Employers Association of New Jersey
A nonprofit association serving employers since 1916

Workplace Monitoring After Stengart v. Loving Care Agency

John J. Sarno, Esq.

April 14, 2010

For Discussion Only

In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology evolve, the line separating business from personal activities can easily blur.

In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy.

In a first impression case, the Supreme Court of New Jersey in *Stengart v. Loving Care Agency, Inc.*, held that company policies do not convert an employee's emails with her attorney - sent through the employee's personal, password-protected, web-based email account, but via her employer's computer - into the employer's property. This decision limits the ability of employers to claim that an employee's personal communications conducted from employer-owned property are no longer private and available for the company's review.

In this case, a discharged employee filed a lawsuit against the company, asserting various claims including violations of New Jersey's Law Against Discrimination. Prior to getting fired, but unknown to the company, she used a laptop computer provided by the company to send emails to her attorneys via her personal, web-based, password-protected Yahoo email account.

After the discharged employee sued, the company extracted and created a forensic image of that laptop's hard drive. As a result of this process, the company's attorneys were able to discover and review many emails between the employee and her attorneys. It was only months later, after discovery commenced and the company was required to respond to requests, that the company informed the former employee and her counsel that it had reviewed these emails. After protracted legal argument, a trial judge found that the employer's electronic communications policy put the employee on notice that her emails would be viewed as company property and, therefore, not protected by the attorney-client privilege.

An appellate court reversed and remanded the lower court's decision. The New Jersey Supreme Court took case for review.

The Supreme Court reviewed various versions of the company's electronic communications policy and found it problematic for the company. The court's primary concern was that the company asserted that the employee's emails with her attorneys were not private, even though she sent them via her personal web-based Yahoo email account. The trial court viewed the company's policy as an adequate warning to employees that there would be no reasonable expectation of privacy in any communications made using company laptops or servers regardless of whether the email was sent via a company email account or a personal web-based email account. The appellate court, however, pointed to language in the policy permitting some personal use and found that an objective reader of that language could have reasonably believed that personal emails with her attorney would be permitted.

The Court also reviewed the way courts have historically viewed employer-issued workplace regulations and found that such regulations should concern the terms of employment and reasonably further the legitimate business interests of the employer. Though many aspects of the policy were specific enough to aid the company in conducting its business, the court found that the company's overbroad interpretation of its electronic communications policy reached into the employee's personal life without a sufficient connection to the employer's legitimate business interests. The company's ownership of the computer that the employee used to send emails to her attorney was not enough to convert those emails into company property. An employer may discipline or terminate an employee who is engaging in business other than the company's business during work hours, the court said, but that right does not translate into a right to confiscate the employee's personal communications.

This decision appears to be limited to an employee's use of her personal email account to communicate with her attorney. Courts have enforced clear electronic communications policies and have often held that employees do not have a reasonable expectation of privacy when they Some decisions have applied this view to communications between an employee and his attorney but this decision chips away at this line of cases. How far courts will go is not clear, but employers can expect challenges that rely on the appellate court's opinion. The Stengart court emphasized the need for clear and unambiguous policies. Therefore, employers should adopt electronic communications policies if they do not have them or review existing policies for inconsistencies and ambiguities.

As a communications media, e-mail has figured prominently in several high-profile employment cases. For example, Citibank, one of the nation's largest financial institutions, was recently sued by African-American employees who discovered that e-mail messages containing racial and ethnic "jokes" were being circulated among managers at corporate headquarters. They have alleged that the offensive electronic message created a hostile work environment. Also, two African-American employees sued Morgan Stanley for harassment based on race. In this case, the employees alleged that a white employee sent an e-mail that contained racial comments, using the electronic password of a black employee.

Generally, employers are liable for employee conduct that violates the rights of others and that occurs within the scope of the employment relationship. Such is the case when a supervisor unlawfully discriminates against or harasses a subordinate. While using e-mail to harass an employee presents a unique problem, communications via e-mail are no different than verbal or non-verbal communication. While the harassment suit against Morgan Stanley was eventually dismissed, it was because the content of the electronic message did not rise to the level of harassment, not because the electronic communication was excluded from the law. Therefore, as a practical matter electronic communications should be included in a company's harassment policy.

Electronic communications, like all communications in the workplace, reflect a company's culture and environment. The reality is that employees often engage in an e-mail subculture that forwards jokes and pictures freely. The problem with "point, click, send" is that electronic messages multiply effortlessly and information is difficult to control. An e-mail policy with clear guidelines is one way to limit liability exposure.

Privacy in the workplace is not an absolute right and there are business justifications for invasions of personal privacy. For example, employers must ensure safety of employees, protect against sabotage, protect intellectual property, and protect themselves from harassment suits; not to mention preventing lost productivity due to online shopping. Indeed, monitoring employees' online activities is a growing issue. A recent report issued in 2001 by the Privacy Foundation found that about 35% of workers in the United States with regular online access are under generalized electronic surveillance. Further, the rate of surveillance has been increasing about twice that of the number if employees with Internet access.

In most cases, employees' expectations of privacy are lowered with a written policy. Such policies put employees on notice of electronic monitoring and, therefore, their continued employment constitutes consent to such a condition. Implied consent can also be given for monitoring stored electronic mail. Additionally, such monitoring can occur without the consent of employee, if it occurs within the regular course of business and the employer has a "legal interest" in the communication, such as to determine whether an employee is disclosing confidential trade secrets. However, such nonconsensual monitoring must be limited in time and purpose. The scope of the exception may not include personal communications. So the best policy is to have a policy.

The first step in developing a policy is to recognize that e-mail is considered a "document" by court rules. As a document, e-mail is subject to litigation discovery, subpoena, search warrants and Freedom of Information Act requests. After suit has commenced, "deleting" relevant or embarrassing e-mail may constitute a violation of court rules or, in a criminal proceeding, obstruction of justice. Don't forget, even deleted e-mail messages usually can be retrieved. It is important, therefore, that employees understand that they should act with appropriate care, attention and decorum when composing and sending e-mail. Conversational or casual e-mail can easily be misunderstood. For example, in both the Microsoft antitrust litigation and the American Home Products fen-phen litigation, e-mails have provided "smoking guns" for prosecutors and plaintiffs.

As a company record, e-mail should be retained in accordance with the organization's records retention policy. Employees must be informed that all electronic messages are company property, that there is no right to "ownership" simply because an employee composed and sent an electronic message, and that employees do not have any privacy interest in any communication created or sent in a company computer, or received by a company computer.

Companies may prohibit electronic soliciting, although the practicality of enforcing such a policy should be thought through carefully. For example, policies requiring that the computer systems are to be used *only* for business reasons, but that are not enforced for birthday, wedding or other personal messages, may open a company open to allegations of unfair labor practices or selective/discriminatory enforcement.

Employers may also adopt written monitoring policies. These policies can include monitoring of e-mail and general internet activity. Employers that do not adopt expressed, written monitoring guidelines and that do not make sure that each employee is aware of the policy can face invasion-of-privacy claims, wrongful termination suits and, possibility, criminal penalties.

Many companies monitor electronic communications. An effective electronic media policy should educate employees about the proper use of company systems, as well as create the legal justification for employee discipline. Moreover, it is essential that the policy diminish any expectation of privacy. No model policy will fit every company since needs will vary according to the nature of the company business and culture. At a minimum, however, a basic policy should address the following:

• Does the policy apply equally to all employees? The scope of the policy should be clear and state, if appropriate, which employees will have e-mail or Internet access.

• Will the company monitor all or some electronic communications? If so, will monitoring be random or based on some reasonable suspicion of wrongdoing?

• Will the policy incorporate other policies or standards? If so, will the company's harassment or non-solicitation policies be incorporated or cross-referenced?

• Will employees be permitted to use their own software for business purposes? If so, will the company permit them to treat that software as personal property?

• Will employees be permitted to use e-mail for limited personal reasons, such as birthday announcements or the sale of a car? If so, where does the policy draw the line between limited and excessive personal use?

• Who enforces the policy? Will it be enforced consistently or selectively?

It is clear that while employers will be able to monitor emails, they will have to tread lightly on those that are "personal" particularly if the emails are covered by the attorney-client privilege.