Window Peeping in the Workplace: A Look into Employee Privacy in a Technological Era

Donald H. Nichols

Follow this and additional works at: http://open.mitchellhamline.edu/wmlr

Recommended Citation
Available at: http://open.mitchellhamline.edu/wmlr/vol27/iss3/11

This Article is brought to you for free and open access by the Law Reviews and Journals at Mitchell Hamline Open Access. It has been accepted for inclusion in William Mitchell Law Review by an authorized administrator of Mitchell Hamline Open Access. For more information, please contact sean.fellofer@mitchellhamline.edu.
© Mitchell Hamline School of Law
WINDOW PEEPING IN THE WORKPLACE:
A LOOK INTO EMPLOYEE PRIVACY IN A
TECHNOLOGICAL ERA

Donald H. Nichols†

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>I. INTRODUCTION</td>
<td>1588</td>
</tr>
<tr>
<td>II. A PROBLEM OF IGNORANCE?</td>
<td>1588</td>
</tr>
<tr>
<td>III. PRIVACY AT RISK</td>
<td>1589</td>
</tr>
<tr>
<td>IV. EMPLOYERS MONITOR EMPLOYEES.</td>
<td>1590</td>
</tr>
<tr>
<td>A. How It Is Done</td>
<td>1591</td>
</tr>
<tr>
<td>B. Why It Is Done</td>
<td>1591</td>
</tr>
<tr>
<td>V. PERSONAL HOME COMPUTERS</td>
<td>1592</td>
</tr>
<tr>
<td>A. In the Context Of Telecommuting</td>
<td>1593</td>
</tr>
<tr>
<td>B. In The Context Of Litigation</td>
<td>1593</td>
</tr>
<tr>
<td>C. Employer-Owned Home Computers</td>
<td>1594</td>
</tr>
<tr>
<td>VI. THE LAW</td>
<td>1595</td>
</tr>
<tr>
<td>A. The Common Law Seems To Govern The Issue</td>
<td>1595</td>
</tr>
<tr>
<td>B. The Common Law In Minnesota</td>
<td>1597</td>
</tr>
<tr>
<td>VII. RECENT LEGISLATIVE ATTEMPTS TO ADDRESS THE PROBLEM</td>
<td>1598</td>
</tr>
<tr>
<td>VIII. DISCOVERY ISSUES</td>
<td>1600</td>
</tr>
<tr>
<td>A. Discovery Of Electronically Stored Information</td>
<td>1600</td>
</tr>
<tr>
<td>B. Northwest Airlines v. Local 2000</td>
<td>1601</td>
</tr>
<tr>
<td>IX. EMPLOYEES MUST TAKE STEPS TO PROTECT THEIR PRIVACY</td>
<td>1602</td>
</tr>
<tr>
<td>X. NEW TECHNOLOGY WILL BRING NEW PROBLEMS</td>
<td>1603</td>
</tr>
<tr>
<td>XI. TECHNOLOGICAL ADVANCES CALL FOR AFFIRMATIVE LEGAL ACTION</td>
<td>1605</td>
</tr>
<tr>
<td>XII. SUMMARY</td>
<td>1607</td>
</tr>
</tbody>
</table>

† Donald H. Nichols, the founding partner of the law firm of Nichols Kaster & Anderson, practices in the area of employment litigation. Mr. Nichols serves as chair of the Technology Committee for the Minnesota State Bar Association and has presented numerous seminars concerning technology and the law. The author would like to thank his friends and colleagues Douglas A. Hedin and Maurice W. O’Brien for their insights, and his law clerk, Heidi A. O. Fisher for her assistance in the writing of this article.
I. INTRODUCTION

If an employee has a computer terminal at his job, it may be his employer's window into his workspace. In the modern workplace, most employees have a "personal computer" or PC. These computers often contain the most personal information and thoughts of the operator. However, the owner of the PC is the employer. As our dependency on the personal computer increases, should employees take steps to protect their privacy? Do employees have any privacy protection in the workplace?

The purpose of this article is to discuss the various ways in which our personal and professional lives are intertwined in cyberspace, where anyone can "window peep" into them. It will first introduce the problem and discuss the various means with which employers monitor their employees. Next, it will look at the current state of the law, as well as discuss a recent decision in Minnesota. Finally, it will suggest ways for employees to protect their privacy against the peering eyes of their employers. This article discusses technology that may be obvious to some. However, as different members of the legal community have different levels of technological skill, it bears repeating.

II. A PROBLEM OF IGNORANCE?

Most employees who have computers at work often check their e-mail first thing in the morning, about the same time they sort through their postal mail. In both cases, they likely assume that they are the first, and only, person to be reading the contents. This is because reading someone else's mail can be illegal.

In the case of e-mail, an employee may feel the added security of entering his password as a means of retrieving his mail which reinforces his belief that his e-mail is private. Unfortunately, he is wrong. Reading employee e-mail, from a different computer terminal and without the employee's consent, is technologically possible, often entirely legal, and routinely practiced by employers to

1. Anne L. Lehman, E-mail in the Workplace: Question of Privacy, Property or Principle?, 5 COMM.LAW CONCEPTUS 99, 99 (1997). In her article, Lehman's opening paragraph sets forth a typical workplace scenario. Id.

2. Birnbaum v. United States, 588 F.2d 319, 319 (2nd Cir. 1978). In Birnbaum, suit was brought under the Federal Tort Claims Act by individuals whose letters to and from the Soviet Union were opened and photocopied by the CIA. The plaintiff's were awarded $1,000 each in compensatory damages. Id.
monitor their employees.⁵

The problem is that many people view use of their employer’s e-mail system the same as making a telephone call, and subsequently feel the e-mail messages they send on their company’s internal system should be free from intrusion. Indeed, they are likely to converse freely over the e-mail system, talking about a range of topics in an open and frank manner. If something is written and an employee does not want it inadvertently seen, they mistakenly believe that they can simply “delete” the message.

Many employees are under the false assumption that when they “delete” or “trash” a message, that is in fact what has actually occurred. On the contrary, deleting a message often merely changes the location where the message was stored, and ultimately, an employer may still retrieve those “deleted” messages.

Information deleted from a personal computer is generally easily recoverable, whether from the machine’s hard drive or elsewhere.⁴ Use of the “delete” button on a computer does not destroy the information, but merely hides it from view.⁵ A personal computer can betray confidences by failing to destroy files that its users sought to remove by use of a “delete” button.⁶

Likewise, most employees do not know that it may be possible, at any time in the future, to retrieve a list of all websites visited. This may be done one month or ten years in the future. Whether an employee checks his stocks or the weather, or accidentally clicks on a link that takes them to a pornographic website, his computer’s memory is busy filing away these nuggets of information about his computer usage.

III. PRIVACY AT RISK

Privacy is quickly becoming a concern to internet users. There are news stories of hackers, of people using credit card numbers from the internet, and a host of other invasions. Indeed, users have a reason to be concerned. Soon most everything will be connected through internet protocol. The internet is a network of linked devices including the millions of personal computers that

---

3. Lehman, supra note 1, at 102.
4. Id.
6. Id.
are connected to it. Computers pose a substantial threat to user privacy because they may render vast amounts of personal data instantly accessible to strangers. When tied to a network, an individual's personal computer makes access to the internet available at her desk.

Users leave extensive data trails which may seem anonymous, but which can be linked to a person later. For example, while at this point in time it may pose a challenge to discover information about an ancestor, in the future an individual may be able to easily ascertain and acquire information about a person, even down to the internet sites they visited. Subsequently, issues arise in dealing with privacy issues and where that privacy line should be drawn.

Because of this technological minefield, it is important for users to understand what happens when they click their mouse or hit the enter key. Internet use is not the same as making a private phone call because of federal rules prohibiting wire-tapping. When one breaks the telephone connection, the words are gone. There is little fear that the conversation had in confidence has been monitored. If that conversation took place though e-mail, or even in a letter drafted but never sent, she may have just stepped on a landmine.

IV. EMPLOYERS MONITOR EMPLOYEES

It is fast becoming a fact of life, employers monitor employees' use of technological equipment. We have entered a time when the amount of information that can be obtained about an employee increases with every keystroke of the employer's computer. "The rapid development of information technology and the mass availability of information have the potential to [completely] eclipse an employee's right to privacy in the workplace."

In a 1999 survey of nearly a thousand large companies, it was reported that 45% of them monitored their employees' e-mail, computer files, and phone calls. Almost two-thirds reported some

8. Schwartz, supra note 5, at 1622.
9. Id. at 1617.
10. Mike Tonsing, Privacy in the Cyberian Workplace, 46 FED. L. 42, 42 (June 1999).
type of electronic monitoring.\textsuperscript{12}

A. How It Is Done

Employers monitor employees in a number of ways. Generally, the employer is allowed to monitor employee activity including telephone calls and e-mail and computer use. Moreover, new technologies make it possible for employers to monitor many aspects of their employees' jobs, especially on telephones, computer terminals and through electronic and voice mail. Employers can use computer software that enables them to see what is on the screen or stored in the employees' computers. Generally, since the employer owns the computer network and the terminals, she is free to use them to monitor employees. Frighteningly, some computer monitoring equipment allows employers to monitor without the employees' knowledge.

Typically, if an e-mail system is used at a company, the employer owns it and is allowed to review its contents. Electronic and voice mail systems retain messages even after the messages have been deleted. While it appears that they are erased, they may be permanently "backed up" on magnetic tape, along with other important data from the computer system.

B. Why It Is Done

Employers may have legitimate business interests justifying some employee monitoring. "In twenty-five years, I believe everyone will be under surveillance ... [p]eople will see surveillance as reducing the cost of doing business and permitting more truth to come out."\textsuperscript{13} By allowing employees internet and e-mail access, employers are opening themselves up to potential harassment claims. Many sexual and racist jokes float around in cyberspace, and if one finds its way onto a company computer, it may be forwarded to other employees. The content of the e-mail may become the basis of a lawsuit.\textsuperscript{14} In one case, an employer was the subject of

\textsuperscript{12} Nichols: Window Peeping in the Workplace: A Look into Employee Privacy in Published by Mitchell Hamline Open Access, 2001

\textsuperscript{13} Pink Slip, N. Y. TIMES, Dec. 16, 1999, at E1.

\textsuperscript{14} Steiner v. Showboat Operating Co., 25 F.3d 1459, 1463 (9th Cir. 1994)
six harassment claims because an employee downloaded the contents of an adult bulletin board onto the company's computer system.\textsuperscript{15}

Employers are also concerned about loss of productivity. In an article in the Wall Street Journal, an Internet retailer stated that 65 percent of its orders are placed during work hours and "spike" during the lunch hour.\textsuperscript{16} Since this traffic drops dramatically on the weekends, the obvious conclusion is that many employees are shopping online during the workday when they are supposed to be working.\textsuperscript{17} A recent survey showed that employees at three different companies collectively spent "the equivalent of 350 eight-hour workdays accessing the Penthouse Magazine Web site in a single month."\textsuperscript{18}

In addition to lawsuits and loss of productivity, companies are also concerned with other harmful situations, such as loss of trade secrets and contracting e-mail viruses. For example, one strain of computer virus caused an estimated damage of $80 million. Increased personal use of a company's computer systems may render a company more vulnerable to these disasters. Employers argue that without monitoring systems in place, they cannot protect themselves. Given the employee's privacy concerns, and an employer's legitimate business needs for some control over their systems, a solution that would provide the perfect balance of rights and expectations remains elusive.

V. PERSONAL HOME COMPUTERS

At home, on a personal computer, a user bears many of the same types of risks to privacy when he goes on to the internet as he...
bears when he logs on at work. The difference being, of course, that his employer has no right to monitor what the employee does in the privacy of his own home and has no right to inspect his home computer—or does she?

We tend to feel safe in our own homes and see them as the one place that is completely off limits to our employer. We can vent our professional frustrations to others without the fear that someone will overhear. But sometimes, our employer can intrude on our sanctuary in the normal course of our employment. One such situation is telecommuting.

A. In The Context Of Telecommuting

With the rise in technology, many companies have realized that allowing employees to telecommute makes business sense. Employees can log on to the company network from home, and complete their work from there. In employment situations where the employee does not have to be physically present at the office to do his job, the company can save the money of providing workspace for that employee.

However, for the employee, it is a gray area in the realm of privacy. Once he logs onto his employer’s network, his employer may have access to his “private files” stored on his home computer. The employer should not have a legitimate business need to examine these files, but nevertheless, the employee may be vulnerable to employer snooping. Employers know that in order to telecommute, an employee must have the tenacity to keep on task and not succumb to urges to do housework or cut the lawn. Employers may be able to monitor what an employee is doing on their home computer if logged on to the network, but should they? Or is that stepping over the line?

B. In The Context Of Litigation

What happens when an employee becomes involved in litigation with his employer? In a recent decision by the U.S. District Court in Minnesota, a magistrate judge granted a motion allowing an employer to inspect and copy an employee’s personal home computer. 19

Northwest Airlines was involved in litigation with Local 2000, its airline attendants' union. The attendants allegedly held a "sick-out" in which a large number of them called in sick on the same day(s). Northwest claimed this was an attempt to cripple the airlines and propel them to meet demands in an ongoing contract negotiation. Northwest sought to inspect an employee's home computer because it believed the event was planned via e-mail. The magistrate judge allowed it.

C. Employer-Owned Home Computers

Sometimes, as a benefit of a position at some public or private entity, the employer will supply the employee with a home computer. Although the employee may not really be a "telecommuter," their employer will provide him with a home computer on which to gain access to the company system, write, and do personal business. This arrangement is commonplace with institutions of higher learning, such as colleges, universities, and law schools.

Indeed, this was the practice at Harvard Divinity School when, in 1998, the dean was asked to resign because of his computer use in the privacy of his official residence. The dean's home computer was owned by the school, and when he required more memory, the school's technician came to his residence to bring him a new computer and transfer his files. During the course of the transfer, the technician noticed large amounts of pornographic material that had been downloaded from the internet.

The technician reported the pornographic downloads to his supervisor, and the dean was asked to resign. Although the dean browsed the internet and downloaded these pictures in the privacy of his own home, and on his own time, the president of the university nevertheless decided that the dean was now unfit to keep his employment. Of course, in this particular case, the argument can be made that the viewing of pornographic sites is inconsistent with

(granting motion in a suit against union for alleged illegal "sick-out" seeking e-mail communications of union members purportedly planning these activities).

20. Id.
21. ROSEN, supra note 11, at 159.
22. Id.
23. Id.
24. Id.
25. Id.
the morals and values portrayed by the divinity school. However, it serves to illustrate how precarious a position an employee may find himself in if his employer learns about his private, legal computer activities in the home.

VI. THE LAW

A. The Common Law Seems To Govern The Issue

As with many new things, the law is lagging far behind technology, and is in an ever-present state of "catch-up." Presently, an employee’s right to computer privacy is largely governed by state tort law. There are four distinct torts protecting the right to privacy: intrusion upon seclusion, appropriation, publication of private facts, and false light publicity. The tort most relevant to e-mail interception by employers is the unreasonable intrusion upon the seclusion of another. 26

The critical issues to examine when determining employer tort liability for monitoring or intercepting employee e-mail messages are: (1) does the plaintiff have a reasonable expectation of privacy and, if so, (2) was there a legitimate business justification for the intrusion sufficient to override that privacy expectation. 27 These principles were handed down in 1987 in the leading Supreme Court decision, Ortega v. O’Connor. 28

In Ortega, the matter involved a public employer who searched an employee’s office for evidence that he may have sexually harassed women. Without distinguishing between private and public property, the employer’s investigators found and read personal letters, and seized them along with other things including photographs, appointments books and an unpublished book. 29

In writing for the majority opinion, Justice O’Connor held that the amount of privacy that employees can legitimately expect in different parts of the workplace varies with how much privacy they actually experience. For example, O’Connor explained that public

27. Id.
employees' expectations of privacy in their offices, desks, and file cabinets may be reduced by virtue of office practices, procedures or regulations. Pushed to its logical extreme, as long as the employer takes steps to reduce an employee's expectation of privacy, they can all but eradicate their right to privacy in the workplace. Then, however, the balancing of employer's justifications for instruction will always tip in his favor.

Following from O'Connor's line of reasoning, whether an employer's monitoring of an employee's computer use would violate an employee's common law right to privacy seems to depend upon unique circumstances. Central to the determination is the employee's development of a reasonable expectation of privacy with respect to her use of the computer system. Unfortunately, since the employer usually owns the computer system, courts generally hold that employees have no expectation of privacy while using them.

Further, employers can justify the monitoring of workers if employees are informed of surveillance policies beforehand. In many cases, employers print their monitoring policies in employee handbooks, or go as far as requiring employees to sign a waiver as a condition of employment. Such advance notice places the employer in a stronger position to argue that its employees do not have a reasonable expectation of privacy in their e-mail messages and thus avoids having to rely on the court's own notion of what privacy expectation is reasonable. However, there is a problem

32. O'Connor, 480 U.S. at 715. Justice O'Connor in O'Connor states that "[w]e have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable." Id. In 1993, the Supreme Court decided Harris v. Forklift Systems, 510 U.S. 17, 17 (1993). Harris was a sexual harassment case in which Justice O'Connor, again writing for the majority, laid out a two pronged test to determine if the harassment would violate Title VII. This test employed both objective and subjective standards. Not only must an employee feel subjectively harassed, but the conduct must be such that an objective, reasonable person would also view the conduct as severe or pervasive enough to create a hostile or abusive environment. Id. at 21-22. This objective/subjective test may lend itself well to an analysis of reasonable expectations of privacy in the workplace.
34. Id. (citing Ny, Son of the Polygraph, ACROSS THE BOARD, June 1989, at 21-22).
with this practice. On the typical first day of work, employees are bombarded with forms to sign and papers to read. An employee may sign the employee handbook or waiver without much thought, only to be held to that standard later on.

Without clear policies, most employees proceed under the misconception that their personal and business communications on business time and equipment remain private. However, even when employers promise to respect the privacy of e-mail, courts are upholding their right to break promises without warning.  

In fact, in cases involving e-mail sent from work, courts are increasingly holding that employees have little expectation of privacy. This may be because of Justice O'Connor's reasoning in *Ortega*: "as long as network administrators have the technical ability to reach their employees' e-mail, employees should have no reasonable expectation that their e-mails aren't being read." Rather than giving private e-mail the same legal protections as private letters, courts are increasingly treating e-mail as if it were no more private than a postcard.

**B. The Common Law In Minnesota**

In 1998 the Supreme Court of Minnesota finally recognized a common law right to privacy in *Lake v. Wal-Mart Stores, Inc.* In that case, two young women filed a complaint against Wal-Mart when they learned a Wal-Mart employee was circulating a photograph of the women nude. They alleged the four traditional invasion of privacy torts. The Court held that the right to privacy existed in the common law of Minnesota, including causes of action in tort for intrusion upon seclusion, appropriation, and publication of private facts.

In *Wal-Mart*, the Court discussed how the tort of invasion of privacy was rooted in a common law right to privacy, and how as
society changes over time, the common law must also evolve.\textsuperscript{43} In recognizing the tort of invasion of privacy, the Court decreed that the right to privacy is an integral part of our humanity, and that the heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.\textsuperscript{44} In light of the Court's ruling, time will tell if the Minnesota courts will find invasion of personal electronic information a type of privacy interest worthy of protection.

VII. RECENT LEGISLATIVE ATTEMPTS TO ADDRESS THE PROBLEM

The fourth amendment of the United States Constitution protects citizens' privacy by prohibiting the government from conducting unreasonable searches and seizures of citizens' property.\textsuperscript{45} This privacy protection applies to public employers and prevents them from conducting certain searches in the public workplace.\textsuperscript{46} This theme has been expanded, and now includes the concept that employees in the private sector have reasonable expectations of privacy from their employers as well.\textsuperscript{47}

In the late 1980's, Congress amended the Federal Wiretap Act by passing the Electronic Communications Privacy Act ("ECPA").\textsuperscript{48} The ECPA makes intercepting electronic communications illegal.\textsuperscript{49} However, it distinguishes between intercepting electronic communications while it is in transit and when it is in storage.\textsuperscript{50} Employees should note that the ECPA provides two exceptions from liability

\textsuperscript{43} Id. at 234.
\textsuperscript{44} Id. at 235.
\textsuperscript{45} Thomas P. Klein, \textit{Electronic Communications in the Workplace: Legal Issues and Policies}, 563 PLI/PAT 693, 729.
\textsuperscript{46} O'Connor v. Ortega, 480 U.S. 709 (1987) (holding that employees have a reasonable expectation of privacy in the workplace). The court addresses privacy concerns of both public and private employees. They cautioned, however, that these expectations could be reduced by actual office practices and procedures, or by legitimate regulation. \textit{Id.} at 717.
\textsuperscript{47} \textit{Supra} note 31 and accompanying text.
\textsuperscript{48} Electronic Communications Privacy Act, 28 U.S.C. \textsection 2810 (2000). The amendment was so significant that the entire act is now generally referred to as the ECPA. McGuire, \textit{supra} note 16, at 5.
\textsuperscript{49} 28 U.S.C. \textsection 2810 (2000).
\textsuperscript{50} \textit{Id.} Compare Title I and Title II. \textit{See also} Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (holding that seizure of a computer, used to operate an electronic bulletin board system, and containing electronic mail which had been sent to the bulletin board, but not read by intended recipients, was not an unlawful intercept under the Federal Wiretap Act).
for employers who monitor their employees' e-mail.

First, the provider of an electronic communication service may retrieve information maintained on that provider's system. What this means for the employer is that, if it operates its own internal email system for its employees, it would be able to access information stored on that system without violating the ECPA.

Second, the ECPA allows access to stored electronic communications when the access was authorized by a user of the system; for example, when the employee has given consent. This may come into play where, as previously noted, an employer has an employee sign a waiver as a condition of employment, or inserts its monitoring policy into the employee handbook and the employee signs an acknowledgement of receipt.

Of course, it may be the case that the ECPA may not apply at all. A federal district court has held that private employers who do not provide electronic communication services "to the public" are not liable under the ECPA for monitoring communications on their system.

Minnesota has its own version of the ECPA. The state language is substantially the same as the federal ECPA. However, no cases to date have involved the statute in the employment context.

Minnesota also has a statute under the criminal code that makes it a crime to "window peep." As applied to a workplace environment, this statute prohibits conduct such as installing surveil-

53. 18 U.S.C. § 2701(c)(2)(2000); see also Am. Computer Trust Leasing v. Jack Farrell Implement Co., 763 F. Supp. 1473, 1493 (D. Minn. 1991) (holding that a software vendor who used a modem to access customer's system did not violate Title II of the ECPA because the customer authorized the access in the license agreement).
57. MINN. STAT. § 609.746. "A person is guilty of a misdemeanor who enters upon another's property ... [and] peeps in the window ...." MINN. STAT. § 609.746, subd. 1(a) (1987).
lance equipment in restrooms and locker rooms. Even in the absence of this or similar statutes, cases involving this type of conduct may be the only "intrusion upon seclusion" cases that an employee is likely to win against an employer.

VIII. DISCOVERY ISSUES

A. Discovery Of Electronically Stored Information

In the modern age of computers, we store a magnitude of information electronically. In many cases, it is the sole location of that information. As our reliance on networked technology increases, it will become more and more important to be allowed access to that information for litigation purposes.

"[I]t has become evident that computers are central to modern life and, consequently, also to much civil litigation. As one district court put it in 1985, 'computers have become so commonplace that most court battles now involve discovery of some computer-stored information.'"

Federal Rule of Civil Procedure 26(b)(1) allows discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending litigation to include "books, documents, or other tangible things." Rule 34 seems to aid an interpretation that this includes electronic data, providing that a party may serve a request for, among other things, "data compilations from which information can be obtained, translated ... by the respondent through detection devices into reasonable usable form." In addition, the Manual for Complex Litigation provides clear authority for discovery of computerized information stating:

The potential benefits that may be derived from computerized data ... are substantial both in the discovery process and at the trial .... Accordingly, a party may be required

58. MINN. STAT. § 609.746, subd. 1 (d) (1987).
59. S. Elizabeth Willborn, Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace, 32 GA. L. REV. 825, 844-46 (1998). Intrusion on seclusion suits rarely succeed, except in the most egregious cases because employees have difficulty proving that the workplace is a sufficiently private area to create reasonable expectations of privacy. Id.
61. FED. R. CIV. P. 26(b)(1) (emphasis added).
not only to furnish pre-existing hard copies of computerized data, but also to provide new printouts of pertinent items or of data in machine readable form ....

Courts have decided that "today it is black letter law that computerized data is discoverable if relevant."68

B. Northwest Airlines v. Local 2000

In Northwest Airlines, a magistrate judge allowed the discovery of an employee's home computer.64 Accompanying the magistrate's order, he issued a document setting forth the protocol for inspecting and copying the hard drive of the computer.65 The protocol in the order is a tacit recognition of the inherent risk of granting the discovery in the first instance. While allowing a copy to be made of the entire hard drive, it limits inspection, directing "you shall not read or review Data on the equipment which does not fall within the discovery period and does not relate to the persons or subject matter listed."66

Although this directive is given, it may be impossible to determine what is or is not relevant without reading unrelated, possibly highly personal information. Included on a personal computer may be all facets of health, marital, sexual orientation, hobby and personal preference information. All of an individual's private thoughts may be on display for others to comb through. Much of this data may be irrelevant to the pending litigation, but embarrassing or damaging to the person if known to others.

Rule 26(b) compels discovery of relevant information, or information reasonably calculated to lead to the discovery of admissible evidence.67 Rule 34(a) provides that a party has a right to inspect and copy "any designated documents", or to inspect and copy any tangible things which constitute or contain matters "within the scope of Rule 26(b)."68 By insisting that discovery be limited to

64. Supra, note 19 and accompanying text.
66. Id. at ¶ 5.
67. FED. R. CIV. P. 26 (b).
68. FED. R. CIV. P. 34 (a).
relevant, or “reasonably calculated to lead to admissible” information only, the rules attempt to limit the type of intrusion the Northwest magistrate has allowed to occur. Since an entire copy of a personal hard drive was allowed to be taken, the potential for abuse of the process is great.

IX. EMPLOYEES MUST TAKE STEPS TO PROTECT THEIR PRIVACY

Employees need to be aware of the current legal climate and how it affects them. Given that presently courts have been upholding an employer’s right to monitor employees at will, employees should take affirmative steps to protect their privacy.

First, employees should limit the amount of personal business they do at work. Where most employees usually spend more than half of their waking hours at work, this is not an easy task.

Making personal phone calls on breaks from personal cell phones instead of company phone lines will reduce the likelihood of company intrusion. Along those same lines, bringing a personal laptop to work may ensure that an employer will not be able to monitor it, since it is not her property. It is important to remember, however, that if an employee hooks his personal computer into the employer’s network system, he may be monitored. It may make sense to save use of a personal laptop for personal business, if it needs to be done.

Employees should instruct friends not to send personal e-mails to a work e-mail address, especially e-mails containing sexual or racist jokes. If a company is monitoring employees and it notices an employee receives these types of e-mails often, he may be targeted for extensive surveillance. If an employee does receive these types of e-mail, he should not forward them under any circumstances.

In light of the law’s “expectation of privacy” benchmark, employees should do what they can to establish a reasonable expectation of privacy. Although at least one court has allowed monitoring even when employees have been told they will not be monitored, 69

69. In Smyth v. Pillsbury Co., a federal court ruled in favor of the employer when an employee brought suit for invasion of privacy. Smyth v. Pillsbury Co., 914 F.Supp. 97, 97 (E.D.Pa. 1996). The employer had told its employees that their e-mail was confidential and would not be used as a basis for discipline, but later fired an employee for sending inappropriate and unprofessional e-mail messages to his supervisor. The court found that the employer owned all of the equipment and, therefore, that the employee had no reasonable expectation of privacy.
establishing a reasonable expectation of privacy may, at least, compel an employer to notify an employee if he is going to be subject to monitoring.\textsuperscript{70}

While an employer should not normally have access to an employee’s personal home computer, we have seen that in some situations, all bets are off. The most beneficial thing a user can do for himself is to understand how his computer works, and where the information goes when it is deleted. By periodically and permanently erasing embarrassing personal information from his hard drive, he may be able to avoid the airing of dirty laundry in the course of litigation.

Just as technology has created a new host of privacy problems, technology may provide some answers to those problems as well. For instance, the problem with e-mail is that it is becoming infinitely searchable and infinitely retrievable.\textsuperscript{71} However, technology now exists that allow a sender to encrypt his e-mail messages so that it can’t be read unless it is decoded.\textsuperscript{72} In addition, there are now sites on the internet that allow users to send encrypted e-mail without leaving any records that can be subpoenaed or searched.\textsuperscript{73} Some websites allow users to view other websites through a separate “cloak” site, which has the effect of allowing an employee to view web pages without his employer knowing anything but that he is viewing the “cloak” site.\textsuperscript{74} As surveillance technology becomes more and more advanced, there will be technologies developed to preserve employees’ right to privacy.

X. NEW TECHNOLOGY WILL BRING NEW PROBLEMS

The suggestions mentioned may help to preserve some modicum of privacy for employees, but only if they are consciously aware of monitoring and take steps to protect themselves. Unfortunately, future computers will make it less likely that employees will even be

\begin{itemize}
\item Moreover, the court ruled that the employer’s interest in preventing misuse of e-mail outweighed the employee’s expectations of privacy. \textit{Id.}
\item \textsuperscript{70} \textit{Infra} note 83 and accompanying text.
\item \textsuperscript{71} ROSEN, \textit{supra} note 11, at 173.
\item \textsuperscript{72} \textit{Id.}
\item \textsuperscript{73} \textit{Id.} One such cite is ZipLip.com. \textit{Id.}
\item \textsuperscript{74} ROSEN \textit{supra} note 11 at 174. An example is Anonymizer.com. \textit{Id.} However, this will be of no use if your employer is monitoring you by viewing exactly what is on your screen at any given time, as opposed to monitoring a list of sites you visit.
\end{itemize}
aware of the technology around them. The Sensor Fusion project is one example of how this may happen.\footnote{Erica Rowell, \textit{Turned On and Jacked In-Computer’s Future Lies in Making Its Physical Presence Less Known,} at \url{http://www.abcnews.go.com/sections/tech/CuttingEdge/cuttingedge.html}.}

The Sensor Fusion project is focusing on microelectromechanical systems, or MEMS, which is a technology that mixes computers with tiny devices like sensors embedded in chips.\footnote{Id.} The purpose of the MEMS is to develop ways to fold computer tasks into the environment.\footnote{Id.} This technology will involve day-to-day interaction with things we don’t think of as computers.

An employee who is careful about the ways in which he uses his company’s e-mail system, but not as careful about other areas of his work environment because he does not consider them to be subject to monitoring might be surprised to learn the extent of his employer’s invasion.

The computers themselves are getting “smarter.” IBM's “Blue Eyes” research project is developing software that makes it possible for a computer to “know” when someone is looking at its screen.\footnote{Id.} The computer accomplishes this by taking pictures of the room and, using a highly technical method, detects human retinas.\footnote{Id.} If a computer can detect if someone is looking at its screen, it goes without saying that the computer will probably be able to transmit that information to an employer. Therefore, not only will an employer know what is on his employee’s screen, she will be able to tell if he is looking at it, or if he is on an extended break. It might be possible to find out \textit{just how much time} an employee spent working on that proposal, or if “the light was on but nobody was home.”

Soon, “Blue Eyes” technology may be used in cars to detect drowsy drivers.\footnote{Id.} Will an employer someday be able to tell how efficiently an employee is working by monitoring his level of alertness while looking at the computer screen? Should his employer know if he had difficulty sleeping the night before? As the law stands today, as long as his employer gives notice that he is subject to monitoring, there may be no expectation of privacy in the methods they
use to monitor, or the information they may be able to glean.\textsuperscript{82}

XI. TECHNOLOGICAL ADVANCES CALL FOR AFFIRMATIVE LEGAL ACTION

The legal face of the technological conundrum is currently being viewed by the courts. Of the three branches of government, the courts have been challenged with the legal issues involved more than the others. As a theoretical matter, this has its advantages. For instance, attorneys and judges are used to dealing with privacy issues. In our adversarial system, new common law can be formed from new twists on old problems. Likewise, these players are adept at making constitutional inquiries and arguments and fighting to protect the rights of citizens.

Conversely, this branch of government sometimes moves too slowly. Issues are not decided in days or weeks, but they may take years. Keeping up with the new technological advances and the new legal issues they create seems a task that our court system is ill-equipped to handle. It may be time to take more positive steps in addressing the issues, and a more active role in keeping up with new problems as they occur.\textsuperscript{83}

For example, currently, privacy issues in the workplace are defined by the common law "reasonable expectation of privacy" threshold. As computers become more and more a part of our everyday lives, to the point where most people are not consciously aware of them, it may become more difficult for any employees to assert an expectation of privacy, just as it becomes easier for em-

\textsuperscript{82} Another related, and very controversial issue, is DNA testing. The mapping of the human genome opens up a world of opportunities in medical and disease research. \textit{Will Cracking The Code For DNA Crack Employee Privacy?} EMPLOYMENT AND LABOR LAWCAST, Vol. VI, No. 16, 2 (2000). However, there are serious fears that it could lead to genetic discrimination by health insurers and employers. \textit{Id.} In fact, President Clinton has already issued an executive order banning genetic discrimination against federal employees. \textit{Id.} The dangers to employee privacy here are self-evident.

\textsuperscript{83} In the context of unions, there has been a lot of talk about protecting their members' rights to privacy in the realm of technological monitoring by negotiating protections in collective bargaining agreements. To date, in Minnesota at least, no such agreements exist. Part of this may be due to the fact that, as opposed to the Minnesota courts, arbitrators in labor disputes have been recognizing employees' rights to privacy in the workplace for many years. The Minnesota Supreme Court only recently decided \textit{Wal-mart}. \textit{Supra} note 40 and accompanying text.
employers to infringe on it.

To keep up with the daily advances in technology, our legal system might look to its legislative branch for change.84 However, even the legislative branch may move too slowly for the new technological legal issues. A good start would be to analyze, objectively, the current law and make changes to fit the true nature of the situation.85 It should not be enough to have a paragraph in an employee handbook reciting that “the computer systems are company property and subject to monitoring.”

In order to legitimately remove an employee’s expectation of privacy, there should be a statutorily mandated “counseling” session in which an employer representative explains the company policy, and what exactly is subject to monitoring. As in Minnesota’s Drug and Alcohol Testing in the Workplace Act, a form should be developed and signed by the employee that indicates they have received and understood this information.86

In addition, lawmakers should scrutinize the ownership/expectation of privacy relationships. Just because an employer owns the computer an employee works on, that alone should not be the test of reasonable expectation of privacy. The logical extreme of this analysis would dictate that an employer could read a private note written on company paper with a company pen. Indeed, as the cost of technology decreases, the dichot-

84. On July 20, 2000, legislation was introduced in both houses of Congress which would require companies to tell employees if they monitor their computer, Internet or telephone use. ACLU Applauds Bipartisan Legislation To Protect Employees’ Privacy, at http://www.aclu.org/news/2000/n07200b.html. The bill would only require that employers provide annual notice of monitoring. Id. In actuality, what the bill seems to be proposing is simply to require companies to notify employees that they have no expectation of privacy. However, the Bill does offer some protection against monitoring without notice. Employers who violate the law would be subject to paying damages, up to $20,000 per employee and $500,000 per incident. Id.

85. Some states, such as Wisconsin, have legislated a right to privacy. Wis. Stat. § 895.50 (1996). However, this particular statute, while recognizing a right to privacy, provides that the right of privacy recognized “shall be interpreted in accordance with the developing common law of privacy.” Id. Consequently, while recognizing a claim for invasion of privacy, the legislation does nothing to protect employees above what the courts have already done. Id.

86. MINN. STAT. § 181.953 (4) subd. 6 (1993). “Before requesting an employee or job applicant to undergo drug or alcohol testing, an employer shall provide the employee or job applicant with a form, developed by the employer, on which to acknowledge that the employee or job applicant has seen the employer’s drug and alcohol testing policy.” Id.
omy between the computer and the pen and paper will decrease as well. Even the laws against window peeping appreciate that although an employer may own an employee restroom or locker room, there are areas of our lives that must remain private.

The Legislature should keep abreast of new technology and anticipate the problems and abuses that can arise. By legislating privacy protections, less harm will come to employees who suffer in the process of waiting for the court system to address intrusions into privacy by overstepping employers who were free to intrude because “there was no law against it.”

XII. SUMMARY

It is indisputable that privacy is a basic American value, one whose importance has become increasingly challenged in the information age. It is surprising how recent changes in law and technology have been permitted to undermine sanctuaries of privacy that Americans have long taken for granted. The privacy issue has become so much more evident in the computer age that we tend to forget that privacy problems existed before computers. What computers have done is to make the invasion of privacy faster and more efficient.

Indeed, traditional “window peeping” is taken very seriously, and our criminal justice system has addressed the situation by making it a crime. It is unfortunate that a similar invasion of privacy is overlooked merely because it is technologically perpetrated.

Modern technological efficiency does not come without a price, and that price may be a loss of privacy. However, we can’t place blame on technology for our privacy problems; the decision to gather data about people is not made by the computer, but by the people behind the computer system. Thus, there is a range of technological, legal and political responses that might help us rebuild in cyberspace some of the privacy and anonymity that we demand in real space.

Currently there are few laws regulating employee monitoring. Our system of laws, stemming from common law, does not react quickly enough to the almost daily technological change. Courts and legislatures are one step behind in interpreting and creating laws that will adequately reflect the interaction between computer technology and society. Our legal system must recognize the problem and outline a framework in which balance can be struck be-
tween employees’ privacy interests and the employers’ legitimate interests in using technology to monitor employee productivity and effectiveness.

A uniform workplace privacy law, consistently enforced, may be the only adequate means of protecting individuals in this age of technological innovations. Until that time, private citizens and employees must take steps to protect themselves from the intrusions of others.