BARRAN LIEBMAN LLP
ATTORNEYS

Government Searches of Workplace Computers: Civil Issues for Employers and Employees

Federal Bar Association

Paula A. Barran
Barran Liebman LLP
www. barran. com

INTRODUCTION

In a typical workplace, the employer owns the computer, the storage media, the network, the furniture, the workspace and the work product. Employment settings, however, are regularly used and misused by employees for their personal pursuits. Many factors contribute. The computer equipment is readily available, the employee may work in a relatively private space, computer access can be blindingly fast, and children and other family members are not around to watch what is happening. In such cases, employers have found to their dismay that their computer systems have been used to commit various kinds of computer crime including the viewing of child pornography.

Police and investigators are probably derelict in their duties if they do not follow up on the workplace computer in the case of a suspect who is thought or known to be engaging in computer-based criminal activity. That, of course, puts employers in the crosshairs.

LAWS THAT MERIT CONSIDERATION

- Constitutional law. Various amendments found in the Bill of Rights offer protections against governmental intrusion. The First Amendment protects association. The Third protects a home from invasion. The Fourth affirms the right to be secure from unreasonable search and seizure in "persons, houses, papers and effects" whereas the Fifth provides a zone of privacy by protecting against testimonial self-incrimination. The Ninth appears to preserve other rights that are "retained" by the people. These guarantees are viable in the workplace, but they are restricted. The state as employer has rights vis á vis its employees that the state as sovereign does not have. Otherwise, government could not function. "When a citizen enters government service, the citizen by necessity must accept certain limitations on his or her freedom. See, ***e.g., Waters v. Churchill,*** 511 U.S. 661, 671, 114 S.Ct. 1878, 128 L.Ed.2d 686 (1994) (plurality opinion) ("[T]he government as employer indeed has far broader powers than does the government as sovereign"). Government employers, like private employers, need a significant degree of control over their employees' words and actions; without it, there would be little chance for the efficient provision of public services." *Garcetti v. Ceballos*, 547 U.S. 410, 418-419 (2006). At a state level, Oregon's constitution has provisions similar to the federal Constitution, but the extent of its protection may be greater than offered on a federal level. Or. Const., Art. I, Sec. 9., ***State v. Caraher***, 293 Or. 741, 653 P.2d 942 (1982).

- Federal legislation**.**

    - Congress enacted the Video Privacy Protection Act, 18 USC § 2710, to prohibit the disclosure of videotape rentals without notice to and consent from the consumer involved. The statute resulted from the fallout after the failed nomination of Robert Bork to the U.S. Supreme Court. During his confirmation process a newspaper had obtained a list of videotapes that his family had rented from a neighborhood store. The Senate Report, SREP 100-599, 1988 USCCAN 43421 explained that the new

law followed a long line of statutes passed by Congress to extend privacy protection to records that contain information about individuals.

- Congress also passed the Cable Communications Policy Act of 1984, 47 USC § 521, et seq. It was intended to establish a national policy concerning cable communications and to protect personally identifiable information collected or to be collected with respect to subscribers, who are entitled to notice of the nature of use of such information.

- The Electronic Communications Privacy Act of 1986, 18 USC § 2510 *et seq.*, addresses wiretaps as well as "stored communications"; the law was dramatically affected by the events of September 11, 2001 and the passage, a few weeks later, of the Patriot Act (specifically, the USA PATRIOT Act, PL 107-56, 115 Stat 272 (2001)) which is identified as "An Act to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes." The wiretap provisions of the ECPA generally prohibit any person from intentionally intercepting any wire, oral or electronic communication during its transmission, although with exceptions for interceptions done with consent or in the ordinary course of business. The provisions relating to Stored Communications (18 USC § 2701 *et seq.*) protect against unauthorized access or divulging of contents of communications that are in temporary intermediate storage incidental to transmission, but there are exemptions for coverage providers. There are related state law provisions codified at ORS 133.721, *et seq*.

- The National Labor Relations Act, 29 USC § 151 *et seq.* provides some workplace related protections including from surveillance and interrogation.

- The Americans With Disabilities Act, 42 USC § 12101 *et seq.*, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 USC § 201 *et seq*. both provide for confidentiality of medical or personal health information. ORS 659.400 *et seq*. provides similar protections.

- The Fair Credit Reporting Act 15 USC § 1681 *et seq*. limits the circumstances under which background checks and other "mode of living" inquiries may be made. It also prohibits certain reporting agencies that collect information on consumers from disclosing their records to third persons who are not authorized, and establishes procedures to correct inaccurate information.

- In 1974, Congress enacted the Family Educational Rights and Privacy Act (FERPA), 20 USC § 1232(g) which protects the privacy and confidentiality of educational records.

- The Federal Privacy Act, 5 USC § 552(a) provides confidentiality and privacy protections of information in the possession of federal agencies. The statute provides that the federal government may not maintain secret records and that individuals have a right to know what files exist on them.

- The Employee Polygraph Protection Act, 29 USC § 2001 *et seq*. (and the similar provisions of state law codified at ORS 659A.300) limit the circumstances under which a polygraph may be required or used.

- The Tax Reform Act of 1976, 26 USC § 6103, established protections for the confidentiality of individual tax returns including limitations on third party disclosures.

- Personal financial records received additional protections under the Right to Financial Privacy Act of 1978, 12 USC § 3401, et seq.

- On May 21, 2008 the Genetic Information Nondiscrimination law was signed. The law prohibits discrimination based on genetic information including an individual's own genetic tests, the tests of family members, and the manifestations of genetic diseases or disorders in family members. Title I of the statute amends ERISA, the Public Health Service Act, the Internal Revenue Code, parts of the Social Security Act, and includes provisions relating to privacy and confidentiality. Title II prohibits employment discrimination on the basis of genetic information. Title II applies to private employers as well as state and local government employers as long as they have 15 or more employees. It also covers employment agencies, labor unions, and joint labor-management training programs. Provisions are also applicable to Congress and the Federal Executive Branch agencies. The law was passed in large part because there have been such extraordinary developments in the field of genetics. The information that can be gleaned from such developments is advantageous medically but presents risks when one considers the extent to which the information can be used. On the one hand, individuals may be able to learn whether they are at risk for developing certain conditions; on the other hand, they may be concerned that if the information becomes known they will not be able to obtain employment in a desired field or, perhaps worse, will lose medical coverage. The statute prohibits the use of genetic information in making decisions related to any terms, conditions or privileges of employment. It prohibits covered entities such as employers from intentionally acquiring the information and absolutely prohibits the use of genetic information in making employment decisions. Any information that comes to employers must be treated as confidential medical information. The statute also sets a "floor"; in other words it does not preempt state laws that provide equal or greater protection. Remedies can be extensive and include reinstatement, hiring, promotion, back pay, injunctive relief, compensatory and punitive damages against private employers, as well as attorney fees and costs. The EEOC has issued regulations to implement the statute.

- State legislation**.** In addition to the state laws that are aligned with federal protections cited above, there are a number of privacy related laws.

  - There is a crime of invasion of privacy (ORS 163.700) if a person invades a reasonable expectation of privacy and knowingly observes, or photocopies, or makes a visual recording of another person in a state of nudity without consent, in a state of nudity where the other person has a reasonable expectation of privacy and a related civil cause of action at ORS 30.865 which provides for attorney fees.

- Public employee personnel records are public records within the meaning of Oregon's Public Records Act. Personnel disciplinary actions, and documents related thereto, ORS 192.501(12) (2001), are exempt from disclosure. Also, information "of a personal nature" kept in a "personal medical or similar file" is exempt absent clear and convincing evidence of the public interest if "disclosure would constitute an unreasonable invasion of privacy" ORS 192.502(2).

- It is an unlawful employment practice for an employer to require, as a condition of employment, any employee or prospective employee to refrain from using lawful tobacco products during non-working hours except when the restriction relates to a bona fide occupational requirement or when an applicable collective bargaining agreement prohibits off duty use of tobacco products. ORS 659A.315. State law also makes it unlawful for any person "to obtain or attempt to obtain the whole or any part of a conversation by means of any device . . . if all participants in the conversation are not specifically informed that the conversation is being obtained." ORS 165.540(1)(c). ORS 659A.303 protects genetic privacy.

- State common law**.** There are four separate and distinct legal theories called "invasion of privacy," each of which requires proof of a private fact and that the invasion or intrusion was unreasonable and without consent: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) placing a person in a false light; and (4) appropriation of name or likeness. See *Hinish v. Meier and Frank Co.*, 166 Or. 482, 113 P.2d 438 (1941), *Anderson v. Fisher Broadcasting Co.*, 300 Or. 452, 712 P.2d 803 (1986), for a general discussion of the tort. Proof of invasion of privacy by intrusion upon seclusion requires an intentional intrusion, physical or otherwise, upon plaintiff's private affairs or concerns, carried out in a way that would be offensive to a reasonable person. *Leggett v. First Interstate Bank of Oregon*, 86 Or. App. 523, 739 P.2d 1083 (1987) (telephoning employee's doctor). Invasion of privacy by public disclosure of private facts requires a showing that there was an objectionable disclosure of private facts to the public generally or to a large number of persons. *Tollefson v. Price*, 247 Or. 398, 430 P.2d 990 (1967) (publication of notice offering to sell debts). "False light" privacy is somewhat analogous to defamation. If information is publicized to a large number of people and causes them or some of them to believe something false about a person, the claim lies in invasion of privacy by false light. *Morrow v. II Morrow, Inc.*, 139 Or. App. 212, 911 P.2d 964 (1996) (performance documentation stored on accessible network of employer's computer system); see also *Gardner v. Martino*, 2005 WL 3465349 (D. Or. 2005). Invasion of privacy by appropriation of a name of likeness applies to those situations in which names, photographs or other identifying information is used without consent to advertise or otherwise support another entity.

WORKPLACE PRIVACY: PUBLIC EMPLOYMENT

The U.S. Supreme Court's decision in *O'Connor v. Ortega*, 480 U.S. 709 (1987), outlined and established key principles relating to workplace privacy for public employees. Magno Ortega was the plaintiff in the underlying litigation. He was a physician and psychiatrist responsible for training physicians in psychiatric residency programs in a public hospital. After years of apparently successful performance, Dr. Ortega's superiors became concerned about possible improprieties in the acquisition of equipment and treatment of some hospital employees. In the course of investigating these concerns, the employer entered Dr. Ortega's office while Dr. Ortega was still on administrative leave pending investigation of the concerns about his performance. Although the investigative team was made up of the employer's own personnel, the hospital was

a public hospital and as a result the investigators were public officials. In a thorough search they seized items from Dr. Ortega's desk and file cabinets.

In connection with his termination from employment, Dr. Ortega commenced suit over the invasion of his interests. Because of the public nature of his employment he alleged a violation of the Fourth Amendment; in this regard the Fourth Amendment is enforced by 42 USC § 1983 which was the remedial basis for the lawsuit.

O'Connor v. Ortega establishes a number of important questions in the context of employee searches (the case did not address searches in the criminal context):

- Although the Fourth Amendment protections are often thought of in a criminal context, they are just as important in a civil context including, for example, in employment. The Fourth Amendment is not limited to circumstances when the individual is suspected of criminal behavior.

- Searches and seizures by government employers or supervisors of the private property of their employees are subject to the restraints of the Fourth Amendment.

- Fourth Amendment rights are implicated only if the conduct at issue infringed "an expectation of privacy that society is prepared to consider reasonable." That expectation of privacy depends upon the context including the use to which an individual has put a location.

- There are no clear legal guidelines to establish "employer space" and separate it from "employee space."

- Because there are societal expectations of privacy in one's place of work, there can be no categorical rule or principle that public employees may <u>never</u> have an expectation of privacy. "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."

- Expectations of privacy may be reduced by virtual or actual office practices and procedures or legitimate regulation. Because the great variety of work environments in the public sector presents a case-by-case context, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis. The contextual evidence in this case included that Dr. Ortega had a private office and did not share his desk or file cabinets with anyone else. Work related residency training files were not kept in his private office. There was no regulation or policy discouraging employees from storing personal papers and effects in their offices.

Because the factual record established to the court's satisfaction that Dr. Ortega had a reasonable expectation of privacy in the context of his desk and file cabinets in his office, the court was able to outline the parameters of a reasonable search in the workplace. Of course in the criminal context a valid search warrant is essential except in very limited circumstances. But, as the court observed, the only cases to imply that a warrant is required involved searches that were not work

related. So the court was initially left to determine whether a search warrant is required for searches by public officials of public employees' work spaces. Against the legitimate privacy interests of public employees, the court concluded it had to balance "the realities of the workplace." Workplace realities strongly suggest that the warrant requirement is an unworkable mechanism. That is so because employers must frequently enter the offices and desks of their employees for legitimate work related reasons wholly unrelated to things like investigative processes. This is in sharp contrast to the criminal searches which are conducted for the purpose of gathering evidence and which do not normally have other more benign explanations. For example, an employer may need to review correspondence or reports or obtain files which are available only in an employee's office when the employee is away or they may need to safeguard or identify property or records in connection with a pending investigation into suspected misconduct. In the court's view "requiring an employer to obtain a warrant whenever the employer wished to enter an employee's office, desk, or file cabinets for a work related purpose would seriously disrupt the routine conduct of business and would be unduly burdensome." Indeed, the court expressed its concern that government would cease to function if every employment decision became a constitutional matter.

Although warrants in the criminal context issue, if at all, upon a showing of probable cause, the court concluded that probable cause is too high a standard for workplace searches. Instead, the governmental interest in the efficient and proper operation of the workplace sufficiently authorizes intrusions, and is important enough to give public employers wide latitude to enter offices for work-related non-investigatory reasons as well as for searches conducted pursuant to investigations of work-related misconduct.

In sum, according to the Court, searches of public employees must be justified under a standard of reasonableness both in the inception of the search and in the scope of the intrusion, so long as the question relates to employment (non-criminal) investigations. A search will be justified at its inception when there are reasonable grounds for suspecting that it will turn up evidence that the employee is guilty of work related misconduct or that the search is necessary for a non-investigatory work related purpose. A search will be permissible in scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the claimed misconduct.

Quon v. City of Ontario, 130 S.Ct. 2619 (2010) further defined privacy expectations in employment. In 2001, the City of Ontario, California provided alphanumeric pagers to certain members of law enforcement to help them mobilize and respond in emergency situations. Although the pagers were not directly addressed in separate policies, the City had a computer usage, internet and email policy putting employees on notice of the City's right to monitor and log all email and internet use. While that explicit language did not apply to the text messaging which uses different technology, employees were told that the same principles would apply. Nevertheless, when the City audited some of the text messages, employees complained and the Ninth Circuit concluded that there was a reasonable expectation of privacy in the text messages and that even a search for legitimate work-related reasons was not reasonable in scope because there were less intrusive means that the department could have used. The Supreme Court disagreed, concluding that the search for the text messages was reasonable. Although the opinion did not expand previously established principles, it did make a number of points clear:

- The Fourth Amendment applies when the government acts in its capacity as employer. Searches must be evaluated against the operational realities of the workplace in order to determine whether Fourth Amendment rights are implicated and the employee's reasonable expectation of privacy must be addressed on a case-by-case basis. If an employee has a legitimate privacy expectation, an employer's intrusion for non-investigatory work-related purposes or work-related misconduct must be judged by the standard of reasonableness. These are the factors emanating from *O'Connor v. Ortega*; the *Quon* court recited them, noted that they represented the plurality, and suggested that the court is still not certain whether the plurality approach is the right one.

- The court must proceed cautiously in considering Fourth Amendment implications of emerging technology "before its role in society has become clear." Rapid changes in technology, and the lack of a clear understanding as to what society accepts as proper behavior, have a bearing on how a court might view a situation and workplace norms should contribute to that analysis, if they have developed.

- Cases may be resolved without determining whether an employee had a reasonable expectation of privacy. The special needs of the workplace may justify an exception to the warrant requirement, particularly where there is a non-investigatory work-related purpose or the investigation of work-related misconduct. In such a case the employer must justify the search at its inception and adopt measures reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search.

In the *Quon* case the Court made short work of justifying the search at the inception. There were reasonable grounds for suspecting the search was necessary because employees had vastly exceeded the number of text characters allowed and the City was among other things attempting to determine whether the contract with its character limitation was appropriate. This was a legitimate work-related reason, and the public employer had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related texting or, on the other hand, that the City was not paying for extensive personal texting.

The court also felt that the scope of the search was reasonable. It was efficient and expedient. Even though the plaintiff had gone over his monthly allotment many times, his employer requested only two months worth of transcripts. Moreover, the employer redacted all messages that the employee sent while off duty "a measure which reduced the intrusiveness of any further review of the transcripts."

The Ninth Circuit had viewed the standard as requiring an employer to adopt the least restrictive alternative (529 F.3d 892 (9th Cir. 2008)). The Supreme Court refused to accept that as a guiding principle, noting that it had repeatedly refused to declare that only the "least intrusive" search is reasonable under the Fourth Amendment.

THE RIGHT TO CONSENT

Warrantless searches may of course be authorized by consent. In an employment environment the question of who has the right to consent could be of great consequence in a subsequent criminal proceeding. *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007), later opinion on denial of rehearing at 497 F.3d 890 (9th Cir. 2007), establishes some ground rules. An employee who had used his workplace computer to view child pornography challenged introduction of the evidence from the computer; it was critical evidence supporting his conviction. The dispute was set in motion when the owner of the internet service provider who provided service to the employer contacted the FBI to identify that the employee had accessed child pornography websites from a workplace computer. The FBI worked with the business' IT administrator. The company's IT department placed a monitor on the computer to record internet traffic and spot checked to confirm that the employee's activity involved viewing images of child pornography. The company regularly monitored workplace computers and made sure employees were aware of that activity.

Whatever the instructions from the FBI might have been, the employer entered the employee's private office (having obtained the key from a company executive), and made two copies of the hard drive of his office computer. At about the same time, the company's corporate counsel advised the FBI that the company would cooperate fully in the investigation and voluntarily turned the computer to the FBI. This communication explicitly stated that a search warrant would be unnecessary and, accordingly, the FBI did not obtain a warrant.

When the trial court denied a motion to suppress the evidence from the computer, the employee entered a written plea agreement conditioned upon his right to appeal the denial of the motion to suppress. Those arguments were made to the Ninth Circuit which concluded that the search was proper. Even though the employee retained a legitimate expectation of privacy in his workplace office, the employer retained the ability to consent to a search of his office and his business computer. As a result, because a valid third party consent to the search was given, the evidence was properly before the court.

The opinion outlined the analysis in logical steps:

- The Fourth Amendment protects people, not places. Even though for most people computers are private spaces, the validity of that expectation depends entirely on the context.

- A criminal defendant may invoke the protections of the Fourth Amendment only if he can show he had a legitimate expectation of privacy in the place searched or the items seized.

- The use of a password on a computer and a lock on a private office door are sufficient evidence of a subjective expectation of privacy.

- Any subjective expectation of privacy must also have been objectively reasonable. This employee's expectation was objectively reasonable because his office was not shared by

coworkers and was kept locked. Even though there was a master key, the existence of a master key will not necessarily defeat a reasonable expectation of privacy and in an office given over for personal use.

- A computer assigned to an employee located outside of a private office, coupled with corporate policies of monitoring, may not allow for an objectively reasonable expectation of privacy; this issue was not, however, decided.

- A well settled exception to the requirement that there be a valid search warrant is a search done on valid consent obtained by the government.

- Consent given by a third party who possesses common authority over or other sufficient relationship to the premises or effects sought to be inspected is sufficient.

- Even where a private employee retains an expectation that his private office will not be searched, such interest may be subject to the possibility of an employer's consent to a search of the premises which it owns.

- The employer could validly consent to a search of the hard drive of the workplace computer because it is the type of workplace property that remains within the control of the employer even if the employee has placed personal items in it. Even though the computer was subject to an individualized log in, the company through its IT department had complete administrative access to anyone's computer and had installed a firewall to monitor internet traffic from the organization. Monitoring was routine and employees were apprised of the monitoring through training and a policy in the employee manual. Employees were also told computers were company owned and not to be used for activities of a personal nature.

Efforts to present the case for rehearing *en banc* were rejected. Three concurring judges joined in an opinion clarifying the facts.

The order denying rehearing en banc was accompanied by a dissent in which 11 judges joined. Those judges would have drawn a distinction between a policy that allows an employer to monitor the computer, and what happened in this case which is that the employer consented to a warrantless physical search by criminal law enforcement agents. The dissenting judges had this to say about the implications of employer monitoring of employee computer use:

> "Plainly put, it is preposterous to conclude, as the panel opinion does, that an employer's policy of remote electronic monitoring of its employees' computer use either (1) constitutes express authorization by an employee for the company to give consent to law enforcement to conduct a physical search for a computer in the employee's locked private office or (2) establishes mutual use and joint access over such an office. We should have taken the case en banc to correct the panel's erroneous holding regarding an

> employer's ability to consent to a search of an employee's workspace, and to provide certainty in the law so that employers and employees can structure their behavior accordingly." 497 F.3d 890 at 897 (2007).

EVALUATING THE EXPECTATION OF PRIVACY

Magistrate Stewart's exhaustive analysis of employee expectations of privacy is a helpful starting point for anyone attempting to understand the legal issues. The analysis appears in *Thygeson v. U.S. Bancorp*, 2004 W.L. 2066746 (D.Or. 2004). Thygeson was terminated after eighteen years of employment after the employer discovered inappropriate materials he accessed on his workplace computer. His manager received reports from some of Thygeson's subordinates that he was sending emails with inappropriate attachments. Those complaints led to a request from the internal systems analyst to provide a report showing internet activity over an extended period of time so that company management could determine if Thygeson was using his office computer for business purposes or otherwise. Management also asked for a search of the network drive to determine if he had saved any pictures on the employer's computer network. The report produced a listing of internet sites that Thygeson had visited, which was created by network resources (and did not involve entering Thygeson's office). A quick calculation suggested that Thygeson was spending an average of four hours a day visiting internet sites on his work computer, something that his job did not require. Systems also searched the network drive for photographs and that search resulted in evidence of inappropriate emails containing pictures of nudity and sexually offensive jokes that he had saved on the network drive.

Of no small importance in Magistrate Stewart's analysis were the company policies concerning the use of computer equipment at work. She excerpted:

> U.S. Bancorp's Employee Handbook states: "Our ... personal computers, ... including e-mail, ... are intended for Company business only." Harvey Aff (June 18, 2004), Exhibit 1, p. 7. The Handbook also states: "Do not use U.S. Bancorp computer resources for personal business" and "Do not access inappropriate internet sites and do not send e-mails which may be perceived as offensive, intimidating, or hostile or that are in violation of Company policy." *Id* at 8. Furthermore, it adds: "Like voice mail, computer systems or other office equipment, e-mail is the exclusive property of U.S. Bancorp and is not intended for personal use." *Id.* With respect to monitoring, the Handbook states:
>
> U.S. Bancorp reserves the right to monitor any employee's e-mail and computer files for any legitimate business reason, including when there is a reasonable suspicion that employee use of these systems violates ... a company policy, or may have an adverse effect on the Company or its employees. Examples include but are

> not limited to e-mails containing sexual innuendo or off-color jokes; ... [or] excessive or unauthorized use that violates Company policy. *Id* at 9.
>
> In a section entitled "Privacy in the Workplace," the Handbook states:
>
> U.S. Bancorp may assign workspace, equipment, or other company property for use in performing your job accountabilities. Company property is not intended for personal use. U.S. Bancorp reserves the right to access and/or search workspace and equipment that has been assigned to you.... U.S. Bancorp reserves the right to monitor employee accounts and electronic forms of communication, including e-mail, telephones, computer systems, and other electronic records for any legitimate business reasons. *Id* at 10.

Among his other claims, Thygeson sued for invasion of privacy, claiming that the computer searches resulted in an intentional intrusion upon his solitude or preclusion or private affairs done in a manner that would be highly offensive to a reasonable person. Thygeson argued that he had a reasonable expectation of privacy in these materials since they were saved in his "personal" folder on his work computer and some were saved after he accessed them through his personal email account, which he had accessed from his office computer hardware but using internet access to reach his personal email account.

The court rejected arguments that Thygeson had a reasonable expectation of privacy in the contents of his personal folder on the company network. He used his employer's computer and network for personal use and saved personal information in a location that could be accessed by his employer, despite warnings in the handbook that personal use was prohibited and monitored. The employer provided the computer, internet access, and the network. "Thygeson could not have a reasonable expectation of privacy in anything he chose to put in the network folder to which U.S. Bancorp retained the key."

Thygeson had not password-protected his materials, but even password protection would probably not have created an expectation of privacy under these circumstances. That was so because he was specifically warned that office computers were not for personal use and activity on them could be monitored.

In contrast to the situation in ***Thygeson***, other factual circumstances might create a reasonable expectation of privacy. For example, a search of a computer in a private office to which an employee had exclusive use might be invasive. In ***Leventhal v. Knapek***, 266 F.3d. 64 (2nd Cir. 2001), an employee of a state agency alleged his Fourth Amendment rights were violated when the agency searched the hard drive of his office computer. The computer was in a private office. It was not shared. The public and visitors did not have access to the computer. Any maintenance was done with advance notice and, when other employees searched unattended computers, such searches were infrequent and only for selected documents. Moreover, the

agency did not have a general practice of searching office computers and nobody had placed the employee on notice that he should have no expectation of privacy in the contents of his office computer. The same was true in ***Restuccia v. Burke Tech***, 1996 W.L. 1329386 (Mass. Super. 1996). There again, there was no policy against using the office's email system for personal messages, employees were never told supervisors had access to their email using supervisory passwords, and there was no information about any files being saved into locations to which supervisors had access.

A Wisconsin case, ***Fischer v. Mt. Olive Lutheran Church***, 207 F.Supp.2d 914 (W.D. Wis. 2002), added an interesting twist when the church employer accessed the content of the individual's email account by guessing at his password. In that case, the court denied summary judgment because "it is disputed whether accessing plaintiff's email account is highly offensive to a reasonable person" and "whether plaintiff's email account is a place that a reasonable person would consider private."

In the employment setting, a number of factors can contribute to creating an expectation of privacy, or creating circumstances in which an expectation of privacy is subjectively unreasonable. Factors to evaluate include the following:

- The degree to which fellow employees, supervisors, subordinates, guests and/or the general public may have access to work space.

- Whether the object of the search is secured within luggage, a briefcase, a purse or other enclosure.

- Whether the employee has brought in something not work related and likely to be viewed as private (purse, briefcase, gym bag).

- The nature of the workplace, such as whether employees must have security clearances.

- Whether the object of the search is confined to issues pertinent to the workplace, or instead has as its objective the gathering of evidence for criminal proceedings.

- The existence of policies and their content.

- Whether the employee has taken some special steps to keep the material private or protected such as, for example, secret passwords (even those installed in contravention of an employer policy).

- Whether or not the employee can limit access through the use of keys or other physical security.

- Circumstances suggesting the employer has given the employee permission or authority to use equipment for personal reasons.

- Whether computer data is stored stand alone on a hard drive or other media, or network.

SOME PRACTICAL RESPONSES

Clear workplace policies that define equipment use and privacy rights are valuable to employers who find themselves caught in the middle between law enforcement and employee rights. When no policies are in place, or when the policies don't quite address the question adequately, employers are safest when searches are authorized by a valid warrant.

Employers who find themselves needing to respond immediately to the presence of law enforcement personnel may be able to buy a little bit of time before turning over computer equipment or allowing searches of the contents in those circumstances in which a warrant is not presented. For example, the employer can negotiate to keep custody of the computer equipment, prepare a ghost image of the hard drive, and turn off the employee's access to the system temporarily. This would also allow law enforcement time to obtain a valid search warrant, hopefully without the risk that pertinent data will be lost. As always, it is good to have something in writing that confirms there was a discussion and agreement.