PBN .com
UPDATED DAILY
APRIL 4-10, 2011
VOL. 25, NUMBER 52
$2.00

PROVIDENCE BUSINESS NEWS
YOUR LOCAL SOURCE FOR BUSINESS NEWS IN SOUTHERN NEW ENGLAND

Email privacy not a guarantee in workplace

GUEST COLUMN

Brian J. Lamoureux and William E. O'Gara

One of your employees is not happy with you. She believes you discriminated against her in the latest round of promotions. Seeking vindication, she uses your company's laptop and server to access her Gmail account to send what she believes to be confidential and privileged emails to a lawyer she wants to hire to sue you.

The emails detail her complaints as well as her lawyer's thoughts about the weaknesses in her case. Unbeknownst to the employee, the Internet browser she uses to access her Gmail account automatically stores or "caches" an image of the Gmail screens into temporary memory on your company's server. She quits and files a discrimination complaint.

As part of the process of dealing with the lawsuit, your IT department retrieves all of the employee's electronic files, including the "screenshots" of the inbox of her Gmail account which reveals the communications between her and her lawyer. You turn these images over to your lawyer, who uses them to poke holes in the employee's case during her deposition. The employee claims that you cannot use those emails because they were unlawfully obtained and violate the attorney-client privilege between her and her lawyer.

Who wins? Unfortunately, there is no clear answer. A recent decision by a California appellate court has created a clear split of legal authority on the issue. That decision squarely conflicts with a landmark decision issued by the New Jersey Supreme Court last year. In the New Jersey case, a woman used her personal, Web-based Yahoo account to communicate with her attorney on a company computer and through a company server. The employer sought to use those emails to defend against the woman's discrimination claims. The New Jersey court sided with the woman, and determined that the employer improperly obtained the emails. The court noted that the employer's written policy was too vague and unclear because it did not explicitly state that the company could and would access private, Web-based emails. The court also was troubled that the company's policy contradicted itself by suggesting that the company's computers could be used for "occasional[ly]" sending personal emails.

The New Jersey court . . . determined that the employer improperly obtained the emails.

The California court reached a different result, albeit in different factual setting. In that case, the employee not only used a company computer to send emails to her attorney, she used her company-based email account to do so. At first blush, this difference from the New Jersey case may explain why the California court reached a different result than the New Jersey court. However, the California court went a step further, noting that the employee's use of a company computer was "akin to consulting her attorney in one of [the company's] conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation" would be privileged. This language suggests that the California court is warning all employees – regardless of whether they use Web-based or company-based emails – that they should not expect any privacy in emails sent through a company computer or server. Given the widespread ability for employees to communicate privately after-hours using their own computers and free email services, it is likely that courts will find the California court's reasoning more persuasive in future cases where a company has a clear email policy.

What should employers take away from this unsettled legal landscape?

Among other things, employers need to have a written and clear policy that:

- Addresses the use of company computers for personal reasons, including sending or receiving personal emails through Web-based and other private email providers;
- Explains that the company will monitor its computers for compliance and inspect all files and messages on its computer system;
- Makes clear that employees may (or may not) have a right of privacy in emails sent or received on company computers. Employers need to give careful thought about how much leeway and privacy, if any, they want to give their employees when it comes to using a company's computer system.

Employers also need to keep in mind that a written policy is only effective if it is actually followed, enforced, and updated as necessary. Unfortunately, many employers are reluctant to spend the minimal time and resources necessary to craft a solid email and computer policy (or to revise one that's woefully outdated).

Failing to have an effective policy puts employers at a significant disadvantage in all types of litigation because relevant and helpful evidence might get excluded in court. n

Brian J. Lamoureux is senior counsel at Pannone Lopes Devereaux & West, LLC in Providence. He, along with PLDW partner William E. O'Gara, advises employers regarding various employment-related issues. They can be reached at bjl@pldw.com.