California Court: Emails Sent To Plaintiff's Attorney On Employer's Computer Are Fair Game

Insights
1.31.11

A California appellate court recently decided that an employee's email messages to an attorney about suing her employer could be used against her at trial. The messages were not protected by the attorney-client privilege, because the employee knowingly sent the messages from her work email account. This unusual legal result was made possible because the employer had a written policy that clearly stated messages sent on the employer's electronic communications system were not private. *Holmes v. Petrovich Development Company, LLC.*

If you have not recently done so, now is the time to update your electronic communications policy to notify employees that messages sent on your computers and electronic devices are not private.

Sender Beware . . . Except In New Jersey
You may recall our Alert last spring of a similar case in New Jersey with a different outcome. *Stengart v. Loving Care Agency, Inc.* ("Are Employees' Personal Emails on Work Computers Private? â€˜Sometimes' Rules N.J. Supreme Court," Apr 6, 2010). In that case, the employee sent emails to her attorney from an employer-provided laptop computer using a private, password-protected Yahoo email account. Unbeknownst to the employee, the laptop was configured to automatically save temporary copies of all Internet pages viewed, including her web-based Yahoo account. When the employee was terminated and returned the laptop, the employer found the emails.

The New Jersey court decided that the employee's emails to her attorney were privileged, because the employer's electronic communications policy permitted occasional personal use of the corporate email system, and was silent about whether the company could or would review private, password-protected email accounts.

The Employer's Policy Is Key
By contrast, in the recent California case, the employer's policy was much clearer about what conduct was prohibited. Employees were told that company computers were to be used for company business only and could not be used to send or receive personal email. Employees were warned that the company would monitor its computers and could inspect all files and messages at any time. Finally, employees were advised that they had no right of privacy with respect to any personal information or messages created or maintained on company computers.

"Like Consulting Her Lawyer In Her Employer's Conference Room"

When the plaintiff employee sent emails to her attorney despite all of these warnings and prohibitions, the court likened it to "consulting her lawyer in her employer's conference room, in a loud voice, with the door open, so that any reasonable person would expect that their discussion of her complaints about her employer would be overheard by [the employer]." Under these circumstances, the court found that the email messages were not privileged. The fact that the company as a practical matter did not enforce its computer monitoring policy or inspect employees' personal email communications did not void the policy. The employer won the case.

Practical Steps You Can Take Now

You've heard it before, but the *Petrovich* case is a great reminder of how important well-drafted policies are to protecting employers' rights in the workplace, especially where electronic communications are concerned. Carefully review your electronic communications policy to be sure it clearly specifies what personal use is permitted (if any) and what emails and computer use will be subject to monitoring and review. Don't overlook new innovations like social networking sites (Facebook, LinkedIn, Twitter) and smart phones that may not have existed when the policy was created. If you would like help updating your electronic communications policies, or creating new ones, please contact your regular Fisher Phillips attorney.

This Legal Alert provides an overview of a particular new legal decision. It is not intended to be, and should not be construed as, legal advice for any specific fact situation.