STAFFORD FREY COOPER

Danford D. Grant

BEST PRACTICES REGARDING EMPLOYEE COMPUTER USE

Grand Hyatt Seattle
721 Pine Street, Seattle, WA 98101
Thursday, December 13, 2007

I. Introduction

Companies have compelling reasons to protect private and confidential information. Securing business information preserves trade secrets and other intangible assets, and protecting customer information creates trust and brand loyalty, reduces litigation, and prevents liability. In addition, the spread of misleading and inaccurate information through email and the Internet can damage a company's reputation.

Controlling the flow of information presents one of today's greatest challenges for businesses. Email, peer-to-peer (P2P) file sharing programs, unauthorized software downloads, and even the use of home computers and web-based email for work related projects, all expose business data and jeopardize information security. Ironically, the effort to increase security sometimes has the opposite effect. For example, some employees remove secure information from corporate networks for legitimate purposes (to work on at home or while traveling, for example) because corporate security and firewalls make it difficult to log-on remotely.

Notwithstanding the technical, legal, and social-behavioral challenges companies face, it is critical for businesses to create, implement, and follow an effective information security policy. Many of us have heard dramatic stories about data loss during the past several years. For example, in January 2007 TJX Companies (TJ Maxx) reported a loss of customer information stored on a company computer. Two weeks later, a lawsuit filed in federal court alleged that "millions" of TJX customers had their "personal financial information compromised" and their "privacy rights violated" because of the company's "failure to maintain adequate computer data security."[1] Nine months later the company settled the suit (and others arising from the same breach) for $107 million dollars.[2] Closer to home, Boeing lost the personal information of 161,000 employees when thieves stole a laptop used by a Boeing human resources manager.[3] The company was quick to note that the laptop contained only employee information and "no classified, supplier, customer, engineering or material financial information" (i.e., no sensitive business information), which would have presented an even bigger problem. And it is not just large companies that are affected by data loss. Several months ago the City of Algona reported that an employee in the clerk's office stole utility bill payments.[4] Notably, Algona also accepts passport applications—which obviously contain personal information—and the arrested employee was the person at the City responsible for processing those applications (many of which were reportedly found in her home during the utility payment investigation). Every year there are hundreds or perhaps even thousands of incidents like these.

---

[1] Plaintiff's Complaint at 1-2, Mace v. TJX Companies, Inc., No. 1:07-cv-10162 (D. Mass, filed January 29, 2007).
[2] TJX also agreed in late November 2007 to pay Visa up to $40.9 million to replace customer credit cards.
[3] Dan Richman, *Stolen Boeing laptop held ID data on 161,000 people*, SEATTLE POST-INTELLIGENCER (Nov. 19, 2005) at seattlepi.nwsource.com/business/249011_idrisk19.html
[4] www.king5.com/localnews/stories/NW_081707WAB_algona_clerk_payments_stolen_TP.43bad0d3.html

These materials address one of the most important avenues for protecting business and customer information—controlling and monitoring employee computer use. We provide background information regarding employee privacy and an employer's legal (not technological) ability to monitor an employee's computer, email, and Internet use. We also highlight selected practices and policies designed to permit monitoring and protect information from accidental or intentional disclosure. Finally, we include a brief description of electronic discovery obligations because employee computer use can affect an employer's ability to respond to discovery and prevail in litigation.

II. Employee Privacy Rights

A. Generally

Privacy at work is limited. *See G.M. Leasing Corp. v. United States*, 429 U.S. 338 (1977); *see also O'Connor v. Ortega*, 480 U.S. 709 (1987). The right to privacy depends on a person's "reasonable expectation of privacy." *Id.* Courts have repeatedly held that employees have a diminished expectation of privacy in the workplace. *Id.*; *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

Even in California, which protects employee privacy more than most states, an employer can monitor an employee if the monitoring does not violate the employee's reasonable expectation of privacy and would not be highly offensive to a reasonable person. *See e.g., Hernandez v. Hillsides,* 48 Cal. Rptr. 3d 780, 789, (2006). In the workplace, the reasonableness of a person's expectation of privacy depends in large part on the identity of the intruder and the means of the intrusion. *Sanders v. American Broadcasting Companies*, 20 Cal.4th 907, 911, 85 Cal.Rptr.2d 909, 978 P.2d 67 (1999). When the "identity" of the intruder is the employer, and when the means of the intrusion are disclosed to the employee in advance of the intrusion, the intrusion is probably permitted.

B. Selected Sources of Employee Privacy Rights[5]

1. Private Employees

- Privacy torts
- Washington Privacy Act
- Federal Wiretap law and the ECPA
- ADA and state statutes
- Contract
- California Constitution

2. Public Employees

- All of the above, PLUS

[5] This is not an exhaustive list, but merely an example of some of the more common sources.

- Fourth Amendment
- 14th Amendment - Substantive Due Process (*Whalen v. Roe*)
- State Constitutions (Wash. Const. Art. 1, Sec. 7)

C. The Nature and Scope of Employee Privacy Rights

Because the federal and state constitutions apply to government conduct, the nature and scope of an employee's privacy right depends in part on whether the employer is a public or private entity.

1. Public Employers

Public employers have more restrictions than private employers on their ability to search and monitor employees because the constitution protects the privacy of public employees. Unfortunately, the standard available to guide public employers is vague. Specifically, public workplace monitoring and searching must be *reasonable under all the circumstances*. In *O'Connor v. Ortega*, 480 U.S. 709 (1987) the U.S. Supreme Court adopted the "reasonableness standard" and held:

> "Public employer intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."

O'Connor v. Ortega, 480 U.S. 709, 725-26. The Court reasoned that "[a] reasonableness standard permits regulation of the employer's conduct according to the dictates of reason and common sense." Although this is an adaptable standard, it is also unrevealing and difficult to rely on for guidance.

To determine if monitoring or searching is "reasonable" in the government context, courts use a two-pronged threshold test to determine if an employee has a right of privacy in the government workplace. The court first determines if the employee has an actual expectation of privacy (subjective test), and then determines if the expectation is reasonable (objective test). An employee's reasonable expectation of privacy is reduced where the employer informs the employee in advance that he or she will be subject to monitoring. *Biby v. Board of Regents of University of Nebraska at Lincoln*, 419 F.3d 845 (8th Cir. 2005). If the employee has a reasonable expectation of privacy, the court then "...balance[s] the invasion of the employee's legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace." *See O'Connor v. Ortega*, 480 U.S. 709, 719-20 (1987).

Nevertheless, certain searches are unreasonable even without a reasonable expectation of privacy. The U.S. Court of Appeals for the Second Circuit (in New York) has developed a two-part test to evaluate the reasonableness of monitoring or

searching intended to uncover employee misconduct. According to the court, "[a]n investigatory search for evidence of suspected work-related employee misfeasance will be constitutionally "reasonable" if it is [1] justified at its inception, and [2] of appropriate scope." *Leventhal v. Knapek*, 266 F.3d 64 (2d Cir. 2001). A search is "reasonable at inception" if "there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct." A search is "of appropriate scope" if it is "reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct."

Finally, any person, including a public employee, can waive constitutional protections if the waiver is "knowing, intelligent, and voluntary." *Schriro v. Landrigan*, 127 S.Ct. 1933, 1946 (2007). Thus, an employee can consent to an otherwise unreasonable search. *See McDonell v. Hunter*, 809 F.2d 1302 (8th Cir. 1987). Notably, however, a government employer cannot require an unreasonable search as a condition of employment. *See Pickering v. Board of Education*, 391 U.S. 563 (1968). Therefore, an employer probably cannot terminate an employee for refusing to consent to an unreasonable search.

2. Private Employers

In Washington, there is no constitutional right of workplace privacy for private sector employees. *See Roe v. Quality Trans. Servs.*, 67 Wn. App. 604, 838 P.2d 128 (1992). Thus, private employers are less restricted than public employers in their ability to monitor their employees.[6] Although private employers are generally free to search their employees, they "are best advised to conduct such searches in a reasonable manner to avoid emotional distress and invasion of privacy claims."[7] A private employer must avoid highly offensive invasions of an employee's reasonable expectations of privacy. *See Doe v. Gonzaga Univ.*, 143 Wn.2d 687, 705-06, 24 P.3d 390 (2001) (*rev'd on other grounds by* 536 U.S. 273, 122 S.Ct. 2268 (2002)).

Notwithstanding this wide latitude, there are still restrictions on a private employer's right to search and monitor. Restrictions, including those discussed below in Section III, come from general tort law or statutes that protect against specific behaviors or protect specific types of information. For example, the Wiretap Act protects against the interception of electronic communications.

But even when no specific statute applies, an employee's reasonable expectation of privacy can interfere with a private employer's ability to search. *See K-Mart v. Trotti*, 677 S.W.2d 632 (Tex. App. 1984). In *Trotti*, a K-Mart store manager and three assistants searched employees' lockers because store security personnel suspected that an employee had stolen a watch. In addition, the store manager suspected an employee had stolen missing price guns. Employee Trotti used a personal lock to secure her purse and other belongings inside her locker. During an afternoon break,

[6] Notably, this is not true in California because the California constitution applies to both public and private employers.
[7] Michael J. Killeen, EMPLOYMENT IN WASHINGTON § 3-5 (c)(1) at 3-13 (2007).

she returned to her locker and found the lock hanging open and personal items from her purse in disorder. Trotti sued K-Mart, claiming invasion of privacy. A jury awarded $8,000 in actual damages and another $100,000 in punitive damages. Although the court of appeals reversed on other grounds (a defect in the jury instructions), the court nevertheless found that Trotti had a reasonable expectation of privacy in her locker, that K-Mart had invaded that privacy interest, and that the jury's $100,000 award was not excessive under the circumstances. Specifically, the court held that an employer cannot search the locker of an employee when the employee expects privacy in the locker after providing her own lock at her own expense and with the employer's consent.

Employers that want to search should make sure their employees know the employer can and might search. For example, knowing that others within the company have access to an office can defeat an employee's claim to privacy in their office. In *Sorrentino v. Textron Lycoming*, 1995 U.S. Dist. LEXIS 21754 (D. Conn. 1995), the court held that a search of a manager's office and desk are proper if the company has a reasonable suspicion the employee is stealing company material, the office and desk are supplied by the company, and the employee knows the security department has keys to his office and desk.

III. Monitoring and Surveillance of Employees

A. Monitoring Generally

Employers put forth a variety reasons to justify monitoring. A 2001 American Management Association survey reported that 68% of the employers that monitor Internet and email use do so to protect against legal liability.[8] The following are some common reasons for monitoring:

- To curtail employee misconduct.
- To protect trade secrets and customer information.
- To protect against direct liability for negligent supervision or negligent retention.
- To protect against vicarious liability arising from careless or risky employee behavior (the "how's my driving" campaign, for example).
- To protect against employees that mistreat or harass other employees or customers.
- To scrutinize employees who serve the vulnerable (child or elder care, for example).
- To track employees whose personal lives could adversely impact the reputation of the employer (employees of politicians, for example).
- To avoid employees with personal or health problems that result in absences (a risky justification)

[8] 2001 AMA Survey, WORKPLACE MONITORING AND SURVEILLANCE: POLICIES AND PRACTICES (American Management Association 2001).

There are various methods employers use to monitor employees, including drug tests, credit reports, medical reports, private investigators, psychological tests, polygraph tests, questionnaires, telephone and voicemail surveillance, office searches, video surveillance, and GPS or other electronic tracking devices. Employers also use computer surveillance, including reading email, monitoring Internet use, and monitoring computer keystrokes.

B. The Duty to Monitor Employees

In almost all situations, a certain amount of monitoring is good business, and in some situations it is probably required. There is at least a general duty to supervise all employees, and the duty to supervise might include monitoring.

A more specific duty to monitor may arise when an employer has notice of prior or ongoing misconduct. *See e.g., Doe v. XYC Corp.*, 887 A.2d 1156 (N.J. Superior Ct. App. Div. 2005); *see also*, *Does 1 - 9 v. Compcare, Inc.*, 52 Wn.App. 688, 763 P.2d 1237 (1988). In *XYC Corp.,* a network administrator discovered that an employee was accessing pornography on his work computer. Supervisors told the employee to stop and the employee said he would comply with their demand. Later the employee used his work computer to upload nude photos of his daughter (a minor child) to the Internet. The mother of the child victim (and wife of the employee) sued the employer on behalf of the child, alleging that the employer knew or should have known and that it had a duty to report the employee's behavior to authorities. The court held:

> … an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third parties.

Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005). This opinion is unusual, and puts the employer in a law enforcement role, but it may reflect an extension of the modern trend toward a duty to monitor (instead of merely a right to monitor).

On a more basic level, adequate security measures—which probably include effective monitoring—are necessary to protect trade secrets. Trade secrets lose their status as protected secrets when the business that owns the secret fails to take adequate measures to maintain and protect the secret. Although a discussion of trade secrets is well beyond the scope of these materials, a company probably cannot ignore computer policies and procedures intended to protect electronic information and claim it has information security measures adequate to preserve trade secrets.

C. Restrictions on Monitoring

1. Generally

Although the law may be moving toward a more prominent duty to monitor employees, the ability to monitor is not without limits. Specific statutes and the common law provide various protections to employees in certain circumstances. Below are some of the more common employee protections related to communications, computers, and electronic information.

2. Telephone or Voice Conversations

(a) The Privacy Act

The Washington Privacy Act (RCW 9.73.030) requires the consent of **all** parties to **record** a private conversation.[9] The Act applies equally to telephone calls and face-to-face conversations. Notably, however, the Privacy Act does **NOT** prevent a party from listening to (or eavesdropping on) a phone (or face-to-face) conversation—it only prevents recording the conversation. *See State v. Bonilla*, 23 Wn. App. 869 (1979).

Evidence obtained in violation of the Act is not admissible in court. *See Schonauer v. DCR Entertainment*, 79 Wn. App. 808 (1979). Perhaps more important for employers, the Act provides a private right of action for damages for the greater of actual or liquidated damages of $1000, plus attorney fees. Damages for intercepting phone calls can be $100 per day.

(b) The Federal Wiretap Act

The Federal Wiretap Act (18 U.S.C. § 2510-2521), which is now part of the Electronic Communications Privacy Act of 1986, applies to telephone conversations and other wire communications. *Briggs v. American Air Filter Co.*, 630 F.2d 414, 417 (5th Cir. 1980). Notably, The USA PATRIOT Act removed "stored" communications from the definition of wire communications, and therefore the Wiretap Act no longer applies to voicemails (which are in storage and protected by the Stored Communications Act).

The Wiretap Act restricts employers from intercepting a wire communication (like a telephone call or email) unless the interception falls within a statutory exception. There are two primary exceptions applicable to the monitoring of telephone calls by an employer:

- Consent (actual or implied)
- The business extension exception

[9] Soundless video surveillance is permitted under the Privacy Act (but it is a good idea for employers to have a written policy and comply with it, monitor only when necessary, and avoid monitoring in areas where privacy is expected like a bathroom or locker room).

Although consent of one party to a conversation is sufficient under the Wiretap Act, this is not particularly meaningful in Washington because the Wiretap Act does not preempt the Privacy Act, which requires the consent of *all* parties to a conversation. Consent may be implied when an employee is notified of the monitoring and the mechanism and method of monitoring in an employee policy manual. The business extension exception permits an employer to eavesdrop on an employee business call from a telephone extension. However, if the call is private, employer monitoring must stop unless the conversation has the potential to "contaminate" the workplace. *Epps v. St. Mary's Hospital of Athens, Inc.*, 802 F.2d 412 (11th Cir. 1986).

Finally, federal agencies are immune from civil suit under the Wiretap Act.

3. Searching Computer Files

An employer that owns a workplace computer and maintains control over the computer (including a computer used by an employee) can search the computer. The employer also has the authority to consent to a search of the computer by law enforcement. *See United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007). In *Ziegler*, an employee of a private company accessed Internet child pornography from his work computer located in his personal office. The employee's office was locked and his computer was password protected. The employee did not share the computer with anyone. When the employer learned that the employee was accessing child pornography using the computer, the employer contacted the FBI and then cooperated with the resulting criminal investigation. In the course of cooperating, the employer consented to a search of the computer and the government found the child pornography. The employee then tried to suppress the evidence in his criminal trial.

The court held that an employer can consent to a search of an employee's workplace computer. Although the employee maintained a reasonable expectation of privacy in his workplace office and computer because of the lock and the password, the employer nevertheless retained the ability to consent to the search because the office and computer were workplace property that remained under the control of the employer.

4. Monitoring Emails, Instant Messages, and Text Messages

(a) Electronic Communications Privacy Act of 1986 (ECPA)

The Electronic Communications Privacy Act of 1986 prohibits the interception, use, or disclosure of electronic communication under certain circumstances. Under the Wiretap Act (in effect for decades but since 1986 included as a chapter of ECPA), employers cannot "intercept" email unless it falls within an exception. The exceptions in the Wiretap Act relevant to employer email monitoring are (1) consent and (2) an interception in the ordinary course of business. Notably, however, "stored" email is not "intercepted," and therefore email in storage is controlled by the Stored Communications Act (another chapter of ECPA). Email on the employer's server is arguably "in storage." *See Steve Jackson Games, Inc. v. United States Secret Service*,

36 F.3d 457 (5th Cir. 1994). Pursuant to an exception in the SCA, an employer can access email in storage if the employer is the Internet or email service provider, or perhaps even if the employer is an authorized agent of the Internet or email service provider.

(b) Selected Cases

In *Steve Jackson Games Inc. v. United States Secret Service*, 36 F.3d 457 (5th Cir. 1994), the director of network security for a Bell South affiliate investigated the unauthorized duplication and distribution of a computer text file containing information about Bell's emergency call response system. He called the Secret Service when he discovered a document on an online bulletin board operated by an employee of Steve Jackson Games. The bulletin board had 365 users who could send private electronic messages to the board. The messages were stored on computers at SJG, and SJG's systems operators could review and perhaps delete any data on the bulletin board. Secret Service agents secured a warrant and seized the SJG computer that operated the bulletin board. The computer contained 162 items of unread, private email. Secret Service agents read and deleted this private email. SJG and several bulletin board users sued the Secret Service for violations of the Privacy Act, the Stored Communications Act, and the Wiretap Act. The trial court found violations of the Privacy Act and the Stored Communications Act, and awarded over $50,000 in damages and another $250,000 for attorneys' fees and costs. Both the trial court and the court of appeals agreed, however, that the Secret Service did not violate the Wiretap Act because it did not "intercept" any electronic communication. The courts noted a difference in the statute between the definitions of a "wire communication," *i.e.* an aural transfer of information, and an "electronic communication." The courts found that the emails sent to the message board were "electronic communications" and that they were in "electronic storage" even though they had not yet been received by their intended recipients. In other words, the messages were not "intercepted" in transit, but were instead retrieved from storage, notwithstanding that they had not yet reached their intended destination. Because the Secret Service did not access the messages as they were sent, and instead retrieved them from electronic storage, the courts found there was no "intercept" and therefore no violation of the Wiretap Act.

In *Biby v. Board of Regents of University of Nebraska at Lincoln*, 419 F.3d 845 (8th Cir. 2005), the court held that an employer did not violate an employee's privacy when searching the employee's computer for emails relevant to a pending arbitration. The employer's computer policy specifically told employees that computer files, including email, could be searched in response to a discovery request in the course of litigation. In light of this policy, the court found that the employee had no reasonable expectation of privacy in his computer files under the circumstances. The court also rejected the argument that the policy allowed unreasonably broad searches, concluding that the employer needed to search broadly to ensure it had gathered all discoverable documents.

In *Smyth v. Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996), an at-will employee brought suit against an employer alleging wrongful termination and invasion of privacy. The employer fired the employee after intercepting an email the employee sent a supervisor complaining about co-workers and management. Notably, the employer had previously assured employees that email could not be inspected and would not be used as a basis for termination. Nevertheless, the court held that an employee has no reasonable expectation of privacy in emails he sends to other employees over the company system, *even when the company repeatedly assures employees that email will not be intercepted or read and used as a basis for termination.* Although this decision is questionable based on the employer's representations, it illustrates the wide latitude employers have to monitor employee email use.

In *McLaren v. Microsoft Corp.*, 1999 WL 339015 (Tx. App. 1999) (unpublished), Microsoft suspended an employee while investigating accusations of sexual harassment and "inventory questions." The employee asked for access to his email to refute the allegations against him, but was told he could only access messages by telling company officials the locations of the specific messages he sought. General access to the email system required a network password. The employee also had a "personal store" to protect his personal emails, and asked that no one tamper with his workstation or email. After being terminated, the employee sued Microsoft for invasion of privacy, claiming the company had decrypted, "broken into," and released the contents of his personal folders to third parties. Distinguishing the court decision regarding the lockers in *Trotti*, the court held the employee had no reasonable expectation of privacy in his computer or emails. Unlike a locker, whose purpose is to store *personal* items, Microsoft provided computers to employees so they could perform the functions of their jobs. Additionally, email transmitted through a network is accessible by third parties, even if the employee later stores the email in a password-protected personal folder. Thus, the court concluded that the employee could not manifest–and Microsoft did not recognize–a reasonable expectation of privacy in files stored on his computer workstation. Moreover, the court concluded that even if the employee had some expectation of privacy, Microsoft's invasion of that privacy was not "highly offensive" and therefore could not give rise to legal liability. Notably, the court reached this conclusion without discussing Microsoft's computer use policy.

In *U.S. v. Simons*, 206 F.3d 392 (2000), the CIA's Foreign Bureau of Information Services (FBIS) monitored employees for any violations of the FBIS Internet usage policy which required employees to limit their Internet use to official government business. The policy also informed employees that the FBIS would audit and monitor Internet use. When a firewall test indicated an employee's computer was used to visit non-work-related websites, supervisors used a remote workstation to examine the contents of the employee's computer, including his Internet usage and downloads. They found over 1,000 downloaded pictures, and the several samples they viewed were pornographic. The employer then copied all the files on the employee's computer from a remote workstation. A criminal investigator from the CIA viewed selected files and discovered they were pornographic pictures of minors. The employer then physically entered the employee's office, removed his hard drive, replaced it with a copy, and gave

the original to the FBIS Area Security Officer, who gave it to the criminal investigator. An FBI agent later viewed over 50 images on the hard drive, many that contained child pornography. The agent then obtained a search warrant to search the employee's office and computer. When agents executed the warrant, they copied the contents of employee's computer, diskettes found in his desk drawer, computer files on a zip drive connected to his computer, videotapes, and a number of documents. In the employee's subsequent criminal prosecution, the employee sought to suppress the pornographic pictures, claiming they had been discovered in a search and seizure prohibited by the Fourth Amendment. First, the court concluded that the employee had no reasonable expectation of privacy in his computer because of the employer's computer policy. Next the court concluded that although the employee had an expectation of privacy in his office, which he did not share, the employer's entry to retrieve the hard drive was a reasonable workplace search because "FBIS had an interest in fully investigating [the employee's] misconduct...." The court concluded:

> In the final analysis, this case involves an employee's supervisor entering the employee's government office and retrieving a piece of government equipment in which the employee had absolutely no expectation of privacy—equipment that the employer knew contained evidence of crimes committed by the employee in the employee's office. This situation may be contrasted with one in which the criminal acts of a government employee were unrelated to his employment. Here, there was a conjunction of the conduct that violated the employer's policy and the conduct that violated the criminal law.

Accordingly, the court upheld the conviction.

In *TBG Ins. Services Corp. v. Superior Court*, 96 Cal.App.4th 443, 117 Cal.Rptr.2d 155 (2002) an executive-level employee used two computers owned by his employer, one at the office and one at home. According to the employee, the home computer was a perk given to every executive and it was universally accepted that such computers could be used for both personal and business purposes. However, the employee had signed an electronic and telephone equipment policy agreeing that his computers could be used only for business purposes, the company could monitor his computers on an "as needed" basis, and communications using his computers were not private. The company fired the employee after discovering he had repeatedly accessed pornographic websites at work. The employee claimed that he did not intentionally access the sites, but they simply "popped up" on his computer. He also argued that the company's allegations of pornography were a pretext and he had been fired to prevent the vesting of company shares three days later. When the employee sued for wrongful termination, the employer served a discovery request for the home computer. Although the court found the employee had privacy interests in personal information he kept on the home computer (e.g. finances, family communications), it also noted that "the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to his use of his employer's computers." Thus, the court concluded that when the employee signed the

equipment policy, the employee had the opportunity to consent to or reject the invasion he now challenged, and he had therefore waived whatever privacy right he may have had in the home computer. The court therefore ordered production of the home computer, but also stated that the employee could ask to exclude specific information from discovery.

5. Monitoring Employee Blogs and Websites

Businesses are often confronted by websites, newsgroups, message boards, and chat rooms used by employees to criticize companies and their executives. This behavior is generally referred to as “cybersmearing,” and often damages an employer’s reputation. Cybersmearing can occur in either public forums or private blogs. When the information is untrue, the employer may have a cause of action against the employee for defamation.

A business must be careful before accessing a private website or private blog. Pursuant to ECPA (specifically the Stored Communications Act), an employer may be liable for accessing an employee’s private website or blog without permission. For example, in *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 872 (9th Cir. 2002), a pilot operated a secure website on which he criticized his employer, Hawaiian Airlines. The pilot that operated the blog gave access to other Hawaiian Airlines pilots, two of whom then provided their access passwords to Hawaiian Airlines management without permission of the pilot operating the blog. One of those pilots cooperating with management never personally accessed the employee’s website. The court noted that the Stored Communications Act authorizes users of a website to give permission to others to access the site, but nevertheless concluded that because the pilot who authorized the airline to access the site had never himself accessed the site, he was not a "user" under the Stored Communications Act and had no authority to authorize a third party to access the site. Accordingly, the court reversed summary judgment in favor of Hawaiian Airlines and sent the case to trial.

In *Bennett v. Detroit Police Chief*, 274 Mich.App. 307, 732 N.W.2d 164 (2006), a Detroit police officer created, registered, and operated a website featuring articles and editorials critical of Detroit Police Chief Jerry Oliver. The website also hosted various blogs where users shared their opinions. Chief Oliver suspended the officer’s duty status without pay, and the Board of Police Commissioners agreed the officer had engaged in misconduct that prevented him from continuing his duties as a police officer. A grievance arbitrator upheld the Board’s decision. The officer sued the City of Detroit, its mayor, and Chief Oliver for wrongful discharge for the lawful exercise of his constitutionally guaranteed free speech rights. The court held that Chief Oliver was acting within the scope of his authority and exercising a government function, and was therefore entitled to governmental immunity from the plaintiff’s tort claim. It similarly granted immunity to the city based on its exercise of a government function. The court also upheld dismissal of the claim against the mayor, finding no evidence of his involvement in the suspension. Although the court decided city officials were immune from suit and dismissed the employee's claims for damages, the Michigan Employee

Relations Commission ordered the City to reinstate the employee in a parallel proceeding, concluding he was fired for engaging in protected speech. Last week (on December 4, 2007), the Michigan Court of Appeals affirmed the MERC decision in an unpublished opinion.[10]

Other notable examples of employee firings based on blogging—which may or may not be allowed—include the following:

- Google terminated Mark Jen after only 10 days of employment after Jen posted critical comments about his experiences at his new employer.[11]

- Delta Airlines fired Ellen Simonetti after she posted suggestive photographs of herself on her blog, "Queen of the Sky: Diary of a Dysfunctional Flight Attendant." The blog did not specifically name Delta Airlines. Simonetti filed a claim with the EEOC for sex discrimination, alleging several male employees were not disciplined for similar conduct. She received her right to sue letter, and her case is pending in a Federal court in Georgia.[12]

- Friendster hired Joyce Park to reprogram its website to combat sluggish site performance. Friendster fired Park when she commented on her blog that the former site was "pokey."[13]

- Microsoft fired an employee after he posted pictures on his blog showing Apple computers being delivered to the Microsoft campus.

A 2005 CNN article indicates that other companies including Starbucks, Wells Fargo, and Kmart have also fired employees for blogging.[14]

IV. Recommended Policies and Practices

A. Best Practices Generally

As the Supreme Court noted in *O'Connor v. Ortega*, 480 U.S. 709, 725-26, "[e]xpectations of privacy in employees' offices, desks, and file cabinets, … may be

---

[10] City of Detroit v. DPOA, No. 268278 (Dec. 4, 2007) (unpublished).
[11] Evan Hansen, GOOGLE BLOGGER HAS LEFT THE BUILDING, CNET News. Com, February 8, 2005 (available at http://www.news.com/Google-blogger-has-left-the-building/2100-1038_3-5567863.html, last accessed 12/8/07).
[12] *Id.*; Katherine L. Kettler and John F. Hyland, PRIVACY AND SECURITY IN THE WORKPLACE: EMPLOYEES AS THE PROBLEM AND VICTIM, Practising Law Institute, 903 PLI/Pat 227 (2007); "ELLEN SIMONETTI," Wikipedia, the Free Encyclopedia (available at http://en.wikipedia.org/wiki/Ellen_Simonetti, last accessed 12/8/07).
[13] Kettler and Hyland, *supra*; JUDITH MESKILL, FRIENDSTER FIRED TROUTGIRL FOR BLOGGING?!, thesocialsoftwareblog, August 2004 (available at http://socialsoftware.weblogsinc.com/2004/08/30/friendster-fires-troutgirl-for-blogging/, last accessed December 9, 2007).
[14] Kate Lorenz, AVOID GETTING FIRED FOR BLOGGING, CNN.com and CareerBuilder.com, April 2005 (available at http://www.cnn.com/2005/US/Careers/04/05/blogging/, last accessed 12/9/07).

reduced by virtue of actual office practices and procedures, or by legitimate regulation." Accessibility of an employee's office will reduce an employee's expectation of privacy in his or her office. Notice of monitoring email and Internet activity reduces expectations of privacy in email and Internet activity. Thus, to effectively monitor employees, an employer should inform the employee that it will (or at the very least reserves the right to) monitor email and computer use. For example, in *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000), the government employer had a policy that (1) prohibited employees from accessing unlawful material on work computer, (2) prohibited employees from using the Internet for anything except official business, and (3) disclosed that periodic inspections would occur. The court held that this policy was sufficient to defeat an employee's constitutional privacy claim after the employer searched the employee's computer and discovered child pornography.

B. Best Practices with Regard to Computers and Technology

1. Email and Internet Use

Employers rely on a variety of reasons to monitor emails and computer use:

> Employers contend that e-mail monitoring is important because the use of e-mail (and the Internet) can bring in viruses that can harm the employer's computer system. Employers are liable for defamation, copyright violations, and sexual harassment, which can take place over e-mail. Chevron Corporation was sued for hostile work environment when some employees sent around via e-mail a joke list called "Why beer is better than women." The case settled … for $2.2 million.

Daniel J. Solove et al., INFORMATION PRIVACY LAW, 857 (2d. ed. 2006).

In some cases, allowing an employer to monitor illegal activity or unprofessional behavior is more important to courts than an employee's expectation of privacy. Nevertheless, as noted above, absent a specific statutory prohibition, whether monitoring is allowed usually turns on whether the employee has a reasonable expectation of privacy. Providing notice of monitoring will typically reduce or eliminate an expectation of privacy in email, Internet use, computer files, and text messages.

Notably, computer password protection probably does not create an expectation of privacy, so employers should feel free to encourage password use to increase overall system security. *See Garrity v. John Hancock Life Insurance Co*., (D. Mass. 2002). In *Garrity*, the court held that even though the employer showed employees how to create private passwords and personal email folders, employees had no reasonable expectation of privacy in email because they assumed the recipients of their emails might forward them to third parties, and they also assumed that their employer was capable of looking at email on the company's intranet system.

All email and computer monitoring should be fair and consistent with a disclosed policy. At a minimum, employers should adopt the following policies and procedures regarding computers and email use:

- Give prominent notice that employer computers, computer files, and email, are subject to monitoring;
- Save incoming and outgoing email and review it from storage, instead of intercepting its transmission;
- Establish an email retention schedule and comply with it;
- Train employees that prohibitions on discriminatory and harassing behavior apply to email;
- Train employees not to send or discuss trade secrets over email;
- Prohibit employees from using P2P software;
- Prohibit employees from downloading unauthorized software.

2. Blogging

As noted above, an employer can be liable for accessing a private blog without permission. An employer, however, can monitor a blog that is accessible to the public. Employer's need to be careful before terminating employees or bringing actions related to cybersmearing and defamation. The constitution protects free speech. The National Labor Relations Act prohibits an employer from taking any action that could reasonably be construed to chill discussion about wages and other terms and conditions of employment. *Cintas Corp.*, 344 N.L.R.B. No. 118 (2005). And although employers often attempt to bring John Doe lawsuits to determine the names of anonymous posters, in certain circumstances the First Amendment protects an employee's right to speak anonymously. *See, e.g., McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995); *see also Talley v. California*, 362 U.S. 60 (1960) (persons can distribute handbills without identifying the party who printed, wrote, compiled, or manufactured them). Finally, Anti-SLAPP legislation in many states (which are well beyond the scope of these materials) prevents lawsuits intended to halt protected speech.

Accordingly, we recommend that employers consult with legal counsel before taking any action in response to employee blogging that occurs outside the workplace. On the other hand, employers can implement policies regarding the use of work computers.

3. Preventing Disruptive Emails

Besides the ability to monitor employee email and computer use, employers should develop plans for dealing with employees or former employees that deplete system resources or use computer resources in a manner that disrupts the system. When the attacks come from former employees, and there is no technological solution, the only option may be a lawsuit. In addition to injunctions, some employers have used the tort "trespass to chattels" to hold employees and former employees liable for sending mass emails. Trespass to chattels is intentionally meddling with property

belonging to another that causes harm to the chattel (like an employee meddling with a computer or network belonging to an employer). In *School of Visual Arts v. Kuprewicz*, 3 Misc. 3d 278, 771 N.Y.S.2d 804 (2003), a former employee used unsolicited emails to send large volumes of pornography to the company's Director of Human Resources. The court expressly ignored that the emails contained pornography, and held that the emails were a trespass to chattels because they depleted hard drive space, drained processing power, and adversely affected other system resources. However, in *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 71 P.3d 296 (Cal. 2003), although a former Intel employee sent six emails to 35,000 Intel employees (a total of 210,000 emails), the court held the employee did not trespass because the email barrage did not physically damage, cause a functional disruption, or deprive the company of use of its computers.

V. Electronic Discovery

A. Introduction

Over a year ago, amendments to the Federal Rules of Civil Procedure took effect that (in part) formalized the rules regarding electronic discovery that had been developing over the preceding few years. Although it has been clear for some time that electronic information is a critical component to discovery and litigants are entitled to access, a recent business survey indicates that only 6% of companies said they could immediately and confidently handle e-discovery requests, and more than half said they might not be able to enforce a litigation hold.[15] Their worries arise in part from the need to organize unwieldy information systems and the inability to control employee data. For example, in order to effectively respond to an e-discovery request, a business MUST know where all the potentially responsive data is located. If employees duplicate data on flash drives, work from home on personal computers, and take notes on a personal PDA, the company and its lawyers can easily miss and omit relevant data from a discovery response.

A detailed discussion about e-discovery is beyond the scope of these materials, which are intended only to scratch the surface of the issue and point out a few critical problems.

B. General Rules

Electronic information is different from paper in several important ways:

- The volume of electronic information is significantly greater;
- The data comes from a variety of sources;
- The data contains hidden information (metadata, for example);
- The usability of data is often dependant on the program that created it;

[15] Nikki Swartz, *Firms Unprepared for E-Discovery*, THE INFORMATION MANAGEMENT JOURNAL at 6 (Nov/Dec. 2007).

- The data can be changed without user intervention (automated functions);
- The data is rarely "deleted" (delete usually means "ignore/hide," not destroy).

The rules for dealing with electronic information expect companies to have it, expect companies to preserve it in anticipation of litigation, and expect companies to produce it when required.

The amended discovery rules expressly refer to electronically stored information and include electronic information within the universe of initial disclosures (items that must be provided to the other side before the other side even asks for it). The amended rules require lawyers for the parties in litigation to "meet and confer" regarding their obligations to preserve and produce electronic information, and to develop a discovery plan that includes the production of electronic information. In fact, the court's case scheduling order will include a provision directing the disclosure of electronic information. The amended rules also contain other significant provisions, including the ability to specify the form in which a party should produce electronic information, the ability to recover privileged information that has been inadvertently disclosed, and immunity from sanctions for electronic information lost as a result of the routine good-faith operation of the information system.

One of the first things you are likely to notice in response to new or potential litigation is a request from counsel to discuss your electronic discovery obligations. In fact, court cases over the past few years have imposed non-delegable duties on lawyers to communicate e-discovery obligations to clients and to direct a client's electronic data preservation and collection efforts. Lawyers have been sanctioned for their part in a client's failure to preserve data in anticipation of litigation or produce it in the course of litigation.

C. Best Practices

1. Generally

The key to an effective e-discovery plan is similar to an effective information security plan:

- Put policies and procedures into effect that minimize the unnecessary duplication and spread of company data (without interfering with business functionality);
- Assume at least one employee will violate the policies and therefore effectively investigate and question where all the data MIGHT be located;
- Have (and follow) a careful and considered records retention policy; and
- Issue timely (immediate) instructions to preserve data when necessary.

Thus, the precautions causing stress in the business world that must be taken in response to the amended discovery rules are in some ways merely reflective of precautions that should be taken by every company to protect its information.

At a minimum, expect the following from your outside counsel in response to a lawsuit:

- An initial and later a more detailed conference between the client, the client's IT team, and the legal team to determine the structure/character of the company's IT system and the scope of the company's electronically stored information (who has it and in what form);
- Direction from the lawyers to preserve potentially relevant data, which includes directions to employees to preserve data (the litigation hold);
- Participation in the collection of data

2. Steps in the Electronic Discovery Process

1) Initial meeting between lawyer and client to determine contact list and scope of information for initial litigation hold
2) Issue litigation hold

   - Develop schedule for additional notices
   - Notify all potential custodians and IT personnel of their obligation to preserve information (with specific direction on mechanisms)
   - Disable all automatic systems that purge or delete data

3) Detailed meeting between lawyers and client for lawyers to learn about client's IT systems and document custodians, and for client to learn about its obligations

   - What is the potentially relevant data?
   - What is the relevant time frame?
   - What type of data are we dealing with (email, excel, powerpoint, pdf)?
   - Who has the potentially relevant data?
   - Where is the data located? (home computers, blackberries, PDAs, thumb drives)
   - Is the data "reasonably accessible?"

4) Preserve the data (probably through a vendor if justified).
5) Collect the data (probably through an outside vendor).
6) Prepare the data for attorney review (by vendor or attorney).
7) Attorney review.
8) Produce the data (by attorney).

3. The Big Problem/Risk

Data preservation is usually very expensive. Adequate preservation must occur almost immediately (otherwise data will be changed). The standard for determining what preservation efforts are reasonable will take time to develop. Thus, a company expecting a lawsuit today has to make a calculated risk regarding its preservation obligations, based on the cost of preservation and the value of the potential claims in the litigation. It is still unclear what a company must do to comply with its preservation obligations, but the risks and sanctions for doing too little can be significant.