Proskauer

New Jersey's High Court Ruling Reaffirms Employer's Right To Monitor and Restrict Computer Use -- Provides Guidance for Effective Internet Usage Policies

April 5, 2010

On March 30, 2010, the New Jersey Supreme Court issued a much-anticipated ruling concerning the extent to which employers can monitor and restrict their employees' personal use of company computers. In *Stengart v. Loving Care Agency, Inc.*, __ N.J. __, __ A.2d __, 2010 WL 1189458 (2010), the Court addressed a narrow set of facts – emails sent by an employee from a company laptop via a web-based email account (Yahoo) to her attorney – and determined that they were protected from disclosure by the attorney-client privilege. In reaching this conclusion, the Court also ruled and provided insight on a far broader and more practical issue for employers – namely, how to draft enforceable computer usage policies and/or make existing policies more effective.

The case concerned Marina Stengart, the former Executive Director of Nursing for Loving Care Agency, Inc., (Loving Care), a provider of home-care nursing and health services. Stengart received a laptop computer from Loving Care to conduct company business. Stengart eventually left her employment, returned the laptop, and filed an employment discrimination lawsuit against Loving Care and others. In an effort to preserve electronic evidence for discovery in the litigation, Loving Care hired experts to create a forensic image of Stengart's laptop's hard drive. Among the items retrieved were temporary Internet files containing emails Stengart had exchanged via a personal, password-protected web-based email account with her lawyer.

Throughout the proceedings, Loving Care argued that Stengart had no expectation of privacy concerning her emails with her lawyer because they were sent and received from a company laptop over the company's computer system, and Loving Care maintained a written Internet usage policy that warned all employees that the company reserves the right to intercept and disclose "all matters on the company's media systems" at any time without notice. Following opinions from courts in Massachusetts and New York, the Supreme Court disagreed with Loving Care and held that the emails sent from her personal, password-protected email account were absolutely privileged from disclosure [1]—regardless of the company's comprehensive prohibition on personal Internet use. While significant from a litigation perspective, the opinion provides far more practical guidance for employers concerning their computer use policies.

Making Your Company's Internet Usage Policy Enforceable

While *Stengart* makes clear that the attorney-client privilege protects email communications between an employee and her private legal counsel, the Court also confirmed that New Jersey employers may adopt—and enforce—lawful policies relating to computer use. Even though the ruling only has a bearing on New Jersey-based entities, all employers can benefit from this decision by making your company's Internet usage policies more comprehensive.

1. Design your Internet usage policy to protect your business. The Court observed that companies can adopt policies relating to computer use "to protect the assets, reputation, and productivity" of your business and to "ensure compliance with legitimate corporate policies." Personal emails or other communications which divulge confidential or proprietary information or otherwise impugn the good will of the organization can be expressly prohibited.

2. Notify employees that *all* workplace computers may be monitored. *Stengart* recognizes that employers may monitor and regulate the use of company computers. Employees should be told that this monitoring may include office and laptop computers, whether used on company property, at a home office, or at another remote location.

3. Warn employees that the Internet usage policy covers *all* personal emails. Employers can alert employees that every email they send or receive is subject to review by the company. This warning may expressly apply to all emails sent and received over company computers, servers, or other equipment. Importantly, this provision can also cover those emails sent and received through company equipment via personal, password-protected web-based accounts, such as Gmail, Yahoo, Hotmail or the like.

4. Alert employees that deleted personal emails may be recovered. *Stengart* also suggests that employees be expressly warned that the contents of their personal emails may be stored on company hard drives and/or forensically retrieved and read by the employer.

5. Advise employees that all company email is property of the company. To resolve any ambiguity about whom "owns" personal email, employees should be told in unequivocal terms that no email should be considered private or personal and that all emails, without exception, are the sole property of the company.

6. Enforce your policy. *Stengart* recognizes that employers can discipline or terminate employees for violating the Internet usage policy. By way of example, an employee known to spend too much time during the workday sending and receiving personal emails (even with her private lawyer) may be disciplined for violating a policy permitting only occasional personal use of the Internet. Likewise, an employee may be disciplined for the transmittal of emails that contain illegal or inappropriate material that might harm the company in some way.

7. Note the law applicable to your out-of-state employees: The *Stengart* ruling applies to employees who perform work in New Jersey. It is unclear, however, if the holding will govern the communications of employees of a New Jersey-based business who are physically located in other states. This is important because there is no universal consensus among the very few states to have addressed this issue. If your employees are physically located in a state that has not considered this issue, or one that has addressed—and rejected—the conclusion reached in *Stengart*, your business may have even more leeway in monitoring and examining the email traffic of out-of-state employees.

While a total ban on personal email usage may be impractical (or impossible), a post-*Stengart* Internet usage policy should sufficiently convey that the company is, in essence, "looking over your employees' shoulders" as they send and receive emails. Providing such express notice will make it difficult for an employee to plausibly argue that she (like Stengart) was unaware that her email traffic could be retrieved and disclosed to the company.

Proskauer submitted a "friend of the court" brief in the case on behalf of Employers Association of New Jersey. If you have any questions about how *Stengart* will impact your Internet usage policy or if you need help editing or drafting such a policy, please contact any of the attorneys listed on this Client Alert or your Proskauer relationship attorney.

[1] Notably, the emails were not sent from a company email account, which can waive the privilege in some cases and jurisdictions.

Related Professionals

- **Gregory I. Rasin**
- **Elise M. Bloom**
  Partner