipation of a lawsuit. However, when such a practice is part of the company's normal routine, no obstruction of justice charge would exist.

There are other reasons a company may want to do this. First, if a certain message is objectionable, it will not be "hanging around" in the system waiting for another employee to run across it, or have it accidentally mailed to them.

Second, cleaning out old information frees up the company's electronic resources. Old data and messages simply use up valuable computer space.

VII. USING THE INTERNET FOR RECRUITMENT

A. The Convenience of Internet Recruiting

Recruiting on the Internet has exploded over the last few years. There are countless websites available for individuals to surf through and gain access to literally thousands of jobs…all right at their fingertips. In fact, it is now the norm to submit application materials and resumes by way of e-mail rather than in a hardcopy format.

Electronic submissions of resumes are simple and greatly reduce the amount of paper employers have to retain. Electronic submissions also greatly reduce the chance that submissions will be lost.

Further, with the software that is available today, when an employer has its resume database in its computer system, searching for individuals with the right skill sets is much easier. These resume search systems allow recruiters to search

their electronically stored resumes and applications by certain desired skills and retrieve only qualified applicants.

Even when resumes are submitted in a hardcopy format, employers most often scan the information into their human resource information systems, which can then be accessed by their resume tracking retrieval system.

B. The Danger of Internet Recruiting

Due to its convenience, many recruiters and companies will only accept electronic submissions from applicants. Moreover, for these same reasons, many employers and recruiters will only post their jobs on Internet job posting boards. Such an approach to Internet recruiting is a mistake…and illegal.

1. Minority access to Internet is low

First, more non-minority individuals have access to the Internet than do minority persons and women. As a result, if a company uses the Internet exclusively to conduct its search for qualified candidates, a disparate impact claim of illegal discrimination against minorities in violation of Title VII could be the result. Therefore, employers should make sure that they are using more avenues to recruit qualified candidates than just the Internet.

2. Key terms used in resume searches may be discriminatory

In 1997 the Walt Disney Company was sued for using a resume tracking system, Resumix. The plaintiffs alleged that this resume tracking software discriminated against minorities on the basis of race because the key search terms used were words more likely to be used by white individuals than by minority applicants. Therefore, when a search was performed, the software program selected the resumes of white individuals since minority persons tended not to use these key terms.

3. Solutions

In order to avoid these problems with tracking software, an accurate job description should first be developed. The criteria listed on the job description should be directly related and relevant to the job, such as education required, job skills, experience, salary range and any other essential job functions. Then, only these job-related criteria should be entered into the resume tracking software system to conduct a retrieval search. This way, the search will be based entirely on job-related criteria and not upon racially discriminatory criteria.

Further, multiple sources of accepting resumes should be permitted. Restricting submissions to only those sent by way of the Internet could present a serious legal problem for recruiters.

VIII. NEGLIGENT TRAINING

A. Poor Training May Be Discriminatory

1. Age may be a factor

The computer age is here…for most Americans. Ninety-nine percent of all businesses in existence today are deeply dependent on computers. However, since this has not always been the case, some older Americans have not had the exposure to computers that Generation Xers have had in their youth. Also, many minorities have not had the same exposure to computers that those non-minority children have experienced. As a result, the area of negligent training has emerged.

For example, assume an older employee has just been terminated because his computer skills were outdated. One good argument for the employee to advance is that his skills were outdated because the training he received was inadequate. The employee may also argue that he was denied training because he was a minority or the member of some protected class.

Further, since younger employees are in fact more comfortable with computer-based training, employers tend to offer this training to younger employees before the offer is made to older workers. The Equal Employment Opportunity Commission's "Uniform Guidelines on Employee Selection Procedures" state that selecting employees for training must be done without discrimination on the basis of age, race, national origin, disability or any other protected category. (29 C.F.R. § 1607.2)

Therefore, when employers tend to choose younger workers for computer training over older workers, the stage is set for an age discrimination suit.

In order to avoid these problems, employers must document the training programs that have been made available to employees. When an employee is failing in his job, the counseling sessions held with the employee should include a discussion regarding additional training needed. If the employee refuses to go to training, the employee should sign and acknowledge that he has declined this offer of training.

2. Access and accommodation for the disabled

Employers also face disability discrimination suits for failing to make training available to those persons who are disabled. Making access ramps available to those in wheelchairs, providing voice-overs or readers for the visually impaired, adding closed captions for the hearing impaired

and offering individualized assistance for the mentally disabled are all examples of reasonable accommodations that employers should provide under the Americans With Disabilities Act of 1990.

In Vollmert v. Wisconsin Dept. of Transportation, No. 98-3673 (7th Cir. Nov. 11, 1999), Jane Vollmert had been employed by the Wisconsin Department of Transportation for over 21 years when the Department installed a new computer system. In her most recent position with the Department, Vollmert processed specialized license plates for the disabled and certain organizations serving the disabled. Vollmert herself suffered from learning disabilities, such as dyslexia. As a result, she had a very difficult time learning how to use the new computer system in her job.

The Department gave her computer training, but she could not retain what she had learned and use it later in her duties. As a result, the Department gave Vollmert one-on-one computer training. However, again, Vollmert was unable to retain this instruction and was therefore unable to apply these skills on the job.

As a result of her inability to operate the computer, Vollmert fell way behind on her production requirements. While Vollmert's co-workers were able to process 50 to 60 applications every two hours, Vollmert was only able to process an average of 67 new applications a day.

Vollmert's union president suggested that the Department hire a specialist to assist Vollmert with her training. In fact, learning disability specialists were available from the state at no charge. However, Vollmert's supervisor denied all of these requests, claiming that Vollmert had already received sufficient training.

The supervisor then gave Vollmert an ultimatum: she could either continue in her current job for another four months, and then be subject to discharge for poor performance if she did not meet the standards set for her, or she could accept a transfer to another position not requiring the use of a computer. Vollmert reluctantly chose to accept the transfer…the sued the Department for disability discrimination under the ADA.

The Department defended itself by claiming that Vollmert was not a "qualified person" for this position any longer since she could not perform its essential functions…one of which was to operate a computer. The Department argued that it gave Vollmert one-on-one training, which did not work. It then claimed to have accommodated Vollmert again by transferring her to another position.

However, Vollmert claimed the training she received did not meet her special needs. Vollmert contended that she could be a "qualified person" for this job if she received the type of training she needed.

The court ruled in favor of Vollmert.

The court based its ruling largely upon the opinion of a vocational expert. The vocational expert testified that Vollmert could become proficient in operating this computer if she was properly trained. The vocational expert stated that Vollmert's disability did not affect her **ability** to learn…it affected the **speed** at which she learned. The vocational expert claimed that if Vollmert was given time to actually learn these skills, she would be able to work at a high level of productivity and efficiency.

However, the expert also noted that this training should be conducted by someone who has experience in working with people who learn at a slower rate that the normal population.

The court therefore ruled that the use of a proper trainer was the appropriate reasonable accommodation… not a transfer.

Therefore, employers should make certain that they are accommodating the needs of their disabled employees so they too are afforded the advantages training brings. When disabled individuals are involved, oftentimes the opinion of an expert will be required.

3. Track sessions

Employers should also track which training sessions their employees attend in order to ensure that all protected classes are given equal opportunities.

The accommodations offered to disabled employees should also be documented.

And finally, if an employee refuses training or a certain accommodation, the employee should sign an acknowledgement that the offer was made and refused.

4. Retain the content of the training offered

More and more, plaintiff's counsels are questioning the validity of the training offered to employees. The argument plaintiff's counsel is trying to make here is that the employer only went through the motions of offering training to its employees and that no real substance existed. The content of the training programs being offered should therefore be retained to show that the training program was of high quality, rather than simply going through the motions.

Further, the credentials of the person teaching the session should also be recorded. The higher the credentials of the person teaching the class, the

more credibility the training session will have when it is being second-guessed in hindsight by plaintiff's counsel.

B. Proper Training Can Reduce Other Liabilities and Improve Efficiency

The best return an employer can get on its new equipment is to make sure its employees are properly trained on how to operate it. If not, then employees will lose a great deal of time either "tinkering" with the equipment, or making mistakes with it. When it comes to computers and the new technology used to store and transmit information, this fact can be especially disturbing. If an employee is not properly trained in how to use new technology, such as a new computer software program, not only will the employee fail to use the system at its maximum effectiveness, which costs the company money in lost productivity, but the employee could easily send the wrong information to the wrong people.

For instance, if an employee sends a person's medical information to unprivileged parties, the company may be facing a lawsuit based upon a violation of privacy. If employees mistakenly e-mail off-color or racist jokes to unintended parties, a lawsuit could easily erupt. If employees mistakenly disseminate a company trade secret to the public, or continually e-mail trade secrets to others outside the premises without first encrypting the message (probably because they did not know how to use the encryption software), the company may lose its right to classify this information as a trade secret and all of the legal protections afforded to trade secrets. Therefore, training employees on new technology is vital to 21st century business.

IX. COPYRIGHT INFRINGEMENT

A. The Danger of Copyright Violations

With all of the information that is available on the web today, the entire world is at one's fingertip. However, that is part of the problem…the entire world IS at one's fingertips…which includes copyrighted information.

Further, software programs exist that will do all kinds of things that will make our lives easier. More than that, almost everyone knows another person who has discovered the latest and greatest software programs that will do everything but gargle for them. As a result, employees often borrow software from their friends and not only install it at home, but they bring it to work and install it for their use there. Again, the employer has another copyright problem.

If an employee brings pirated software into the workplace and installs it, the employer is automatically liable. If the software cannot be validated with purchasing records, for instance, a conviction for violating federal copyright laws may follow.

If an employer is found guilty of infringing on an author's copyright, the cost to the employer could be staggering. First of all, the employer would owe the holder

of the copyright his standard fee for every computer that is using the software. If the copyrighted information is a product like an article, training materials, a photograph or a cartoon, the employer would owe the publication fee to the author for each time the item was copied or used.

For instance, suppose a manager downloaded training materials from BNA's website that ordinarily cost $100.00 each. The manager then copies and distributes these materials to the employees of his company, who number about 200. The employer would owe BNA $20,000.00. Penalties would then be added onto this sum, which are often two times the damages.

B. Contributory Infringement

Employers may be found guilty of violating copyright laws even if it was not the one who actually performed the copying and distribution of these materials. Under the theory of contributory infringement, an employer may be held liable for the copyright violation committed by an employee if the employer had any knowledge of the illegal activity, or should have known, and induced or materially contributed to the illegal conduct.

C. Vicarious Liability

Under a theory of vicarious liability, an employer may be held liable for an employee's copyright infringement if the employer had the right and ability to supervise the employee's activity and had a financial interest in using these copyrighted materials.

Therefore, under one theory or another, employers will most assuredly be held liable for the copyright infringements committed by their employees.

D. Company Policy and Checking Before Downloading

Employers must therefore make it clear to their employees, both verbally and in policy, that they are to never download any materials from the Internet that appear to be copyrighted. (It is always safe to download and use materials from any governmental website.) Employees should be told that if they are in doubt whether or not an item they have found on the Internet, or anywhere else for that matter, is copyrighted, they should contact the author and ask.

If the information was found on the web, this could be as easy as e-mailing the Webmaster and asking. If the material was found some other way, the materials will almost always provide a way for the employee to contact the publisher of the material. Many times, publishers will grant one-time rights to copy and use within the organization. Therefore, violating an author's copyright makes no sense…either ethically or financially.

In order to be diligent, employers should also audit their employees' work areas and personal computers for illegal software. If it is found, it should be removed and disciplinary actions against the employee who installed it should begin.

Employers should also keep a catalogued listing off all the software licenses it has purchased for easy access.

X. DEFAMATION

Generally, the tort of defamation occurs when a false and unprivileged communication, either oral or written, is published to another person that has a tendency to injure another person regarding his/her reputation or occupation. In the world of employment law, the charge of defamation usually arises when corporate discussions occur that are not essential to the employment decision at hand, such as a termination.

With the advent of e-mails and voicemail, it is very easy to be bolder in the comments that are being made since the communication is not occurring in a face-to-face setting. In such instances, managers frequently go too far and say or write things they should not.

For instance, one manager e-mails to human resources a message outlining all of the problems he is having with a certain employee. However, the manager also speculates as to whether or not the employee is "brain damaged," just stupid or a clinical "idiot." The stage is now set for a defamation suit from the employee.

Even though it is perfectly acceptable to communicate performance or behavioral problems to those on a need to know basis, such as to human resources, calling the employee an "idiot," "stupid," or "brain damaged" is inappropriate and defamatory. Further, since this message is sent on e-mail, there is now a permanent record of these defamatory comments, which is why e-mail is especially dangerous.

Managers should be trained in the difference between discussing the performance and behavioral characteristics of an employee and name-calling. The company's policy should also forbid the use of any defamatory and offensive comments, either on the company's computers systems or not.

It may also be a good idea for the company to use encrypted technology when confidential e-mails are sent to reduce the chance of interception or retrieval by unauthorized persons.

XI. TRADE SECRETS

A. What Is A "Trade Secret"?

In general, a trade secret is any information that is:

1. Confidential (or a secret) and

2. Has economic value to the company because it is kept secret.

Examples of trade secrets include client lists, product designs, business plans, company processes, and computer programs.

B. Trade Secrets Must Be Protected

In order to remain a trade secret, employers must treat this information as a trade secret. In other words, if an employer is haphazard with its trade secrets and does not take reasonable measures to keep them protected, the employer will lose the protections offered to trade secrets.

Therefore, it is becoming very common for employers to protect their confidential information and "trade secrets" with various security systems, commonly referred to as "firewall" technology, such as with security screens, encryption, and so on.

In Valco Cincinnati, Inc. v. N & D Machinery, Inc. (1986), 24 Ohio St.3d 41, Valco accused N & D Machinery of procuring its trade secrets in violation of Ohio law. However, the Ohio Supreme Court, quoting the Second Restatement of Torts, reasoned that in order for something to constitute a trade secret and be entitled to protection under Ohio law, the employer must take "measures designed to prevent it, in the ordinary course of business, from being available to persons other than those selected by the owner to have access thereto for limited purposes."

The Ohio Supreme Court did not state what security measures were required for Valco to take in order to protect its trade secrets, but instead stated that Valco should have taken whatever steps were reasonable to protect its information. The court suggested that such precautions could have included the use of "buzzer locks" to restrict the access of personnel to this area where the information was stored, adopting a method of screening individuals before allowing them entrance to such areas, creating security areas in which only authorized personnel would be permitted access, classifying these documents in such a way that only authorized personnel would be permitted to view them, shredding classified documents, and implementing security procedures that would help to protect such information.

Since Valco failed to adopt any reasonable security precautions regarding this information, the court did not view this information as constituting trade secrets.

Based on either state or federal copyright law, several other courts have also required employers to implement reasonable security measures in order to protect such information before allowing an employer to argue that the data constituted a trade secret, such as in Business Trends Analysts, Inc., v. Freedonia Group, Inc., 700 F.Supp. 1213 (S.D. N.Y. 1988); Computer Assoc. International, Inc., v. Bryan, 784 F. Supp. 982 (E.D. N.Y. 1992); Religious Technology Center. v. Netcom On-Line Communication Services., Inc., 923 F.Supp. 1231 (N.D. Calf. 1995); Schalk v. State of Texas, 823 S.W.2d 633 (Tex. Crim. App. 1991).

C. Economic Espionage Act of 1996

On October 11, 1996, President Clinton signed the Economic Espionage Act of 1996 (or the "EEA") into law. Basically, the EEA imposes criminal liability on anyone who intentionally steals a trade secret, assists in the theft, knowingly receives a stolen trade secret or conceals the theft of a trade secret.

Under the EEA, the term "trade secret" is defined as being "all forms and types of financial, business, scientific, technical, economic or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing…" However, the EEA specifically states that if an individual or organization has not taken "reasonable measures" to protect their trade secrets, these protections will be lost.

The penalties for violating the EEA are severe. In addition to incarceration, individuals can be fined up to $250,000.00 and organizations can be fined up to $5,000,000.00.

XII. TELECOMMUTING

A. In General

Without a doubt, one of the greatest challenges facing employees today is balancing home and work lives. One method used by millions of Americans to achieve this balance is telecommuting.

Employees will often perform numerous work-related tasks at home before coming to the office, after going home in the evening and even in lieu of coming to the office. Technology allows employees to dial into the office just as if they were right there on site. Technology also allows employees the opportunity to carry their entire office with them anywhere they go in the form of lap tops, portable hard drives, and so on.

Aside from being extremely popular as an employee benefit, telecommuting has many benefits for employers, such as lower office overhead, lower absenteeism, higher productivity, increased employee retention and higher morale. Still, just as with any aspect of business, employers should approach telecommuting properly and plan its implementation properly.

B. Insurance Concerns

When an employer puts fax machines, computer terminals and other such equipment into an employee's home, it is a good idea to not only make sure that

the company's insurance policies cover this equipment, but these policies should also cover the employee's home, personal property and any personal injuries caused by this equipment, such as a fire, shocking a child, etc. These are real liabilities employers may incur, so it is best to deal with them proactively.

C. Workers' Compensation Claims

Employers should also be prepared to deal with accidents that occur at home with telecommuters while they are acting in the course of their employment. When a telecommuter trips and falls at home, that is the same as tripping and falling at the office. However, the employer has less control of the safety of the workplace in the case of a telecommuter.

In Ae Clevite, Inc. v. Labor Commission and Charles Tjas, No. 990218-CA (Ct. of Appeals of Utah, Feb. 10, 2000), Charles Tjas worked for Ae Clevite, Inc. as its district sales manager for Utah and several surrounding states. Since Ae Clevite did not have an office in Salt Lake City, Tjas worked out of his home. Company-provided supplies, correspondence and other materials were routinely delivered to Tjas' home.

In January of 1997, Tjas went out to salt and shovel his driveway since he was expecting the mailman to make a delivery later that day. While performing these tasks, Tjas fell in his driveway, which left him a quadriplegic.

Tjas claimed that this injury should be covered by Workers' Compensation since his work location was his home and clearing his driveway of snow and ice was part of his job. As a result, Tjas contended that he was injured "in the course of employment."

Tjas' employer disagreed. The employer claimed that it never requested, directed, encouraged or reasonably expected Tjas to salt his driveway as part of his job.

The court sided with Mr. Tjas. The court reasoned that an accident occurs "in the course" of an employee's employment if it occurs while the employee is rendering services incidental to those he was hired to perform "in the place he was authorized to render such service."

The court went on to reason that activities are incidental to an employee's employment whenever these activities advance the employer's interest either directly or indirectly. In this case, Tjas was cleaning his driveway to make it safe for the delivery of company materials he may be receiving in the mail. Receiving information at his home related to his employment was an integral part of Tjas' job.

Tjas Workers' Compensation claim was therefore allowed.

Obviously, this aspect of the law poses a great opportunity for Workers' Compensation fraud. Therefore, only employees whom the employer feels are trustworthy should be afforded the privilege of telecommuting.

In order to deal with this problem, employers may require an inspection of the telecommuter's "work area" in order to ensure that it is suitable for use as a work space.

Further, in ordinary situations, travel between home and work falls under Workers' Compensation's "coming and going" rule. The "coming and going" rule states that accidents that occur between home and work are not covered by Workers' Compensation.

However, when an employee works at home in the morning and then travels to the office later in the day, this may be classified as travel from worksite to worksite. Consequently, accidents that telecommuters incur on their way to the office may in fact be covered by Workers' Compensation.

D. Wage and Hour Issues

If the telecommuter is a salaried exempt employee, only a few wage and hour issues exist, such as whether the employee will be permitted to perform only a few duties from home, then be paid for the entire day.

However, if the employee is non-exempt, then several considerations should be addressed. The following questions should be addressed with non-exempt employees:

1. How will they record their hours?

2. Will the employee be assigned "regular work hours"?

3. Will the employee be required to come into the office? If so, when? Will the employee be paid for traveling into the office or will it be agreed that such travel is a normal commute?

4. Must the employee be accessible by telephone? If so, when?

If the work performed at home by the employee can be classified as a production of goods, then allowing an employee to telecommute may be even further regulated by the Fair Labor Standards Act. Such regulation requires additional record keeping by the employer. Additionally, depending on the industry, the employer may need to obtain a certificate to perform this home-based work.

Further, employers should research the state laws governing work performed at home. Such states as California, New York, Connecticut and Hawaii all have laws that address working at home. For instance, Illinois law requires that an employee's home work area have the proper ventilation and even specifies the

proper cubic feet of airspace an employee must have in his/her work area. Other laws require specific types of record keeping.

Therefore, employers should be diligent and research these laws before implementing a telecommuting program.

E. ADA and Reasonable Accommodation

In EEOC v. Ford Motor Co., No. 12-2484 (Apr. 22, 2014), Jane Harris was employed by Ford Motor Company as a resale buyer. Her job required her to serve as an intermediary between steel suppliers and the companies that use steel to produce parts for Ford to ensure there were no gaps in the steel supply.

Harris suffered from IBS, an illness that causes fecal incontinence. On particularly bad days, she was unable to drive to work or stand up from her desk without soiling herself. She used intermittent Family and Medical Leave Act (FMLA) leave when her symptoms were severe. Eventually, she asked to telecommute on an as-needed basis as an accommodation for her disability.

According to Ford, "The essence of the job was problem-solving, which required that a [resale] buyer be available to interact with members of the resale team, suppliers, and others in the Ford system when problems arose." Ford determined that the position required face-to-face meetings and that e-mail and teleconferencing were poor substitutes for in-person problem solving.

Although Ford had a policy that authorized employees to telecommute up to four days per week, the company initially denied Harris' request to telecommute on an as-needed basis.

According to Ford, "The essence of the job was problem-solving, which required that a [resale] buyer be available to interact with members of the resale team, suppliers, and others in the Ford system when problems arose." Ford determined that the position required face-to-face meetings and that e-mail and teleconferencing were poor substitutes for in-person problem solving.

Ford offered Harris two alternative accommodations:

- She could move her office closer to a restroom, or
- The company could transfer her to a position that was more suitable for telecommuting.

Harris rejected both proposals.

Harris felt that her supervisor began harassing her because of her absences. She filed a discrimination charge with the Equal Employment Opportunity Commission (EEOC). Shortly after she filed this charge, her supervisor began

having weekly coaching sessions with her. These sessions involved reviewing her performance problems that stemmed from her disability-related absences.

Additionally, in her next performance evaluation, Harris was rated as a "lower achiever," and Ford placed her on a performance enhancement plan (PEP). The PEP was designed to help employees improve their performance by establishing concrete objectives they could easily achieve in 30 days. At the end of the 30-day period, Ford determined that Harris failed to meet any of the objectives and terminated her employment.

After investigating Harris' discrimination charge, the EEOC found probable cause that she was discriminated against because of her disability. It then filed this lawsuit against Ford on her behalf. The EEOC alleged that Ford failed to accommodate Harris' disability under the Americans with Disabilities Act (ADA), asserting that the company should have permitted her to telecommute four days per week.

The agency also alleged that Ford **retaliated against Harris by placing her on a PEP** and **terminating her shortly after she filed her discrimination charge**. The district court granted Ford's motion for summary judgment, finding that Harris was not a "qualified" individual on the basis of her excessive absenteeism.

The EEOC appealed to the 6th Circuit.

In a 2-1 decision, the 6th Circuit reversed the district court's award of summary judgment. The 6th Circuit found that there were significant issues in Ford's failure-to-accommodate and retaliation claims.

In the failure-to-accommodate claim, the 6th Circuit **reversed its past decisions on "telecommuting" as a reasonable accommodation**. The court reasoned that technological advances have now made telecommuting a "viable reasonable accommodation."

The majority stated:

> Technology has advanced in the intervening decades, and [as] an ever- greater number of employers and employees utilize remote work arrangements, attendance at the workplace can no longer be assumed to mean attendance at the employer's physical location. Instead, the law must respond to the advance of technology in the employment context, as it has in other areas of modern life, and recognize that the "workplace" is anywhere that an employee can perform her job duties.

The majority reasoned that telecommuting is no longer reserved for "extraordinary" or "unusual" cases and has become common. Therefore, there was a genuine dispute over whether telecommuting was a reasonable

accommodation for Harris' disability, and a jury would have to resolve the dispute.

As for Harris' retaliation claim, the 6th Circuit found sufficient evidence that the **reasons given for her termination were pretextual and warranted a trial.** According to the court, a reasonable jury could infer that there was a pretextual reason for her termination because **"although many of Harris' performance deficiencies were ongoing problems, they prompted a negative review *only* after [she] filed her EEOC charge."**

The 6th Circuit also determined that one of the goals Ford set for Harris in her PEP was impossible to satisfy, thus setting her up to fail.

However …

On April 10, 2015, the 6th Circuit reheard Ford's appeal *en banc,* which means the entire appeals court heard the case. (EEOC v. Ford Motor Co., No. 12-2484 (2015))

This time, the majority found that Harris' "**regular and predictable on-site attendance**" **was** an essential function of her job.

From that, the court found that requiring Ford to permit Harris to telecommute "as needed" for as much as 80 percent of her work schedule would remove one of the **essential functions** of her job.

In fact, and of most significant interest to other employers, the court noted that:

> "**most jobs would be fundamentally altered if regular and predictable on-site attendance [were] removed" from the essential functions.**

Although the EEOC had argued that technological advances have made telecommuting a more viable option for reasonable accommodations, the court noted the agency had still been unable to demonstrate that said technology would enable the essential functions of Harris' particular job to be performed remotely. The court also pointed out that Harris had been allowed to telecommute on a **trial basis** but that **her performance had continued to suffer and she had been unable to perform several of the primary functions of her job.**

WHAT DOES THIS MEAN TO HUMAN RESOURCES?

For quite some time now, the EEOC has held that it considers telecommuting to be a reasonable accommodation worthy of consideration. The 6th Circuit is just the latest in a long line of courts that have adopted telecommuting as a ***possible*** reasonable accommodation.

However, this rehearing of the Harris case sets a very **strict requirement** for allowing telecommuting as a reasonable accommodation. However, the precedent that "**most jobs would be fundamentally altered**" if the employee couldn't deliver some measure of regular, predictable on-site attendance may be persuasive to other courts and beneficial to employers.

While it is true that the constant stream of technological advances has cleared the way for telecommuting as a reasonable accommodation for many workers and many job functions, that still doesn't mean all positions can or should be performed remotely.

This case highlights the importance of complete and accurate job descriptions that clearly represent the essential functions of a job. If an employee's job can't be accomplished outside the physical work location or core business hours, that fact should be clearly reflected in the job description and employment practices and consistently applied to all workers in comparable roles.

F. Isolating The Employee

One of the disadvantages of telecommuting is that employees may very easily become isolated from the work environment and what is going on in the company. Steps should be taken to prevent this from happening.

First, companies may want to consider assigning their telecommuters an e-mail address at their homes. The telecommuters may then be included on all of the routing messages that are sent to employees via e-mail. This electronic link also makes it easier for telecommuting employees to communicate with workplace employees, and vice versa.

Companies may also want to schedule weekly or bi-weekly meetings for telecommuting employees to attend so they can be kept current on what is going on in the company. Telephone conferences could also be scheduled to keep telecommuters current.

G. Policy Guidelines

In order to help ensure the success of a telecommuting program, the company may establish a few general guidelines. Such guidelines may include:

1. Include the employee's home and the equipment placed in the employee's home on the company's insurance policy. Such coverage would include protection against fire, injuries to others caused by any equipment placed in the home and for the equipment itself, depending on the value of the equipment.

2. Have the employee sign an "Inventory Control Sheet." (Sample form is included at the end of this section.) This sheet will list all of the equipment assigned to the employee. The employee will then

acknowledge on this form what equipment the company has placed into his/her home and that it is the property of the company. The employee should also agree to return or surrender the equipment upon request. The employee should also acknowledge that he/she is responsible for this equipment and must reimburse the company for its current market value, or agree to have the value of the equipment deducted from his/her wages, if it becomes damaged beyond normal wear and tear, as determined by the company's management.

3. Guidelines should be established to select only responsible and reliable employees to participate in this program. Examples of such guidelines may include:

   a) Telecommuters must have good work records, which may be demonstrated either through references, internal and/or external, performance appraisals, and the documentation found in the work itself. Of course, these employees should not have any warnings in their records.

   b) Newly hired telecommuters should be required to spend a certain period of time in the office when they start with the company in order to learn who everyone is, the company's culture, the procedures of the areas they will be supporting, etc. Of course, when new employees are hired as telecommuters, interview and reference questions should be geared to determine if these individuals are responsible enough to make good telecommuters.

   c) Constant contact should be maintained with the telecommuters. Communication by way of e-mail and telephone should occur frequently. Meetings should be scheduled regularly, both via telephone and face-to-face in the office. Simply because an employee is a telecommuter does not mean the company never sees them in person.

   d) Equipment should be installed that these employees will need to do their jobs. This obviously includes such items as a computer, a desk, a chair and so on. However, this may also include communications equipment, such as e-mail, a telephone, a fax machine, and so on.

   e) Telecommuters' e-mail should be added to the automatic routing list of the company. Other employees should also have easy access to the telecommuters' e-mail address, and vice versa.

   f) Telecommuters should be given clear directives, which may include deadlines, progress reports assignments (i.e., weekly), etc.

g) If the telecommuters are non-exempt employees, specific guidelines should be established as to how they should complete their timecards.

h) Educate the employee as to how to maintain a true work environment inside their home. Work areas should be regarded strictly as work areas. Hours of work should be established, just as if these telecommuters were coming to the office. The office should be maintained in a safe manner and free of clutter.

i) The laws of the state where the telecommuter resides should be reviewed for any special requirements the employer must meet.

j) The employee's work area should be inspected by the company in order to ensure that it is a safe and proper environment

k) Telecommuters should be instructed to report all accidents they have and injuries they sustain while on the job as soon as possible. It may also be a good idea to install an emergency buzzer for the employee to hit if they become seriously ill or injured.

4. And finally, managers must be trained in how to supervise telecommuters. Special emphasis must be placed on the productivity and performance of the telecommuter, how well the telecommuter is managing their project (Are deadlines being met? Minimal errors? etc.), and whether the telecommuter is keeping in touch with the office (and vice versa).

XIII. THREAT OF SABOTAGE…INSIDE OR OUT

A. A Very Real Threat

Unfortunately, as the use of computer systems in business has increased, so has corporate espionage. Employees have been known to download corporate files onto computer discs and sell them to competitors…or possibly go into business for themselves.

Further, computer deviants are everywhere. Almost everyday, businesses hear of new viruses being launched that will completely disrupt one's computer systems. Even worse, hackers are constantly trying to break into employers' computer systems and steal information. Employers must safeguard against such attacks.

B. Protecting Employer Information From Unauthorized Distribution

Today's PCs can store a tremendous amount of information. Likewise, not only can the standard floppy disc stores 1.44 mbs of information, but such technology as zip drives, which can hold 100 mbs of data, and Super Discs, which can hold 120 mbs of data, make entire harddrives portable. Further, e-mail attachments can now transfer volumes of information to another location very easily.

The challenge for employers to consider when assigning these tools to employees is whether the employees can use this equipment to transport thousands of pages of data outside of the workplace. This fact leaves employers extremely vulnerable as it tries to control its sensitive data and work products.

It is often assumed that everyone who has a PC should be given external e-mail access. It is also often assumed that everyone who has a PC should be given a floppy disc. Further, more and more employers are also issuing Super Discs and zip drives to their employees. While many employees need such equipment to function most efficiently, employers should also consider the downsides of issuing such technology to employees: the employer's data has now become very mobile.

To help prevent the loss of data and its unauthorized distribution, employers' policies should prohibit employees from downloading sensitive materials onto these discs or e-mailing such information outside of the company.

C. Dial-In Access

One positive aspect of computer technology is that employees can now "dial-in" into the office computer system and work on their projects, check their e-mail and function just as if they were at work. However, this technology also affords "hackers" a greater opportunity to "break" into the company's computer systems and either steal information or sabotage it.

If a hacker did gain access to a company's confidential records, such as payroll, home phone numbers, addresses, medical records or company financials, the result could be disastrous.

If a business has the capability to allow its employees to "dial into" the company's computer systems from outside, special protections should be put into place. Protection grids, sometimes referred to as "firewalls," should be constructed to protect the information in the company's systems. Further, employees should have to enter through multiple security walls in order to reduce the chance that a hacker will be able to enter.

D. Scanning For Viruses

No one should be allowed to bring any software or computer discs into the worksite without having screened them for potential viruses. Employers should also require their employees to use these screening mechanisms before downloading information from the Internet. (Viruses often hide in "exe" files and go active once they are downloaded.)

Virus scanning systems can be installed into PC's that will automatically scan discs before the system will allowed them to be opened. Such systems will also automatically scan e-mails to determine if they contain any known viruses before

the e-mail can be opened. It is advisable that all corporate PC's have such software installed.

E. Terminated Employees

And finally, whenever an employee is terminated, the employee should never be allowed to log back into the company's computer-systems. All too often, employees use this opportunity to delete files or possibly even load a virus.

Employees do not have to be terribly sophisticated to enter a virus into the company's computer systems. The virus may be loaded on a disc or zip and loaded within seconds. That is all it takes. The virus may then go live immediately, in a few days or in a few weeks. It may then be impossible to prove that the terminated employee was the one who sabotaged the company.

XIV. ELECTRONIC SIGNATURES IN GLOBAL AND NATIONAL COMMERCE ACT ("E-SIGN" LAW)

A. In General

On June 30, 2000, President Clinton signed the "Electronic Signatures in Global and National Commerce Act", or the "E-Sign Law." Under this law, which took effect on October 1, 2000, contracts that are signed electronically are to be given the same weight under the law as those signed with an actual handwritten signature.

Furthermore, many states, such as Ohio, Indiana, and Kentucky have passed the Uniform Electronic Transactions Act, or "UETA", which is basically the equivalent of the E-Sign Law at the state level.

As a result of these laws, the ability to conduct business on-line and endorse enforceable contracts has just been greatly increased.

B. "Electronic Signature" Defined

An electronic signature is defined under federal law as being:

> "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."

Under this definition, virtually any electronic communication that declares the sender's desire to be bound is sufficient to constitute an electronic signature. The law does not require that any particular type of technology be used to bind the sender, such as encryption. The security measures used by the sender are the prerogative of the sender.

Of course, just as with traditional handwritten signatures, the authentic nature of an electronic signature may be challenged. Just as with traditional handwritten signatures, the possibility of fraud and forgery exists. Therefore, to help reduce the probability of such problems arising, users should understand the difference between an electronic signature and a digital signature.

C. Electronic Signature v. Digital Signature

The difference between an electronic signature and a digital signature is purely technological. All that is needed for an electronic signature is the intent of the sender to be bound, which can be quite risky from a security standpoint.

However, a digital signature requires the use of some type of encryption program to verify the sender's authorization. Clearly, the use of digital signatures is preferable.

D. Exceptions To The E-Sign Law

The E-Sign law does not allow all types of documents to be endorsed electronically or digitally. For instance, such documents as wills, trusts, adoptions, divorces, court orders, cancellation of utility service, cancellation health insurance or life insurance, automobile recall notices and notices regarding the shipment of hazardous materials are excluded from coverage.

Further, transactions involving consumers are also excluded unless:

1. The consumer has affirmatively consented to the use of an electronic signature,

2. The consumer is first provided with a notice of his ability to receive a written record of the document and

3. The consumer has the appropriate hardware and software to read the electronic record.

INVENTORY/FINANCIAL RESPONSIBILITY AGREEMENT

I, _____ (Print Name), an employee of _____, (from hereon referred to as the "Company.") have received the equipment listed below to use only in the performance of my duties with _____ (Company Name).

The following equipment has been assigned to me under this Agreement:

	Name of Item	Serial Number	Date Assigned	Date Returned
1.	_____	_____	_____	_____
2.	_____	_____	_____	_____
3.	_____	_____	_____	_____
4.	_____	_____	_____	_____
5.	_____	_____	_____	_____
6.	_____	_____	_____	_____

I understand and agree that this equipment is the sole property of the Company and it is to be maintained solely for the exclusive use of the furtherance of the Company's business. I understand that the Company may require me to return this equipment for updating, maintenance or for any other reason as deemed appropriate by Company management.

I further understand and agree that it is my responsibility to care for this equipment in a manner that is both professional and ethical while it is assigned to me. I understand and agree to accept full financial responsibility for any of the above-referenced equipment assigned to me, which includes any damage to these items above beyond normal wear and tear, as determined by Company management. I therefore give the Company permission to withhold from my wages or other monies owed to me from the Company to pay for these items should they become damaged beyond normal wear and tear. Further, I therefore give the Company permission to withhold from my wages or other monies owed to me by the Company to pay for the recovery of these items should I fail to return them to the Company's location upon demand. I understand and agree that the amount deducted to pay for these items will be their fair market value, as determined by the Company.

I also understand and agree that I am permitted to use these items only for as long as the Company allows me to and only for as long as I am employed by the Company. Upon demand by the Company and/or whenever my employment ends with the Company. In understand and agree that should I fail to return these items upon demand or when I leave the Company's employment, keeping these items will be considered theft and I will be subject to all applicable civil and criminal penalties.

Should I breach or threaten to breach any section of this Agreement, I agree that I will indemnify the

Company against any and all loss, damage, or expenses, including, to pay for any attorneys' fees, administrative costs and any other costs deemed to be reasonable by the Company that it incurs in order to enforce any section of this Agreement or to correct whatever damages caused by this breach.

The Company's remedies under this Section are not exclusive, and shall not prejudice or prohibit any other rights or remedies under this Agreement or otherwise.

Nothing in this Agreement alters the Employee's employment relationship with the Company. Employment with the Company is still employment at-will. Employment and compensation may be terminated or changed with or without cause and with or without notice at any time by the employee or the Company. Nothing in any document or any statement by any Company representative shall limit the right to terminate or change this employment at-will. No representative, manager, supervisor, or other employee of the Company has any authority to enter into an agreement for employment for any specified period of time or to make any agreement for employment other than at-will. The only Company official who is authorized to make any such agreement is the president of the Company and then only in writing.

_____ _____

SIGNATURE DATE

NOTE: Even though you cannot keep an employee's entire paycheck for not returning items to you, this clause might convince most employees to return such items to you. However, you can ONLY have an employee agree to

XV. COMPANY EQUIPMENT

A. Company and Personal Property, Equipment, Tools and Uniforms

Equipment and vehicles essential in accomplishing job duties are expensive and may be difficult to replace. When using such equipment, employees are expected to exercise care, perform required maintenance, and follow all operating instructions, safety standards, and guidelines.

Employees must notify their supervisor if any equipment, machines, tools, or vehicles appear to be damaged, defective, or in need of repair. Prompt reporting of damages, defects, and the need for repairs could prevent deterioration of equipment and possible injury to employees or others. The supervisor can answer any questions about an employee's responsibility for maintenance and care of equipment or vehicles used on the job.

The improper, careless, negligent, destructive, or unsafe use or operation of equipment or vehicles, as well as excessive or avoidable traffic and parking violations, can result in disciplinary action, up to and including termination of employment.

Employees must return all the Company property immediately upon request or upon termination of employment. Where permitted by applicable laws, the Company may withhold from the employee's check or final paycheck the cost of any items that are not returned when required. The Company may also take all action deemed appropriate to recover or protect its property.

See "Inventory Control Agreement" earlier in these materials.

Equipment or supplies are not to be removed from the employee's work premises without proper authorization.

The Company is not responsible for loss or damage to the employee's personal property. Valuable personal items such as purses and all other valuables should not be left unattended in areas where theft might occur.

B. Data Systems Policy

This Company is committed to providing an environment that helps employees become more efficient and effective through the use of computers and electronic equipment. While such tools may prove to be very useful to employees as they perform their duties, it is important that employees understand that this equipment is the property of the Company. As a result, this technology is to be used primarily for business purposes.

However, nothing is this policy is intended to discourage or prevent employees

from discussing or engaging in activities related to their wages, terms and conditions of employment through these systems.

(According to the NLRB, employers can no longer prohibit their employees from using their email system to discuss unionization, or the wages, terms or conditions of employment, UNLESS it can demonstrate that allowing employees to use your email system for unionization purposes would "interfere with the email system's efficient functioning." This is an almost impossible standard to meet. Of course, the NLRA applies to both union and non-union employers. ALL employees have the right to talk about the "wages, terms and conditions of employees" … union or not.)

Further, all data sent, received or created on the Company's equipment is the property of the Company. The Company may therefore do whatever it wants with this information, which includes reviewing and distributing this data to whomever it wishes. Employees should never consider what they create on the Company's equipment, which includes e-mails, voicemails, and documents retained or viewed on their computers to be private, regardless of the content of the message or the identity of the sender and/or receiver.

The Company may also monitor any employee communications as it deems appropriate, such as in the case of business necessity, for reasons related to safety, or under the order of subpoena, to mention a few, which may include telephone conversations, e-mails, etc. The Company may grant permission to others to do the same without first notifying the employee.

The previous two paragraphs are very important to include in your handbook. Some jurisdictions have ruled that if employees are not put on notice that their communications are not private, then a reasonable expectation of privacy might exist under the law. Therefore, the employer might be violating the law by reading an employee's emails, looking into an employee's computer, and so on. This notice solves that issue.

Every employee is responsible for the secure and responsible use of the Company's data and data systems. Failure to follow the dictates of this policy may subject the employee to the Company's disciplinary process. The following indicates how employees should conduct themselves regarding the Company's data and data systems.

1. Employee Data Electronic Messages Are Never Deleted

In today's legal environment, the courts require employers to monitor and oversee all of its data control systems for illegal and harassing activity. In order to meet these obligations, the Company will review employee e-mail messages, voice mail messages and Internet trails on a regular basis, including employee mailboxes and recycle bins. Therefore, any messages

created, received, stored or sent on the Company's equipment belongs to the Company and may be reviewed and distributed as it desires.

Employees must understand that everything they write on their computers, such as memos, letters, e-mails, and everything they receive on their computers, can never really be entirely deleted. The same is also true of many voicemail systems. Employees should therefore take great care in what they write or say into any of the Company's electronic communications systems.

Further, whatever websites employees visit on the Internet are permanently recorded in their hard drives and possibly on the Company's main server.

2. Access To Data Systems and Passwords

Computer system passwords are confidential and should not be shared with anyone. Employees are not permitted to bypass or attempt to override the established security systems.

Additionally, employees are not to use passwords issued to another employee. If an employee believes a password has been misused, the employee is to report it immediately to their supervisor.

Employees are also not to share their security passwords for access into any of the Company's various equipment or systems. Employees who divulge their security passwords are responsible for the consequences of such disclosure.

3. Data Confidentiality

Employees should not disclose any of the confidential business data residing on the Company's systems to anyone unless they are certain the person has the right and a need to receive it. The Company's confidential business data should only be disclosed to non-company personnel if the employee has received written permission from the appropriate department manager(s). In addition, employees may not remove any Company confidential business data from the Company's systems in the form of tapes, diskettes, printed reports, or any other media from the Company's premises unless it is part of their normal job duties.

Again, nothing in this handbook is intended to discourage or prevent employees from discussing or engaging in activities related to the wages, terms or conditions of their employment.

4. Equipment

All of the communication equipment and systems of the Company, electronic, wire or otherwise, which include e-mail and voice mail systems, are the sole property of the Company and are to be used primarily for business reasons only. Any abuse of Company equipment may result in disciplinary action. However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment through these systems.

The messages contained in this equipment and systems are Company records. The Company reserves the right to access and disclose the contents of an employee's e-mail and/or voice mail messages without permission of the employee. This equipment and these systems may not be used to send messages that are vulgar, obscene, threatening, intimidating, harassing, maliciously dishonest, unlawful or illegally discriminatory.

5. Proper Use of Data Systems

Employees are prohibited from using any of the Company's equipment or systems for any vulgar, obscene, threatening, intimidating, harassing, maliciously dishonest, unlawful or illegally discriminatory purpose, for personal gain or to solicit money for religious or political organizations.

Employees should also understand that many websites now have "spiders" in them that attach to their electronic message and follow the employee back to his/her own e-mail address. Consequently, not only does the site Webmaster know the employee was there and what the employee looked at, but the Webmaster may then begin sending unwanted e-mails and solicitations to the employee's e-mail address. Employees should therefore observe this policy and only visit business related websites on the Internet.

Employees are prohibited from attempting to interfere with or disrupt any network users, services or equipment. Examples of such prohibited conduct include forging, deleting, examining, copying, or modifying files and/or data belonging to other users without their prior consent.

However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment through these systems.

6. E-Mail

The rule of thumb when it comes to e-mail and voice mail is that employees should not say or write anything that they would not want someone other than the intended receiver to hear or read. Remember that even when an e-mail or voice mail message has been deleted from a location, it is still possible to retrieve and read that message.

Employees must understand that any confidential messages they send outside of the Company (i.e., over the Internet) are not secured unless they are encrypted.

Any use of encryption devices for sending messages either inside or outside the Company requires prior management approval.

If an employee needs to send confidential information over the Internet, the employee must inquire as to whether he/she should encrypt the message. If an employee suspects that a message sent internally should also be encrypted, he/she should check with his/her supervisor.

7. Telephone Use

The Company's telephone system may be used for personal matters, but not to excess, as determined by Company management. Under no circumstance should an employee make or charge a long-distance call unless it is work-related and approved by the employee's supervisor.

8. Internet Use

The Company provides access to the vast information resources of the Internet to help employees to do their jobs faster and more efficiently, to be well informed and to communicate with others on matters related to the Company's operations. The equipment used to provide that access represents a considerable commitment of the Company's resources for telecommunications, networking, software, storage, etc. This policy is designed to help everyone understand the Company's expectations for using those resources wisely.

9. Trade Secrets and Confidential Information

Employees are to never send or transmit any of the Company's trade secrets or confidential business data over the Internet without having first encrypted the message. (Of course, no such information should ever be released in any format without the permission of management)

Likewise, employees are to never post Company confidential business

data on the Internet without first obtaining prior approval from Company management. Violations of this policy may result in substantial civil and/or criminal penalties under the Economic Espionage Act of 1996. However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment through these systems.

10. Copyrighted Material

Much of the information found on the Internet is copyrighted material. Such material enjoys all of the protections of federal copyright law as traditional hardcopy materials. Contrary to popular belief, material could be copyrighted without the use of a © symbol.

Therefore, employees should always make certain that it is legal to download material from the Internet before doing so. When in doubt, it is always best to contact the Webmaster and get permission to download material before doing so.

However, information from government websites is considered public material and may be downloaded without any such fears.

However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment through these systems.

11. Software

a) General Policy

It is the policy of the Company to respect all computer software copyrights and to adhere to the terms of all software licenses to which the Company is a party. The Company Senior Network Administrator is charged with the responsibility for enforcing these guidelines.

The Company users may not duplicate any licensed software or related documentation for use either on the Company's premises or elsewhere unless the Company is expressly authorized to do so by agreement with the licenser. Unauthorized duplication of software may subject users and/or the Company to both civil and criminal penalties under the United States Copyright Act.

b) Licensed Software

The Company may license software from many different vendors for use on its data systems. No computer software program may be used on the Company's computers which:

- ❖ Is not licensed to the Company,
- ❖ Is not an original, vendor supplied version of the licensed software, or
- ❖ Was not created by an employee of the Company.

Users may not give software to any outsiders including clients, contractors, customers, and others. The Company's users may use software on local area networks or on multiple machines only in accordance with applicable license agreements.

The software used on the Company's systems must not be used separately on a stand-alone home or office workstation unless a separate license has been purchased for this purpose.

c) Purchasing Software

All software acquired by the Company must be purchased through the IT Department, purchasing, or other appropriate department. Software may not be purchased through petty cash, travel or entertainment budgets. Software acquisition channels are restricted to ensure that the Company has a complete record of all software that has been purchased for the Company's computers and can register, support, and upgrade such software accordingly.

To purchase software, users must obtain the approval of their supervisor or area manager and then follow the same procedures the Company uses for the acquisition of other company assets.

When acquiring computer hardware, software and training must be budgeted at the same time. When purchasing software for existing computers, such purchases will be charged to the department's budget for information technology or an appropriate budget set aside for tracking software purchases.

d) Registering Software With The Company

When software is delivered, it must first be delivered to the Senior Network Administrator so he/she can complete registration and inventory requirements. The Senior Network Administrator is responsible for completing the registration card and returning it to the software publisher. Software must be registered in the name of the Company, job title or department in which it will be used.

Due to personnel turnover, software will **never** be registered in the name of the individual user. The Senior Network Administrator maintains a register of all the Company's software and will keep a library of software licenses.

The register may contain such information as:

- ❖ The title and publisher of the software;
- ❖ The software license;
- ❖ The date and source of software acquisition;
- ❖ The location of each installation, as well as the serial number of the hardware on which each copy of the software is installed;
- ❖ The name of the authorized user or users;
- ❖ The existence and location of back-up copies and;
- ❖ The software product's serial number.

e) Installation of Software

After the registration requirements above have been met, _____ will install the software. Manuals, tutorials, and other user materials will be provided to the user. A copy of the applicable license agreement will be provided to the user. Once installed on the hard drive, the original diskettes will be kept in a safe storage area maintained by _____.

f) Shareware

"Shareware" software is copyrighted software that is distributed freely through bulletin boards and online services. It is the policy of the Company to pay shareware authors the fee they specify for use of their products. Registration of shareware products will be handled the same way as for commercial software products.

g) Home Computers

The Company's computers are Company-owned assets and must be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on the Company's machines. Users are not permitted to bring software from home and load it onto the Company's computers. Generally, Company-owned software cannot be taken home and loaded on a user's home computer if it also resides on the Company's computer. If a user is to use software at home, the Company will purchase a separate package and record it as a Company-owned asset in the software register.

However, some software companies provide in their license agreements that home use is permitted under certain circumstances. If a user needs to use software at home, he/she should consult with the Senior Network Administrator to determine if appropriate licenses allow for home use.

h) Penalties and Reprimands for Software and Copyright Violations

According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as $100,000 per title infringed, and criminal penalties, including fines of as much as $250,000 per title infringed and imprisonment of up to five years. Company users who make, acquire, or use unauthorized copies of software will be disciplined as appropriate under the circumstance.

Such discipline may include termination of employment. The Company does not condone the illegal duplication of software and will not tolerate it.

12. Virus Watch

Employees are to never load information into the Company's computers, whether from a disc or from the Internet, without having the data first scanned for viruses.

Employees are also to never open e-mail messages from anyone they do not know. If unknown e-mails are received, employees should contact the Company's data systems officer.

13. Network Connectivity and Integrity

No hardware or software may be added to the Company's network without the prior approval of the Company.

14. Reporting Problems

If an employee suspects any computer abnormalities or problems, such as a security problem or virus-related problem with regard to any data or information, the employee is to report the problem to his/her supervisor immediately.

15. Reservation of Rights for the Company Only

Employees should not interpret the rights the Company has reserved for itself in being able to intercept, retrieve and/or monitor employee communications as also granting them permission to intercept, retrieve and/or monitor the messages of their fellow employees.

Employees should also not interpret these rights reserved by the employer as constituting a waiver of their duty to keep confidential business data secured, which may include such items as Company trade secrets, corporate financial information, copyrighted materials and other confidential materials or information of the Company.

However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment through these systems.

C. Personal Mail

Employees are not permitted to use Company stationary, stamps, postage meters or other Company supplies for their personal mail. Employees should have all of their personal correspondence sent to their home address, unless they have permission from their supervisor.

XVI. SOCIAL NETWORKING

Although the Company respects the privacy and personal time of its employees, the Company's legal obligations require it to adopt certain guidelines for its employees' activities both inside and outside of workplace that could potentially affect the Company's work environment and interests.

Online social media enables individuals to share their insights, express their opinions and share information all over the world. Unfortunately, every online social tool and medium has both proper and improper uses, each of which has a potential impact on the Company and its work environment, regardless of whether these communications occur at work or on the employees' own time.

In short, employees must understand that the same principles and guidelines that apply to their activities in general also apply to their online activities. This includes all forms of social media, including, but not limited to, online publishing and discussion, such as blogs, wikis, file-sharing, user-generated video and audio, and social networks, such as LinkedIn, My Space, Facebook, Twitter, YouTube and Flickr, to mention a few.

Therefore, in order to honor its legal and business obligations, the following is the company's social media and networking policy. However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment. Should this policy fail to address a certain situation, employees need to consult with their manager, supervisor or human resources if they are uncertain how to proceed.

1. Employees are not to create a blog or an online group related to the Company that appears to be offering the Company's positon on various issues, not including blogs or discussions involving wages, benefits, or other terms and conditions of employment, or any other protected activity.

2. Employees are not to knowingly make any maliciously false representations about their credentials or their work.

3. Employees are not to use the Company's (or any of its affiliated entities) logos, marks or other protected information or property for any business/commercial venture without the Company's express written authorization.

4. Employees are to respect the copyright, trademark and similar laws and use such protected information in compliance with applicable legal standards.

5. Employees are not to comment on any Company confidential business data, trade secrets or proprietary information, such as the Company's business, corporate financial, marketing strategies, clients and vendors, not including comments involving their wages, benefits, or other terms and conditions of employment, or

protected concerted activity, without the advance written approval of their supervisor or the Human Resource Department.

6. Employees are to not make negative comments about customers or vendors in any social media.

7. Using social media on Company equipment during working time is permitted if it is being used for legitimate, preapproved Company business.

8. Employees are to be thoughtful in all their communications and dealings with others, including email and social media. Employees are to never harass (as defined by Company policy), threaten, make maliciously false statements regarding fellow professionals, the Company's products or services, employees, clients, competitors or anyone else. In general, it is always wise to remember that what employees say in social media can often be seen by anyone. Accordingly, harassing comments, obscenities or similar conduct that would violate Company policies is not allowed.

9. Company employees are not to access any unauthorized websites on Company equipment on during working time. The reasoning here by the Company is that many websites sites collect profile information for advertising (SPAM) targeted at individuals with particular affiliations and interests. Use of the sites may increase SPAM to the employee's email account.

   In addition, by going to unauthorized websites, an employee's equipment or network may be exposed to spyware and viruses that may damage the employee's operating system, capture data, or otherwise compromise the Company's privacy, as well as affect others with whom the employee communicates.

   However, nothing is this policy is intended to discourage or prevent employees from discussing or engaging in activities related to their wages, terms and conditions of employment.

10. Supervisors and managers are not permitted to make recommendations of employees or former employees without the written permission of human resources.

11. Employees must also use a disclaimer whenever they are expressing their views through social media that might in any way be viewed as relating to the Company, its employees, its vendors or its competitors. A typical disclaimer might read:

> **"The views expressed herein are mine, _____ (Employee's name) alone and do not necessarily reflect the positions, strategies or opinions of _____ (Company name) in any way."**

12. Employees are not to access internet sites at work or on Company equipment that would be considered obscene, harassing, maliciously dishonest, unlawful or illegally discriminatory.

13. Employees are not to use any form of social media that is vulgar, obscene, threatening, intimidating, harassing, maliciously dishonest, unlawful or illegally discriminatory.

The Company does not routinely monitor social networking sites. However, as with other electronic resources, the Company's systems administrators may perform activities necessary to ensure the integrity, functionality and security of the Company's electronic resources.

Violations of this policy may subject employees to discipline under the Company's "Rules and Guidelines" policy, as determined by management.

Notice: Legal Advice Disclaimer

The purpose of these materials is not to act as legal advice but is intended to provide human resource professionals and their managers with a general overview of some of the more important employment and labor laws affecting their departments. The facts of each instance vary to the point that such a brief overview could not possibly be used in place of the advice of legal counsel.

Also, every situation tends to be factually different depending on the circumstances involved, which requires a specific application of the law.

Additionally, employment and labor laws are in a constant state of change by way of either court decisions or the legislature.

Therefore, whenever such issues arise, the advice of an attorney should be sought.

Scott Warrick, JD, MLHR, CEQC, SHRM-SCP

Scott Warrick Human Resource Consulting, Coaching & Training Services

Scott Warrick Employment Law Services

(614) 738-8317 ♣ scott@scottwarrick.com

www.scottwarrick.com & **www.scottwarrickemploymentlaw.com**

Scott Warrick, JD, MLHR, CEQC, SHRM-SCP (www.scottwarrick.com & www.scottwarrickemploymentlaw.com) is both a practicing Employment Law Attorney and Human Resource Professional with almost 40 years of hands-on experience. Scott uses his unique background to help organizations get where they want to go, which includes coaching and training managers and employees in his own unique, practical, entertaining and humorous style.

That is why Scott has been described as "The Comedian Trainer."

Scott Trains Managers & Employees ON-SITE in over 50 topics … all of which can be customized **FOR YOU!**

LET SCOTT DESIGN A PROGRAM FOR YOU!

Scott combines the areas of law and human resources to help organizations in "Solving Employee Problems ***BEFORE*** They Happen." Scott's goal is ***NOT*** to win lawsuits. Instead, Scott's goal is to ***PREVENT THEM*** while improving ***EMPLOYEE MORALE***.

Scott's book, **"Solve Employee Problems Before They Start: *Resolving Conflict in the Real World"*** is #1 for New Releases on Amazon for Conflict Resolution books!

Scott's "**Employment Law Videos**" on the ADA, FMLA, FLSA and Harassment, **"The Human Resource Professional's Complete Guide To Federal Employment And Labor Law" &** Scott's **"Do It Yourself HR Department"** are favorites for anyone wanting to learn Employment Law and run an HR Department.

Scott has been named one of Business First's 20 People To Know In HR, CEO Magazine's 2008 Human Resources "Superstar," a Nationally Certified Emotional Intelligence Instructor and a SHRM National Diversity Conference Presenter in 2003, 2006, 2007, 2008 and 2012.

Scott has also received the Human Resource Association of Central Ohio's Linda Kerns Award for Outstanding Creativity in the Field of HR Management and the Ohio State Human Resource Council's David Prize for Creativity in HR Management.

Scott's academic background and awards include Capital University College of Law (Class Valedictorian (1st out of 233) and Summa Cum Laude), Master of Labor & Human Resources and B.A. in Organizational Communication from The Ohio State University.

For more information on Scott, just go to www.scottwarrick.com & www.scottwarrickemploymentlaw.com.