Sorting out attorney-client privilege with workplace emails

Every employer with a computer system should have a policy defining permissible uses, including uses by the employer, of that system. It really is that simple.

At this very moment, in workplaces across America, employees are using company computers to send personal emails. Somewhere, a disgruntled employee is sending a message to his or her attorney using a computer provided by the very employer the employee is complaining about. When this email is uncovered later during litigation — and based on our litigators' experience, it will be — a battle will ensue over whether the employer can use it to support its case. Is it a privileged communication between a lawyer and client? Recent cases say: "It depends."

First, some background. For a communication to be covered by attorney-client privilege, it must have been intended to be kept confidential between a client and an attorney, and it must be kept that way. Communications that are shared with others are not protected, and neither are communications that were never intended to be confidential. And the intent to keep a statement confidential must be reasonable. Speaking with a lawyer on a crowded bus, for example, will be an unprotected conversation, even if no one actually overhears it, because it would not be reasonable to expect it to go unheard.

So, whether employee emails are attorney-client privileged usually depends on whether the employee reasonably expected them to be confidential. The issue is somewhat circular. If courts hold that certain emails are confidential, then those decisions create a reasonable expectation of confidentiality. As courts describe the reality regarding expectations, they also help to create it.

One thing is clear: it matters whether the employer has adopted a computer-use policy. These policies say things like, "The computer system is the employer's property and should be used for business purposes only." Good policies explicitly caution workers that the employer has the right to monitor the system. Courts found that such policies destroyed the employees' expectation of privacy in *Scott v. Beth Israel Medical Center, Inc.*,[1] and *Kaufman v. Sunguard Investment Systems*,[2] allowing the employers to have access to messages sent through their server. In *Transocean Capital, Inc.*,[3] however, where the employer had not adopted such a policy, the court upheld the employee's claim of privilege. But even the best computer-use policy is ineffective if it isn't communicated to employees. A federal court made this clear in *Mason v. ILS Technologies*,[4] where it ruled against an employer that had adopted a policy on paper, but failed to communicate it to employees.

What if the employee uses a password-protected, personal web-based email account, such as Yahoo mail or Gmail, rather than the employer's email server?

What if the employee uses a password-protected, personal web-based email account, such as Yahoo mail or Gmail, rather than the employer's email server? Although that may make it more difficult for the employer to retrieve a copy of the messages, it won't make retrieval impossible and it won't necessarily change the result with respect to confidentiality either. Courts have split on this question. > Continued

> While the law is still developing, it seems that courts are more willing to protect email that is sent through a personal web-based account.

A federal court in New York treated web-based emails the same as emails sent using an employer's server in *Long v. Marubeni America Corp*.[5] In that case, the employer's computer-use policy precluded a reasonable expectation of confidentiality. In the case of *Sims v. Lakeside School*,[6] however, a federal court in Washington state distinguished between the two situations. It held that, as a matter of public policy, the employer's computer-use policy did not destroy the employee's reasonable expectation of confidentiality in using a personal, web-based email account.

While the law is still developing, it seems that courts are more willing to protect email that is sent through a personal web-based account. In *Curto v. Medical World Communications, Inc.*,[7] an employee used company-issued laptops in her home office to send her attorney emails through her personal AOL account. The court found that she had a reasonable expectation of confidentiality because, although the employer said it would monitor messages, it was unable to do so since the messages didn't go through its server. In another case, *National Economic Research Associates, Inc. v. Evans*,[8] the court found that an employee who used his company-issued laptop to email his attorneys through his Yahoo account had a reasonable expectation of confidentiality, because he couldn't be expected to know that his employer could retrieve the emails from the laptop. This rationale will be harder to maintain as judges, like the rest of us, become more familiar with computer forensics.

What's the bottom line? Employers should maintain a current computer-use policy, as many are already doing. Communicate the policy to all employees, and make sure you receive and maintain signed acknowledgements from them that they are aware of the policies.

As for employees, they should know their company's computer-use policies and be aware that their employers can retrieve and read their emails. Rather than rely on a privilege that may or may not attach, just follow this general guideline: If you wouldn't want your employer to read it, don't send it from your email at work.

By Wayne Moskowitz |

Wayne Moskowitz has more than 20 years of experience in commercial litigation, and is a published author on the subjects of electronic discovery and appeals. wayne.moskowitz@maslon.com

[1]847 N.Y.S.2d 436 (Sup. Ct. 2007). [2]2006 WL 1307882 (D.N.J. 2006). [3]2006 WL 3246401 (Mass. Super. 2006). [4]2008 WL 731557 (W.D.N.C. 2008). [5]2006 WL 2998671 (S.D.N.Y. 2006). [6]2007 WL 2745367 (W.D. Wash. 2007). [7]2006 WL 1318387 (E.D.N.Y. 2006). [8]2006 WL 2440008 (Mass. Super. 2006).