Are Employees' Personal Emails On Work Computers Private? "Sometimes" Rules N.J. Supreme Court

Insights
4.06.10

Until last week, most employers believed that they had the right to review -- and in fact owned -- any electronic information stored on company computers. In a recent decision, the New Jersey Supreme Court carved out an exception to this rule. When an employee exchanges emails with her attorney through a personal web-based email account using a company computer, that email is attorney-client privileged even though the computer may automatically create a viewable copy of the email's text in temporary internet files on the company computer. In addition to ratifying, once again, the sanctity courts grant to the attorney-client privilege, the case highlights the importance of well-drafted company policies to enforce workplace rules and protect employer rights. Although the precedent applies only in New Jersey, the decision is significant for all employers. *Stengart v. Loving Care Agency, Inc.*

The Facts Of The Case
Marina Stengart worked for Loving Care Agency, Inc., which provides home-care nursing and health services. Stengart worked as the Executive Director of Nursing at Loving Care and was provided with a laptop computer to conduct company business. The company's policy prohibited most personal use of company-owned email and advised employees that the use of the company's computer system was not to be considered private.

During her employment, Stengart communicated with her attorney several times about her work situation. She used her web-based, personal-password-protected Yahoo email account, but on a company-provided laptop computer. Unbeknownst to Stengart, there was software that automatically made a copy of the web pages she viewed (including the emails with her lawyer), which were saved on the computer's hard drive in a folder of temporary Internet files. Stengart's employment ended and she returned the laptop.

Stengart then sued Loving Care for various claims arising out of her employment, including harassment, discrimination and retaliation. During the course of discovery in Stengart's case, Loving Care and its lawyers reviewed the company's laptop computer used by Stengart and discovered emails between Stengart and her lawyer.

Loving Care and its lawyers disclosed the emails to Stengart's lawyers, but claimed the right to review the emails because they were sent using the company's laptop. Stengart sought return of the

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

emails and other relief and also argued that Loving Care's attorneys violated New Jersey's rules of professional conduct by failing to alert Stengart's attorneys that it had the emails before reading them.

Court Rules: "The Emails Are Private"

Utilizing a two-part analysis, the Court held that Stengart could reasonably expect that email communications with her lawyer using her web-based personal-password-protected account were private, despite the fact that she used the company's laptop to send them.

In coming to this conclusion, the Court first scrutinized Loving Care's Electronic Communications Policy (EC Policy). The EC Policy provided in relevant part that: 1) the company will exercise the right to review all matters on the company's media systems with or without notice; 2) email, voice mail, Internet use, and computer files are considered company property and are not to be considered private or personal; 3) the principal purpose of email is for company business, but occasional personal use is permitted; 4) use of the email system for business activities unrelated to Loving Care was prohibited; and 5) abuse of the electronic-communications system may result in disciplinary action up to and including termination.

The Court rejected Loving Care's argument that its employees had no expectation of privacy in their use of company computers based on the EC Policy, finding that it was unclear based on the language of the policy whether use of personal-password-protected, web-based email accounts via company equipment was covered. Specifically, the Court pointed to the fact that "media system" was not defined in the EC Policy and prohibitions regarding inappropriate use of the "email system" appeared to refer only to company email.

The EC policy did not address personal accounts at all and did not warn that personal emails may be stored on a hard drive and reviewed by the company. In other words, Loving Care's employees did not have express notice that personal emails accessed using a company-owned system were subject to monitoring. In fact, the company acknowledged in the EC Policy itself that occasional personal use was permitted.

Second, the Court analyzed the content of the messages and whether there should be heightened privacy protection for messages between Stengart and her lawyers because of the attorney-client privilege that normally attaches to communications between clients and their attorneys. In its analysis, the Court distinguished between use of a company computer to access websites containing adult and child pornography or sending unprofessional emails to a supervisor (where there is clearly no legitimate expectation of privacy) and the use of a company computer to communicate with one's lawyer (where a legitimate expectation of privacy depends on various circumstances, including what notice is given by the company).

The Court found that Stengart had a reasonable expectation of privacy in her emails with her lawyers under these circumstances because: 1) Stengart had a ***subjective*** expectation of privacy because she used a personal, password-protected email account and not the company's account; 2) Stengart

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

she used a personal-password-protected email account and not the company's account; 2) Stengart had an ***objectively*** reasonable expectation of privacy because the company's EC Policy did not address use of personal email accounts at all and also allowed for some personal use, further muddying the waters as to exactly what use was prohibited; and 3) the emails were not illegal or inappropriate such as to potentially cause harm to the company, but instead were attorney-client communications historically considered to be private.

The Court also ruled that Loving Care's lawyers' review and use of the privileged emails violated the state ethics rules governing the inadvertent disclosure of privileged communications. Although the Court noted that Loving Care's attorneys did not act in bad faith and believed that they legitimately attempted to preserve evidence to defend a civil lawsuit, it still found the attorneys erred in not setting aside the possibly privileged communications once they realized they were privileged. This factual background may have led the Court to take a broader view on the issue of whether Stengart's emails sent using the company-owned systems were private.

Your Policies Should Give Clear Notice Of What Is Prohibited

The Court in *Stengart* confirmed that employers can adopt and enforce lawful policies relating to computer use in order to "protect the assets, reputation and productivity of a business and to ensure compliance with legitimate corporate policies." Yet, the Court went so far as to opine that a policy that banned all personal computer use â€“ even if it provided clear notice that an employer could retrieve and read an employee's attorney-client communications on a personal email account using the company's systems â€“ would ***not*** be enforceable, because of the important public policy concerns underlying the attorney-client privilege.

While this specific holding applies only to New Jersey employers, this case should remind all employers how important well-drafted policies are to enforcing workplace rules and protecting employer rights. This is particularly true in the area of electronic communications where technology continues to develop at a rapid pace creating an ever-changing legal landscape in this area of workplace privacy.

For maximum protection, you should carefully review any electronic-communications policies to be sure those policies reflect the intent and practice regarding the scope of any prohibition on, or monitoring of, personal use of your computer systems. Make sure that any such policies take into account today's technology in order to specify what personal use is prohibited and what emails and computer use will be subject to review. For instance, if you intend to prohibit personal use of web-based password-protected email using the company's computers, or to monitor such communications, you need to specifically say so.

Finally, ensure that any policies (especially those involving monitoring of personal email) comply with the laws specific to your jurisdiction, make sure that such policies are clearly communicated, acknowledged by employees in writing and consistently enforced.

If you have questions, or would like help updating your electronic communications policies, please contact your regular Fisher Phillips attorney.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.

contact your regular Fisher Phillips attorney.

This Legal Alert provides information about a specific court ruling. It is not intended to be, and should not be construed as, legal advice for any particular fact situation.

Copyright © 2024 Fisher Phillips LLP. All Rights Reserved.