USE AND ABUSE OF COMPUTERS IN THE WORKPLACE

by
Bob Gregg
Boardman & Clark LLP
One South Pinckney Street, 4th Floor
P. O. Box 927
Madison, WI 53701-0927
Telephone (608) 283-1751
rgregg@boardmanclark.com

Our major form of workplace communication is becoming electronic. People do not have face-to-face, oral conversations. Email is taking over. It is fast, efficient—and dangerous.

Employees just rip off an email with far less thought or editing than a letter. The e-system has replaced the break room for office gossip, harassment, betting, romantic advances and a myriad of other forms of indiscretion or illegality. Yet, when the employer imposes rules or monitoring, employees resist, or sue, over invasion of personal use of "their" computer.

Further, e-discovery and public record requests are eroding the concept of personal use in favor of the "right to know."

E-DISCOVERY IN LITIGATION

E-discovery is a driving force in changing employers' computer policies and practices. It used to be privacy cases and harassment claims which were the impetus in workplace computer practices. Now, electronic discovery concerns are becoming the driving force.

Both federal and most state court systems have adopted electronic discovery rules. The federal rule is Rule 26(a) which requires that employers disclose, at the beginning of litigation and prior to any discovery by plaintiffs, a copy of or a description by category and location of any documents (paper or electronic) that may support its claims or defenses.

BOB GREGG is a partner with Boardman & Clark LLP, Madison, Wisconsin. He has over 30 years of experience in the area of employment relations and has conducted over 3,000 seminars on employment law. Bob litigates employment cases. His main emphasis is to help employers identify and resolve problems before they turn into lawsuits.

Rule 26 also requires one to freeze the electronic system and preserve all Electronically-Stored

Information (ESI) "on notice" that there may be litigation.

ESI includes all "writings, drawings, graphs, charts, photographs, sound recordings, images and other data or data compilations stored in any medium from which information can be obtained." So this is much broader than just the computer. It includes:

- Computer use (intranet and internet)
- Telephones
- Cell phones
- Text messages
- Tapes, CDs, disks
- Locaters/global positioning
- Electronic calendars
- Message systems

Not just the email:

- Reports
- Graphics
- Electronic files
- Charts
- Records
- Contracts
- Drafts and redrafts
- Calendars
- Network access records
- "Documents of any kind"

Duty to Preserve the Records. Read Rule 26 carefully! The rule is about preserving information when on notice that there may be litigation. This does not mean waiting until an official summons and complaint is served upon you. It does not mean when a letter from a government agency is received. Instead, the obligation arises when there is any practical reason to believe future litigation might occur over an issue.

So, the may be can be triggered by any dispute with a vendor or customer that goes beyond a casual disagreement (*i.e.*, letters start to be exchanged over the issue). Any letter from an attorney. Anytime an employee is fired during economic times where the next job is hard to find. Any accident causing personal injury or property damage. These and more events should prompt one to freeze the system and inform all involved to not delete anything without authorization.

Archiving overkill? The general rule is that records should be preserved once there is reason to

know of or "anticipate" a claim might ensue. Some organizations are now taking extra precautions and archiving all emails for the full statute of limitations period for any possible sort of claim. This can be six years, or more in some states. These records may then be destroyed according to an established procedure under the control of the organization's IT professionals (and perhaps HR and risk management, as well).

Failure to preserve is "spoliation. Absence of computer records creates the appearance that one is trying to hide the truth. It can create the presumption that any unproduced record should be viewed as an admission of fault. This created a $2.1 million verdict against the employer in *Arndt v. First Union Bank*, 613 S.E.2d 274 (N.C. Ct. App., 2005).

Employers lose cases and are sanctioned by the courts because they did not preserve email and other ESI. A sanction of $175,000 was imposed for deleting emails after the company should have been on notice of a potential claim (legal counsel, HR and IT failed to effectively communicate). *Zubulake v. UBS Warburg LLC*, 217 FRD 309 (S.D. NY, 2003). The defendant may have to bear the full cost of retrieval and restoration of improperly deleted electronic records. [$236,000 in *Rowe Entertainment v. William Morris Agency*, 205 FRD 421 (S.D. NY, 2002); over $1 million in *Medtronic Sofam or Danek v. Michelson, 229 F.R.D. 550; 2003 U.S. Dist. Lexis 14447 (W.D. Tenn., 2003).*]

Other sanctions for spoliation include:

- You pay to have it restored
- You pay penalties
- The court "suppresses" your evidence
- Presumption of guilt
- **You lose!** Court grants summary judgment due to your bad faith.

Say nothing—type nothing. In an article on "Emergency Response Coordination," the authors, liability defense attorneys, advised that there should be no emails, text messages or e-journal/planner notes made during or immediately following an emergency event. The warning was that all of this is discoverable. In the height of the moment, those involved may tend to put down first impressions and unfounded opinions which later turn out to be inaccurate. However, once in the system, they become "evidence" and possible admissions. The advice was that there should be only official communication on the systems and that reviewed by a coordinator in advance; no personal messages or notes. (Emergency Response Team Coordination, *For the Defense Journal*, Defense Research Institute, July 2006.)

This advice seems almost impossible to follow in today's electronic environment, where everyone has computer access and most communication is electronic. Routine communications between field and central office is usually by email or electronic texting and a "clearance" process would slow this down in an emergency situation.

The article does illustrate the issue of electronic discovery. Plaintiff attorneys now acquire reams of "informal" texting and emails and comb through them for anything which might support a case, no matter how "off the cuff" the message may have been. Once in the email "record," the comment has a *life*, far more significant than oral stray remarks. So, defense attorneys are now advising a process which protects against that problem, but might also impair the effectiveness of responders.

EMPLOYEE USE OR ABUSE

Use

Whose system is it anyway? The computers were purchased using the employer's budget. They are labeled as "property of" the company or public agency.

but

The computer sits on the desk of an individual, who has a personal email address. The Constitution, U.S. Electronic Communications Privacy Act, and other state and local laws can provide expectations of privacy and restrictions on "invading" the employees' usage.

and

In the public sector, the public owns the system. All government property and systems are for the people and ultimately belong to the people. The public has rights to know what is going on in the government system, with their tax dollars. Anyone can make a "public records request."

Public Records/Freedom of Information Requests

Private romance or public scandal? In the case of *In re Petition of the Bd. of Commissions of Arapahoe County* 95 P.3d 593, 2003 Col. App. Lexis 1151 (Col. Ct. App., 2004), the lower court ruled that 101 romantic and sexually explicit email messages between a county clerk and his girlfriend can be released to the public. They were sent or received on the county's computer system during the course of the work week. Therefore, the messages can be "public records" subject to public information requests and public disclosure. [This case was later reversed on appeal and remanded to classify some of the emails as "private." *Denver Publishing v. Bd. of County of Arapahoe*, 121 P.3d (90 Col. S.C., 2005).]

Busted by your Blackberry? In *Consumer Federation of America v. Dept. of Agriculture*, 2006 U.S. App. Lexis 16446 (D.C., 2006), the court ordered all contents of several FDA officials' electronic calendars released pursuant to a Freedom Of Information request, even though the calendars contained personal and family information, as well as work appointments. A public interest group suspected that FDA officials had secret meetings with industry lobbyists resulting in "watering down" regulations on Lysteria (a dangerous food toxin). The staff calendars might

show those meetings. The court ruled the calendars to be public records, including all personal contents.

Bobach v. City of Reno, 932 F. Supp. 1232 (D. Nev., 1996) involved city employees pocket pager messages which were then retrieved and stored in the computer system records. This was under the Fourth Amendment (search and seizure rules), not a public records case, but it shows how all phone messages, pagers and other "personal" devices can get incorporated into the "public record" and became fair game for discovery or disclosure.

The *Consumer Federation of America v. Dept. of Agriculture* case was under the Federal FOI Act, which does not generally apply to state and local government. **Each state's public records laws differ**. For instance, the Florida courts give more protection to employee personal usage. In *State of Florida Times Publishing Co. v. City of Clearwater*, 863 So.2d. 149; 2003 Fla. Lexis 1534 (Fla., 2003), a newspaper requested all personal emails sent or received by two employees for a 12-month period. Using the Florida statutory definition of Public Record, the court held these were not "public records . . . made or received in connection with public business." The court rejected the argument that anything placed or stored in a publicly-funded system is a "record." The court also found that the city's employment policy on rights to access employee computers still did not convert personal messages into "in connection with public business . . . records." A similar decision was made in *Griefs v. Pinal County*, 2 CA-CV-2006-052 (Az. Ct. App., 2006).

So, be careful in mixing your personal life with your office calendar and email. The public may discover your favorite liquor store, restaurants, children's soccer schedules, proctologist appointments, and your bookie's number. The divorce attorneys may find out who is meeting whom on all those "honey, I had to work late" occasions and the email details.

ABUSE—PRIVACY, PIRACY & PANDERING

Laws. A number of federal and a growing number of state laws cover employers obligations in privacy and confidentiality. They obligate employers to keep some information secure, and monitor for illegal use. Yet other laws restrict employers rights to investigate workers use of the system. Among the federal laws are:

U.S. Constitution:

> First Amendment. Rights of expression, public employees may have protection to express themselves on matters of public concern, on the employer's system.
>
> Fourth Amendment. Public employees have more protection than those in the private sector from "unreasonable search and seizure," including use and contents of the electronic system.

18 U.S. Code §1702, Obstruction of Correspondence, Mail Privacy. It is illegal to read another's mail before it is delivered to the addressee. An employer can be liable for intentionally opening and reading employee's personal outgoing mail.

42 U.S. Code §290, Drug and Alcohol Confidentiality, provides for confidentiality of treatment records. These laws prohibit unauthorized release and dissemination of medical and treatment information, including post drug and alcohol testing counseling.

29 U.S. Code §2601 et. seq., the Federal Family Medical Leave Act, as well as the Americans With Disabilities Act, 42 U.S. Code §12101, require medical information to be kept in separate, secured files, with confidentiality. However, both do give the employer a right to access and use certain medical or treatment information when an employee reports a work-related condition, but all medical information must be kept in a separate, secured file.

15 U.S. Code §1681, Fair Credit Reporting Act, requires "accuracy, relevancy and proper utilization of information." This act covers not only standard "credit checks" it also covers employment references and investigations and examinations where outside parties are used as gatherers of the information.

29 U.S. Code §§2001-2009, Polygraph Protection Act, prohibits most private sector employers from requiring mechanical or electronic lie detector tests except under specific circumstances and from using the tests as the sole basis of making employment decisions. The Act also prohibits disclosure of the results beyond those directly involved in the investigation and decision making. This law does not prohibit written "honesty tests" (though some states do) [but also be aware that the ADA may apply if the "honesty test" is found to be "psychological testing"].

5 U.S. Code §522(a), Federal Privacy Act, prohibits federal agencies from disclosing personnel records without the employee's written consent. This can include improper disclosure to staff within the agency itself.

Omnibus Crime Control Act/Electronic Communications Privacy Act, Electronic Communications Storage Act, 18 U.S. Code §2510 *et seq*. (§2701 *et seq*.) prohibits the unauthorized interception and disclosure of wire, electronics or oral communications through the use of electronic, mechanical, or other devices. The federal act gives both civil and criminal penalties for violations. The Act does give employers the right to access email and voicemail in the employer's system, but not a system provided by an outside company. Forbids any person from accessing, without consent, information stored in an electronic communications service (*i.e*., yahoo.com, etc.) and obtaining, altering or blocking access to the information while it is in storage. The employee must consent (actual or implied) to access of their Internet usage.

Health Insurance Portability Accountability Act, 42 U.S.C. 263, Patient Health Care, and Health Insurance Privacy and Confidentiality. HIPPA protects the privacy of medical information. Requires an information management process to assure privacy and prevent improper use. The law provides for civil penalties of $25,000 per year, per violation and criminal liability. [The ADA and FMLA also require "segregation and security" of employees' medical information.]

Family Educational Privacy Act, 20 U.S. Code §1232. Confidentiality of records of participants in educational programs receiving government funds (can include job training programs conducted in the work place), and a variety of state, county, and municipal educational activities not connected to schools.

National Labor Relations Act, 29 U.S. Code §151 *et. seq*. (and many state labor laws). Protects employees concerted activities. Under the NLRA the electronic systems and email are treated the same as verbal discussions and hallway bulletin boards for purposes of distribution and postings of "concerted discussions" and union literature. The employer may commit an unfair labor practice in curtailing this protected speech.

Digital Millennium Copyright Act. 17 U.S. Code §512 limits service providers liability for copyright infringement by users. Includes electronic information under the copyright protection.

Communication Decency Act, 47 U.S. Code §230 insulates the Internet service provider from liability for messages sent on its system.

Computer Fraud and Abuse Act, 18 U.S. Code §1030 prohibits a range of acts, including destruction of records, identity theft, unauthorized entry of systems, altering records, etc.

Transmission of Wagering Information, 18 U.S. Code §1084 prohibits use of wire communications for betting.

Other causes of action exist under state laws or tort action for invasion of privacy, defamation, theft of trade secrets, and negligent supervision (*i.e*., Wis. Stats. 968.31, Interception and Disclosure of Wire, Electronic or Oral Communications).

Harassment/Office Gossip/Discrimination

Most office gossip is now conducted via email. In states or situations in which Workers Compensation preclusion does not nix tort actions, this can lead to defamation and privacy cases. [For more information, request the article *Office Gossip* by Bob Gregg at rgregg@boardmanclark.com.]

Office gossip can result in EEO harassment cases which are not precluded by Worker's Compensation. The gossip far too often focuses on sexuality, sexual orientation, race, religious morality (or lack thereof), and rumors of diseases or psychiatric conditions that other people are alleged to have. These create "hostile environment" cases under Title VII, the ADA and state equal rights laws. *Strauss v. Microsoft*, 814 F. Supp. 1186 (SDNY, 1993) [e-mails about the "spandex queen"].

The loose email comments of supervisors often become evidence in discrimination cases. *Zisumbo v. McCleod USA Telecom Serv., Inc.*, 317 F. Supp. 2d, 334 (D. Utah, 2004) or 154 Fed. Appx. 715; 2005 U.S. App. Lexis 25567 (10th Cir., 2005).

Pornography On The Office Computer

Most harassment and computer use policies prohibit viewing pornography on the workplace computer. A proper policy gives foundation for disciplining or discharging the employee who violates. *United States v. Simons*, 206 F.3d 392 (4th Cir., 2000) [government worker fired after employer intercepted pornography on the office computer].

Duty to report illegal use to police? Third-party action/negligent supervision. In *Doe v. XYC Corp.* 382 N.J. Super. 122 (N.J. S.Ct., 2005), the court found liability because the employer disciplined when it found child pornography on the office computer, but did not report the matter to the police. In the following months, that individual sexually abused his teenage stepdaughter. The stepdaughter later sued the employer. The court ruled that a prompt report of illegal child pornography by the employer to the police would have resulted in an arrest, and either prevented or shortened the abuse of the stepdaughter. Therefore, the employer was liable for the harm she suffered.

Breach of Confidentiality—Invasion of Privacy

The public can get almost everything about government employees in a records request. However, the government employee cannot reveal many things about others without fear of being sued. Governments have sensitive records of both employees and the public.

In the private sector, federal and many state laws protect confidentiality of information. These include: ADA, FMLA, HIPAA and the Immigration Reform and Control Act. Employees who improperly access and reveal this information subject the employer and themselves to liability.

Personal use. Even though one may have job-related access to records, it is not an employee's personal right to access, use or reveal that same information for non-job related reasons.

Curious George gets fired! An employee accessed the confidential, personal salary and investment account information of co-workers in the company computer system. She was fired, and then filed a race and age discrimination case. The plaintiff admitted that she looked into other employees' records because it is "my nature to be curious." The court dismissed the case, finding that the company had a legitimate reason to fire the employee. *Albury v. J.P. Morgan Chase* U.S. Dist. Lexis 5363 (S.D., NY, 2005).

Demand a raise—get fired. A male manager demanded a raise. He believed that women were favored, and presented evidence that his pay was discriminatorily low. The evidence he produced was records of the salaries and fringe benefits of female employees. Rather than getting a raise, the manager was fired for violating confidentiality rules. The court ruled that using confidential information for personal purposes was a serious violation that warranted discharge, regardless of the manager's underlying concern about discrimination. *Cepero-Rivera v. Fagundo* 414 F.3d 124 (1st Cir., 2005).

A Confidentiality Policy Can Provide A Defense

Not all on-the-job activity is job related; employee was outside scope of employment. An employer was successful in getting dismissed from a privacy case by showing that, though the invasion of privacy occurred on the job, it was not job related. A health care lab technician accessed the medical records of her husband's ex-wife and then disclosed the information about the ex to her husband. This resulted in suit of the lab technician personally, and her employer for breaching the laws requiring privacy of medical information, negligent supervision, and failure to maintain proper standards of care. The court ruled that the medical technician was acting *outside the scope of employment* for a purely personal purpose. The technician's actions had no benefit to the employer; the technician had no intent of "serving" the employer when she accessed the records. Thus, the employer could not be held liable. *Korntved, et al. v. Advanced Healthcare, S.C.*, 286 Wis.2d 499; 704 N.W.2d 597 (Wis. Ct. App. Dist. 1, 2005).

Records policy. An important consideration in this case was the company's policy on confidentiality of patient records. The policy expressly forbade looking at records of family members or others out of curiosity or for any other non-job-related reason. The policy was signed by all employees, including the medical tech. This illustrates the growing importance of having some "key" policies signed individually, with a copy in the personnel record.

Theft/Criminal Activity

Employees use the work computer for profit, often by taking business information or trade secrets. Computer crime is a growth industry.

The Computer Fraud and Abuse Act and a variety of state laws protect information from theft, misuses, or piracy.

Identify theft. Personal information from other employees, clients or public records.

* System security is crucial.
* Most identify theft from the workplace is still by paper rather than by computer. (Watch your trash.)

Taking home the e-files. People work at home. The laptop is always with them, with all the work data, and with access to the system. In 2006, the U.S. Veterans Administration reported theft of two laptops containing personal information of millions of vets. Both laptops were being used at home.

Equifax, whose ad is "protect yourself against identity theft" had to give notice in 2006 of a computer laptop stolen during a business trip. It contained names, social security numbers and other personal identity information on 2,500 employees (52% of the entire workforce).

Children of employees use the same laptops, for computer games. Savvy teens can tap into the other information on the computer. They may share it with others. It's fun!

Personal information rules. In the private sector, the Federal Trade Commission has rules on destruction of sensitive employment data. The rules cover employers of one or more employees. All personal data (including phone number, address, Social Security number) must be properly destroyed when the personnel files are purged. Penalties are $2,500 per violation and a former employee may also bring a private suit. (One wonders how this fits with the increasing duty to archive records for the foreseeable statute of limitations years and years.)

Taking and/or destroying company business information. An employer may sue an employee who intentionally deletes company data from a computer. In this case, the employee's job was to go out and identify real estate that the employer might want to acquire. Then, when the employee decided to quit and go to work for himself, he returned the company computer, but first loaded an erasure program onto the computer to delete all of the information he had collected. The court decided that the employer could sue the employee under the federal Computer Fraud and Abuse Act. *International Airport Centers, LLC v. Citrin* 440 F.3d 418 (7th Cir., 2006).

"Proprietary information" restrictions abound. Copyright, patent, finance, trade secrets, and other laws protect much of the information on both the Internet and your own intranet. Employees, especially those who are new to Internet usage, may not be aware of all the implications of their usage. They may download, use and disseminate protected software. They may violate privacy, finance, health, and "dumpster diving" laws by printing out, using and disseminating confidential information without the proper clearances. The companies or individuals whose rights have been violated, whose "property" has been pirated, do not like this, so they often sue for damages. Again, both the individual abuser and the employer who controlled the system may be drawn into the

litigation.

The usage policy should inform employees that receiving, downloading, sending or uploading of proprietary information, trade secrets, and confidential information is prohibited without prior management authorization. The policy should mention that they may be personally liable for violation of the various laws protecting this information, and that the employer can also hold them responsible for any damages and legal fees it expends if their improper activities involve the employer in legal or administrative actions.

Gambling

Some employees, or groups of employees, spend paid time betting over the Internet. Anyone who uses a wire communication or "assists" in betting using the wires may be fined or imprisoned. Each bet is a prosecutable offense. The law also can hold the "facility owners" responsible for allowing the betting.

Is the Internet a "wire connection?" It is if it uses phone lines.

Many state laws prohibit gambling except in licensed premises (*i.e.*, Wis. Stat. §945, *et seq*.). The penalties are much the same as under the federal law.

Negligent Supervision

Employers who know, or reasonably should have known, of illegal activities conducted on their systems, and did not curtail them, may be liable to anyone who is harmed. The employer has the following duties:

- Duty to have policies
- Duty to monitor
- Duty to train supervisors
- Duty to report illegal activity to the police

Union and Other Concerted Activities

The National Labor Relations Act and state labor laws protect employees' rights to engage in "concerted activity." This can include email and electronic postings of union related activity or about common concerns over wages, hours and conditions of employment.

If you allow use for co-workers personal communications on any non work issues, their union related or union organized email may not be prohibited and monitoring must be very careful so as not to be an Unfair Labor Practice or a retaliation claim. *In re EI Du Pont de Nemours Co.*,

311 NLRB 88 (1993). The email system is the same as the bulletin boards for postings, but employers can have a bit more control because the electronic system is not a "limited space" such as a break room bulletin board.

OTHER ISSUES AND TRENDS

Developing Technology

Global positioning and privacy (be careful where you call or e-mail from). Technology now allows employers to track the location of vehicles and employer-provided cell phones and laptops at all times. The boss can tell whether you are at a work site or taking that little personal trip across town. Your claim that you were seeing clients is belied by the record that your vehicle, laptop, and phone were in the vicinity of the horse track all afternoon. That's not all. The locator records are being subpoenaed in divorce cases for evidence of extramarital activity when someone claimed to be working late, etc. Employers should be aware that people carry their phones and laptops in their personal vehicles off the job, and the tracking devices record their evening and weekend whereabouts as well. (We can tell who went to the Republican or Democratic fundraiser, the treatment center, or the red light district.)

The Bush Administration, under the U.S. Patriot Act, was pushing for installation of tracking devices in newly manufactured vehicles. This would allow recording of conversations if the government wishes to activate the "listening option." [See the case of *In re Application of the United States* 349 F.3d, 1132 (9th Cir., 2003).] This effort has been put on hold under the subsequent administration, but is still technologically possible.

Employees may file invasion of privacy cases against employers who track their location without the employee's knowledge. So, employers should give notice and have a written acknowledgment by the employee who is being tracked.

Implants. In 2005, the security firm CityWatcher.com became the first company to implant identity chips in employees. The microchips are injected under the skin in the arm and serve as an ID card and key which are read by the company's security system for access to areas of the premises. VeriChip Corp. has federal approval to market these chips and has now implanted several thousand into employees in various companies. This cutting edge technology makes one wonder how terminations will be handled. [Will the company nurse be present with a scalpel or will this task be delegated to an HR assistant?] On June 1, 2006, Wisconsin became the first state to prohibit the involuntary implanting of microchips, with a $10,000 a day fine.

Laptop while driving. It's not just the cell phone. A surprising number of traffic accidents involve laptop use. A plaintiff's attorney can get the usage records. If they show work-related

use at the time of the accident, then the employer may become a party in the suit. Policies should prohibit unsafe use of the laptops as well as cell phones.

Off Duty - Personal Computers and Websites

Legal use. Generally, an employer cannot discipline for off-the-job legal personal use. However, the more identifiable the employee is and the more impact it has on their work role, especially as a public employee, the more there may be a "compelling interest" for employer action.

Sheriff's deputies have no right to be off-duty porn stars. Two deputies were fired when they were seen engaging in off-duty sex acts on a "private" pay-per-view Internet porn site run by the wife of another deputy (who resigned before he was fired). The court upheld the Department's off-duty conduct rule because their conduct "undermined the public's confidence in police operations." This compelling interest overcame any constitutional off-duty privacy or free expression interest of the officers. *Thaeter and Moran v. Palm Beach County Sheriff's Office* 449 F.3d 1342 (11th Cir., 2006). In *San Diego v. Roe*, 543 U.S. 77 (2004), the Supreme Court upheld discharge of a police officer's off-duty porn activity finding that the off-duty expression was not a protected activity which raised a "matter of public concern."

Police officers or key officials overt off duty racist behavior or websites may be grounds for discharge. "The First Amendment does not require a government employer to sit idly by while its employees insult those they are hired to serve and protect." *Locurto v. Guiliani* 447 F.3d 159 (2nd Cir., 2006). The off duty activities were disruptive of the mission of the police department, to "equally protect all citizens." *Pappas v. Guiliani:* 290 F.3d 143 (2nd Cir., 2003), cert. denied by 539 U.S. 958.

Websites/Blogs/Message Boards/Social Networking

Employees have personal websites, where they may trash their employer. In some situations this may involve use of confidential information from the workplace or the employers records. In others it can be defamatory. Does the employer have the right to discipline? Can the employer invade the personal site to discovery what is there?

There is no expectation of privacy when one posts items on public display. So most blogs or social networking are open to view by one's employer. Nevertheless, there are some protections.

The National Labor Relations Act allows employees to openly critique wages, hours, and terms of their employment. The First Amendment protects public sector employees who raise issues of "public concern" (over one's personal gripes, opinions and displays are generally not protected). Generally, an employer considering discipline for one's off-duty conduct should consider the following factors:

- Does the employee's off-duty conduct have a connection to the workplace?
- Injury to the employer's business or operations;

- Inability to report for work;
- Unsuitability for continued employment;
- Other employee(s) refusal to work with the off-duty offender or danger to other employees

The Federal Trade Commission is also implementing rules which may make the employer liable for an employee's off-duty positive statements about a company's products or services. Over-inflated or "false" claims can be viewed as company *advertising*. The employee may be viewed as an agent of the company.

So, there are valid grounds for providing policies and employee education regarding off-the-job personal and electronic expressions. These policies and training programs should be carefully crafted to balance the issues of employers' legitimate concerns with employees' legal and privacy rights.

A breach of confidentiality, if it is covered by policy or law, is grounds for discharge. It does not matter where the employer committed the breach.

"Invading" a personal website is another matter. If the site is public then there is no invasion. However if it is private, allowing only restricted entry, it can violate the employee's rights. *Konop v. Hawaii Airlines*, 236 F.3d 1035 (9th Cir., 2001). The court found an invasion when the employer used false pretenses to get the access code to an employee's "restricted" chat room (limited to co-workers and friends).

Public chat rooms and e-bulletin boards are often anonymous. The identity of the individuals is not apparent. So how does one root out and stop the illegal defamatory messages? Unlike in print media, you may not just sue the "publisher." The Communication Decency Act insulates the service provider from liability for information sent or posted on its network or message boards. The individual sender can be sued, but rarely the service provider.

If the statements are legally egregious, one may file suit against an "unknown defendant" (A *Doe* case). Then use the discovery rules to try to force the system provider to cough up the identity of the individual. *Immunomedics Inc. v. Doe*, 342 N.J. Super 160 (N.J. App. Div., 2001). These are difficult cases, and often lead nowhere, because bulletin board users do not have to provide the service provider with their true name or email address. Also, the Internet is a public forum, and courts use a heightened First Amendment analysis in deciding whether to allow the discovery or impose liability. So even a private sector employee gets Constitutional rights. *Doe v. The Mart.com, Inc.* 140 F. Supp.2d 1088 (W.D. Wash., 2001).

Disability/Accessibility

Employees sue states over inaccessible computer systems. Employees in several states have sued to block new computer systems which are not accessible. In Arkansas, the state in turn

sued the software company, alleging that it failed to deliver a legally viable product. Computer inaccessibility is often the basis of challenges by employees and customers under the ADA.

POLICIES AND PROCESS

Computer usage policy. Have a comprehensive policy which covers the proper use, security measures and improper usages.

Personal use: to allow (?) or prohibit (?). Some organizations have prohibited all personal use of the computer system. These policies may eliminate the concerns about abuse; they are legally valid and are within the employer's right. However, they are also difficult to enforce, require extra "policing" which takes more time and effort than a standard "monitoring" policy, and generate resistance by employees.

Most employers have a "reasonable usage" practice accompanied by a "monitoring" policy. The warning that all usage will be monitored and recorded by management usually prevents most improper use and keeps other personal use to a low level.

Collateral policies. Also mentioned improper computer use in other relevant policies (*i.e.*, harassment, records confidentiality, safe driving, security of company property, etc.).

"No privacy" warning to all employees (and government officials). Give fair warning that any use of the computer system, Internet or intranet, may be subject to discovery and disclosure. For government employees and officials, it can be a "public use" subject to Public Records Requests.

Include a provision that all contents are property of the employer. Include the warning that use of one's personal home computer, laptop or Blackberry to interphase with the office computer system may make the content of these personal devices subject to discovery and disclosure.

Authorization to monitor. The usage policy should have a user signature (for the personnel file) which authorizes the organization to intercept, monitor, access, retrieve, copy and disseminate any and all information or messages from the individual's computer system or Internet usage. This authorization is also important for compliance with the Federal Electronic Communications Act. The authorization should include an understanding that the employer may consent to a police search and retrieval of information at anytime without further notice.

Periodically monitor. Any policy or warnings lose effectiveness unless there is at least sporadic monitoring of usage and enforcement of sanctions against those who violate the prohibitions. In fact, arbitrators and some courts have ruled that policies have "lapsed through atrophy" and long term non-enforcement has led employees to believe they had regained an "expectation of privacy."

Report illegal usage to the police.

F:\DOCS\WD\25211\149\A0504379.DOC