EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *April 2010*

Company and its Outside Counsel are Barred from Reading Personal E-Mail Messages Between Employee and Her Attorney

As email has become the dominant mode of workplace communication, employers have attempted to make clear through written policies that there is no expectation of privacy when one utilizes company-provided computers and internet systems. Many of these policies should now be rewritten if they are applicable in certain states.

Martin W. Aron, Partner

Barbara A. Lee, Counsel

In addition, employers and their counsel should approach certain kinds of email review and monitoring with great caution, as shown by a recent decision. In a case that has garnered national attention, the New Jersey Supreme Court has barred a company and its outside counsel from reviewing an employee's attorney-client communications that were sent utilizing a company laptop. *Stengart v. Loving Care Agency, Inc. (NJ Supreme Court, A-16-09, March 30, 2010)*

Facts of *Stengart* Case

In *Stengart*, the company had issued a laptop computer to Maria Stengart, the Executive Director of Nursing. Stengart used the company laptop to exchange emails with her attorney using her personal, password-protected Yahoo account rather than her company email account. Unbeknownst to Stengart, the laptop's software captured a "screen shot" of every web page accessed by the user of that computer, and stored these images in temporary internet files. When Stengart resigned from the company, she returned the laptop. She then filed a discrimination lawsuit against the company.

During discovery in litigation, the company asked a forensic expert to recover the files on the laptop that Stengart had used. The experts were able to image the hard drive, which permitted her outside counsel and the company to obtain and review the email communications to and from her attorney before she resigned. When the attorney-client communications were produced to Stengart's attorney, her counsel objected to this intrusion and demanded that all copies of such communications be returned. They sought a court order demanding the return of all of the emails as well as the disqualification of the company's outside counsel who viewed the communications.

The trial court declined Stengart's request for relief, finding that the employer's written policy sufficiently placed Stengart on notice that her emails would be considered company property. On appeal, the New Jersey Appellate Division reversed the trial court's order and directed outside counsel to turn over all copies of the emails and delete any record of them. Thus, before any trial on the merits of Stengart's discrimination claims, the New Jersey Supreme Court was asked to determine whether the emails were protected by the attorney-client privilege and whether the company or its outside counsel violated Stengart's expectation of privacy in the emails, and applicable ethics rules.

The Supreme Court's Decision

The Supreme Court examined whether the company's computer use policy provided sufficient notice that personal emails created on a personal web-based email account but sent from a company computer were subject to review by the company. The Court affirmed and modified the Appellate Division finding that Stengart could reasonably expect that the email communications forwarded to her lawyer would remain private and "that sending and receiving them via a company laptop did not eliminate

the attorney-client privilege that protected them."

Moreover, by reading emails that were at least arguably privileged and failing to notify Stengart promptly about them, Loving Care's counsel violated applicable attorney ethics rules (RPC 4.4(b)). The case was remanded to the trial court "to determine what, if any, sanctions should be imposed on counsel for Loving Care." Such sanctions might include disqualification from representing Loving Care in the litigation, screening of attorneys who read attorney-client emails, imposition of costs or other remedies.

In reviewing the company's policy, the Court determined that the policy failed to give sufficient warning to employees that it applied to personal emails created and sent through a personal, web-based email account rather than the company's own email system. Specifically, the policy did not mention how emails sent using an employee's personal email account would be treated. Nor did the policy inform employees that the company's software system captured images of every email message sent and received, allowing the company to retrieve such messages. Furthermore, the policy's express allowance of occasional personal use of the company's computers and email system created ambiguity with respect to whether personal emails were personal property or company property.

The Court next addressed whether the company had invaded Stengart's privacy by retrieving and reading the privileged emails. In order to find that the company had committed an "intrusion on seclusion," one form of the common law tort of invasion of privacy, Stengart had to show that she had both a subjective and an objective expectation of privacy in the emails to and from her attorney. The Court noted that Stengart's use of her personal email account to communicate with her attorney, and her decision not to save the password for her Yahoo account on the company's laptop computer, were reasonable attempts by Stengart to keep her messages confidential, and thus supported her claim of subjective expectation of privacy. Moreover, the Court's finding that the company's computer use policy was ambiguous gave Stengart an objectively reasonable expectation of privacy in her communications.

Furthermore, the emails contained language making it clear that they were protected by the attorney-client privilege. Sentences at the end of each email from Stengart's attorney contained standard language stating that the message was intended only for the addressee, was personal and confidential, and might be subject to the attorney-client privilege. In response to the company's claim that Stengart had waived the attorney-client privilege by using the company's laptop computer, the Court replied that the company's policy was insufficiently clear to permit a conclusion that Stengart had engaged in any such waiver, which must be "clear and unequivocal" under applicable law.

The Court made it clear that employers may continue to limit their employees' use of computers, internet access, and email accounts as a legitimate attempt to protect company equipment and information. Employers may also limit the amount of time that employees spend using company computer equipment or internet access for personal reasons. The Court found, however, that "employers have no need or basis to read the specific contents of personal, privileged, attorney-client communications in order to enforce corporate policy." In fact, added the Court, even if an employer had a policy that unambiguously banned *all* use of the company's computers and internet access for personal reasons, and provided clear notice that the employer could retrieve and read communications between an employee and his or her attorney using a personal email account via the company's computer system—such a provision would not be enforceable in court.

Implications for Employers and Their Counsel

It is important to remember that this case involves one specific type of communication: messages between an attorney and a client. As such, attorneys will be bound by applicable ethics rules when one comes into possession of such communications. The Court makes it clear that employers can continue to limit employees' computer and internet use as long as there is a business justification for such a limitation. The case suggests the following considerations when developing or modifying a computer use policy:

In reviewing the company's policy, the Court determined that the policy failed to give sufficient warning to employees that it applied to personal emails created and sent through a personal, web-based email account rather than the company's own email system. Specifically, the policy did not mention how emails sent using an employee's personal email account would be treated.

1. Ensure that the computer use policy is written clearly and uses words that individuals who are not knowledgeable about information systems will understand. Terms such as "media systems" may not communicate clearly to employees what the employer is talking about.
2. Establish a clear policy stating that any messages created on or sent through the company's computer network and/or company-owned computers (including laptops and personal data devices issued to an employee) are subject to monitoring, and that employees have no expectation of privacy in such communications.
3. Notify employees at least annually of this policy. The policy should make it clear that "monitoring" occurs not only as the computer is used, but at any later time as well.
4. Consider creating a similar message that appears each time the employee logs onto the company's Internet or e-mail system.
5. Consider prohibiting employees from accessing websites or other electronic information that is not related to the company's business needs.
6. If applicable, include in your policy a statement that the company's computer system captures "screen shots" of a) all communications using the company's computers, even if not connected to the company's Internet service system and even if using a personal e-mail account and b) all communications using the company's e-mail system, even if created on a non-company owned computer.
7. Before reviewing allegedly "private" employee e-mail, go through the following steps:
   - review the actual language of the company's computer use policy
   - make sure that the employee received and signed a statement acknowledging receipt and understanding of the policy and that a copy has been retained
   - ascertain whether the company has allowed private use of computers by employees without attempting to monitor or halt the practice
   - ascertain whether the computer use policy has been enforced
   - consult legal counsel concerning the advisability of whether the e-mail can be reviewed.

Finally, counsel should always be mindful of ethics rules that apply when they come into possession of communications between an employee and his or her lawyer.

The Court made it clear that employers may continue to limit their employees' use of computers, internet access, and email accounts as a legitimate attempt to protect company equipment and information. Employers may also limit the amount of time that employees spend using company computer equipment or internet access for personal reasons.

Boston MA | Ft. Lauderdale FL | Hartford CT | Madison NJ | New York NY | Newport Beach CA | Providence RI
Stamford CT | Washington DC | West Palm Beach FL | Wilmington DE | London UK | Hong Kong (associated office)

Martin W. Aron, Partner 973.520.2315 maron@eapdlaw.com
Barbara A. Lee, Counsel 973.520.2308 blee@eapdlaw.com