

NJ Supreme Court: Employers May Reserve Right Via Specific Policies to View Most 'Private' Employee E-Mails Sent on Company-Owned Computers

MATTHEW V. DELDUCA | DELDUCAM@PEPPERLAW.COM

MAUREEN Q. DWYER | DWYERM@PEPPERLAW.COM

The New Jersey Supreme Court recently handed down a landmark decision dealing with the vexing question of when an employer has the right to monitor and access personal e-mails and other electronic communications by employees using computers owned by their employers. The court ruled that employers may implement policies prohibiting or limiting personal communications on company computers, and employers may discipline employees for violating those policies. The court also ruled that employers may review the substance of most private e-mail and computer communications, but only if the employer has implemented and communicated a detailed policy that effectively eliminates any reasonable expectation the employee may have that his or her computer communications are private. Finally, the court held that employers are never free to review the substance of certain communications, in particular an employee's confidential communications with his or her lawyer.

In *Stengart v. Loving Care Agency, Inc.*, A-16-09, 2010 N.J. LEXIS 241 (Mar. 30, 2010), Marina Stengart used her company-issued laptop to exchange e-mails with her lawyer relating to an employment discrimination lawsuit she was contemplating filing against her employer. Although she used the company-issued laptop, Stengart sent these e-mails via her personal Yahoo account, which was protected with a password. After Stengart quit her job and filed a lawsuit against her employer, the company hired an expert in computer forensics to recover all the files stored on Stengart's company laptop. Among the e-mails recovered were Stengart's communications with her lawyer. Stengart's lawyer asserted that the attorney-client privilege applied to these e-mails and demanded their return. Loving Care

refused to return them, relying on the company's written policy that any communications made on a company computer belong to the company.

In *Stengart*, the court was faced with two issues: (1) the extent to which employers may access personal e-mails sent by employees on company computers via password-protected accounts, and (2) whether the employer may, via a policy, reserve the right to view communications that would otherwise be protected by the attorney-client privilege. Ultimately, the court found that no matter what the employer's policy provides, an employer may never access the substance of employee communications protected by the attorney-client privilege. This ruling is based on the strong public policy concerns supporting the privilege. An important point for New Jersey employers, however, is that the *Stengart* decision also provides specific guidance to employers and courts on two much broader issues: (1) whether employers may implement and enforce policies governing personal use of company computers, and (2) when employers may access the substance of personal communications on company computers.

The *Stengart* decision clearly provides that employers are free to implement policies that prohibit or limit personal use of company computers. Employers are also free to monitor the extent of employees' personal computer use and to discipline employees whose use violates company policy.

Stengart also provides helpful guidance on the issue of when employers may review the *substance* of an employee's personal e-mails and other computer usage. The court noted that New Jersey, like many states, recognizes a cause of action for intrusion

This publication may contain attorney advertising.

into privacy. Unlike most states, New Jersey's state constitution also gives employees in the private sector a right of privacy in the workplace. Under both legal theories, the employee's right to privacy extends to those areas where the employee has a "reasonable expectation of privacy." As a result, employers have always been well-advised to eliminate any "reasonable expectation of privacy" by adopting policies informing employees that they should not expect communications they make on company computers, servers or networks to be private.

In *Stengart*, the Supreme Court focused extensively on the adequacy of the notice provided by the employer's electronic communications policy. The *Stengart* employer's policy was similar to policies implemented by many New Jersey employers and employers around the country. The employer's policy stated that communications on company computers belong to the company and that such communications are not private. The policy also provided that "occasional personal use" of computers was permitted. Like most employer policies, the company's policy provided no detail about the various ways in which the employer could access personal communications, including password-protected communications. The Supreme Court found that the employer's policy did not provide enough detail about the employer's ability to access communications to remove the employee's reasonable expectation of privacy, particularly when using a password-protected account.

As a result, the *Stengart* case drives home that employers that wish to reserve the right to access the substance of employees' personal computer communications in the workplace must have clear policies that provide employees with details about what communications are prohibited and what communications may be monitored. It is essential to implement and communicate those policies to employees in advance. Unfortunately, very few New Jersey employers have policies that would pass muster under the stringent standard articulated in *Stengart*.

Following the *Stengart* decision, New Jersey employers should review their electronic communications policies. Policies must clearly articulate whether personal use of company computers is permitted, and if so, any limitations on such usage should also be clearly defined. In addition, employers that wish to reserve the right to review the substance of personal employee communications on company computers or servers should implement policies that provide significant detail on the ways that access may occur. Finally, company personnel or outside contractors who are asked to monitor or access an employee's personal e-mails should

be trained on the scope of the employer's and the employee's rights relating to those communications.

For any questions regarding electronic communications policies and the right of privacy, please contact the authors.

RSS on www.pepperlaw.com

SUBSCRIBE TO THE LATEST PEPPER ARTICLES
VIA RSS FEEDS. VISIT WWW.PEPPERLAW.COM
TODAY AND CLICK ON THE RSS BUTTON ON
THE PUBLICATIONS PAGE TO SUBSCRIBE TO
OUR LATEST ARTICLES IN YOUR NEWS READER.
