Fox Rothschild LLP
ATTORNEYS AT LAW

April 2010

LABOR & EMPLOYMENT DEPARTMENT

ALERT

New Jersey Supreme Court Opines on Workplace E-mail Policies

By Ian W. Siminoff and Daniel N. Kuperstein

In a recent and long-awaited decision, the New Jersey Supreme Court, in *Stengart v. Loving Care Agency, Inc*., held that an employee had a reasonable expectation of privacy in e-mails she sent to her attorney from her personal, password-protected, Yahoo e-mail account using a company-issued laptop.

The Facts

The plaintiff, Marina Stengart (Stengart), a director of nursing and a long-term employee of a nursing home, Loving Care Agency, Inc. (Loving Care), resigned. After leaving, she filed a lawsuit against Loving Care alleging constructive discharge because of a hostile work environment, retaliation and harassment.

During the course of her employment, Stengart communicated via e-mail with her attorneys about a contemplated lawsuit against Loving Care. She used her company-issued laptop but sent the e-mails via her password-protected Yahoo e-mail account, rather than her work e-mail account.

In the ensuing litigation, Sills Cummis, the law firm that represented Loving Care, chose to preserve the hard drive from Stengart's laptop for electronic discovery purposes. Loving Care hired experts who made an image of the laptop's hard drive in an effort to restore and recover deleted information. These experts uncovered temporary Internet files containing e-mails between Stengart and her attorneys, some or all of which were sent during business hours and dealt with her anticipated lawsuit against Loving Care. Sills Cummis did not inform Stengart or her counsel of its finding. Instead, it reviewed the e-mails and then revealed their identity in responding to the employee's written discovery requests.

The Electronic Communications Policy

Loving Care's electronic communications policy, contained in its employee handbook, provided that e-mail and Internet use were not to be considered private. However, it also indicated that the "principal purpose" of e-mail was for company business and that "occasional personal use is permitted." While the policy prohibited certain uses of the e-mail system, such as job searches, it did not mention any prohibition against communicating with attorneys. The policy made no specific reference to communications via a password-protected, Internet-based e-mail account.

Earlier Decisions

The New Jersey Law Division (the trial court) held that where an employee has knowledge of an employer's policy that warns that Internet use and communication on

the employer's computer systems is not private, and warns that e-mail and Internet use are part of the company's business and client records, the attorney-client privilege does not extend to communications between an employee and her attorney over those systems, regardless of whether the communications are sent via the employer's work or personal e-mail account.

On appeal, the New Jersey Appellate Division reversed the Law Division's decision. The Appellate Division began by noting that it had problems with Loving Care's electronic communications policy, including an issue with the fact that certain terms in the policy were not defined (such as "media systems and services"), and that the policy permitted "occasional personal use," which created ambiguity as to what personal use was allowed. Independent of its concerns with the language of the policy, the court held that in balancing the employer's interest in monitoring its computer network vs. the employee's interest in maintaining the privacy of her communications with her attorney, the balance tipped in favor of the attorney-client privilege.

The New Jersey Supreme Court's Decision

The New Jersey Supreme Court modified and affirmed the Appellate Division's decision, holding that:

(1) Stengart reasonably expected that the e-mails sent between her and counsel via her personal, password-protected, web-based e-mail account would remain private;

(2) The fact that such e-mails were sent and received using a company laptop did not eliminate the attorney-client privilege that protected them; and

(3) Sills Cummis violated New Jersey Rule of Professional Conduct 4.4(b) by reading the e-mails and failing to either promptly give notice to Stengart about them or seek judicial intervention to determine whether the communications were privileged.

Implications for Employers

The decision expands employee privacy rights in the workplace by prohibiting an employer from reviewing the content of an employee's attorney-client communications sent via an employee's password-protected, Internet e-mail account. In fact, the court explained that if an employer were to have a policy that would permit an employer to retrieve and read such e-mails, such a policy would be unenforceable.

Notwithstanding the foregoing, the court held that employers can still adopt and enforce lawful policies relating to computer use to protect the company's assets, reputation and productivity and to ensure compliance with legitimate corporate policies. For example, in the context of an electronic communications policy that permits "occasional" personal use of the Internet, an employer can discipline an employee who consistently and pervasively spends long stretches of work time using the Internet for personal purposes.

We make the following additional observations concerning the *Stengart* decision:

- Having an electronic communications policy is critical to an employer's ability to monitor its employees' e-mail and Internet usage.
- The policy needs to be written in plain English, with technical terms of art, such as "media systems" and "Internet files" defined, and it should also indicate that e-mails are stored on a hard drive and can be forensically retrieved.
- If employers wish to monitor employees' electronic communications sent over company networks via employees' personal, password-protected, web-based e-mail accounts, the policy needs to so state, and be drafted in accordance with the *Stengart* attorney-client exception.
- Employers should clearly define, in their electronic communications policy, what their legitimate interests are in monitoring their networks, such as preventing the waste of company resources and protecting confidential information.
- If feasible, employers may want to consider blocking employees' access to their personal e-mail accounts via company computer systems to ensure that any personal e-mails, including attorney-client

privileged e-mails, are sent from the employees' work e-mail account, where employees arguably have less privacy rights.

• Employers need to procure signed employee acknowledgments regarding employees' receipt of electronic communications policies at the commencement of employment and periodically thereafter.

• Finally, employers should consider providing training to employees regarding their electronic communication policies, similar to the sexual harassment training employers typically provide to their employees.

For more information regarding this Alert, please contact Ian W. Siminoff at 973.994.7507 or isiminoff@foxrothschild.com, or Daniel N. Kuperstein at 973.994.7579 or dkuperstein@foxrothschild.com or any member of the Labor & Employment Department.