New Jersey Law Journal

VOL. 201 - NO 11 SEPTEMBER 13, 2010 ESTABLISHED 1878

IN PRACTICE

EMPLOYMENT LAW

Factors To Take Into Consideration When Drafting Electronic Communications Policies

BY PATRICIA SMITH AND KRISTIN LAROSA

Business, and to some extent personal, use of electronic communications has become ubiquitous in the workplace. Savvy employers have implemented policies addressing appropriate and acceptable use of electronic communications by employees. Earlier this year, the New Jersey Supreme Court issued an opinion that will change the legal landscape of such policies and should be carefully reviewed by employment counsel.

In *Stengart v. Loving Care Agency, Inc*., 201 N.J. 300 (March 31, 2010), the Court addressed the question of whether the attorney-client privilege attached to e-mails exchanged between an employee and her counsel over company-provided equipment and systems, and if so whether she had waived the privilege. The case, however, has implications far beyond privilege issues. In brief, the Court found that employees may have a reasonable expectation of privacy when using employer-issued computers for sending electronic mail (e-mail) even if the e-mail is sent through a personal, password-protected, web-based e-mail account.

The plaintiff, Marina Stengart, was employed by Loving Care Agency, Inc., as an executive director of nursing and was issued a laptop computer for the purposes of conducting company business. During her employment, Ms. Stengart became dissatisfied with certain working conditions and began sending e-mails to her attorney via her work-issued computer, using a web-based, password-protected e-mail account. The bottom of the e-mail received by Stengart from her attorney advised that the information contained in the e-mail was confidential and subject to the attorney-client privilege. Unbeknownst to Stengart, however, the company's browser software automatically saved a copy of these e-mails in a temporary Internet files folder. Stengart ultimately left the company's employ and returned her laptop.

The Appellate Division found that those e-mails were protected by attorney-client privilege and further, in view of the ambiguity of the policy concerning personal e-mail use, an employee could reasonably expect to retain a certain level of privacy in such communications. The Appellate Division determined also that the company's attorneys had violated the rules of professional conduct by failing to alert Stengart's attorneys that it possessed such privileged information.

The New Jersey Supreme Court agreed with the Appellate Division in finding that Stengart had a reasonable expectation of privacy pertaining to e-mail communications with her attorney through password-protected, web-based e-mail accounts. In sum, the Court found that sending and receiving these e-mails using the company-provided laptop did not eliminate the attorney-client privilege. The Court also found that Loving Care's attorneys violated the rules of professional conduct by reading e-mails that may have been privileged without notifying Stengart's attorneys or obtaining court permission to do so.

The Court's holding was based, in part, on the adequacy of the notice contained in the policy. First, the Court found that the policy did not contain any reference to password-protected, Internet-based e-mail accounts. Rather, references in the policy to e-mail systems were directed towards company e-mail accounts. Based on the absence of any reference to private Internet accounts, the Court determined that there was no way employees could be put on notice that their communications would be subject to third-party monitoring if sent on company-issued computers. The Court also noted the absence of any language in the policy warning that

Smith is a partner in the litigation department and a member of the labor and employment group at Ballard Spahr in Cherry Hill. LaRosa is an associate within the group.

the contents of the employees' personal e-mail account could be forensically retrieved and imaged. Additionally, the Court found that the portion of the policy that provided for occasional personal use of e-mail, without properly defining "e-mail" created an element of doubt as to whether those e-mails were company or private property.

The Court also noted the overall lack of inappropriateness or illegality contained in the e-mail correspondence between Stengart and her attorneys, which eliminated any suggestion that their content in any way harmed the company. Instead, the Court noted the long-standing recognition of privacy given to communications between an individual and their attorney. The Court found that Stengart did not in any way waive the attorney-client privilege because she took steps to maintain the confidentiality of the communications by using an Internet-based, password-protected account, and did not save her password on the computer.

Because this was such a novel issue for New Jersey courts, the Court also examined other cases both within and outside its jurisdiction for guidance as to whether under the circumstance Stengart had an objective, reasonable expectation of privacy. The Court pointed to one case in New Jersey where no expectation of privacy was found to exist for an employee who was accessing websites containing adult and child pornography, where company policy authorized it to monitor employee website activity and e-mails. Conversely, the Court cited to another matter which found that an employee had a reasonable expectation of privacy where a company policy failed to advise that it could monitor the content of e-mails issued from a personal Internet-based e-mail account viewed over company computers. In examining the case law, the Court noted that employees generally had a lesser expectation of privacy when using company e-mail as compared to a personal, Internet-based account such as Stengart's. The Court acknowledged that a company's policy that clearly banished an employee's personal use of e-mails would diminish any claim of privacy, but noted that in today's society such a blanket prohibition would be unworkable.

While the holding in *Stengart* focused upon issues of attorney-client privilege, the question of an employee's reasonable expectation of privacy, or lack thereof, in electronic communications has a much broader implications. For example, an employer's search of employee e-mail accounts may support a claim for tortious invasion of privacy. Employees have asserted wrongful discharge claims for terminations resulting from improper e-mail communications over which they claim they had a reasonable expectation of privacy. Public employers' workplace searches must be balanced against an employee's reasonable expectation of privacy. The Court's opinion therefore should serve as a framework for employers seeking to create or revise their electronic communications policies. In light of this holding, employers should take the following factors into consideration when drafting electronic communications policies:

Provide a Clear Definition of E-mail: Employers should be sure to include a proper definition of what constitutes electronic mail and/or e-mail. For example, if an employer intends to include personal, password-protected, Internet-based e-mail accounts as being subject to review and search when transmitted over company property (i.e., a laptop or desktop computer), that should be clearly and expressly stated in the policy.

Provide Written Notice to Employees That Communications May Be Stored and Retrieved by the Employer: Another noted deficiency in the policy addressed in *Stengart* concerned the complete absence of any warning to employees that the contents of their personal, Internet-based e-mails would be stored and could be retrieved and read in the future. If employers intend to equip their systems with the ability to store, retrieve and/or forensically image electronic communications or Internet sites, they should be sure their electronic communications policies describe exactly which types of communications and/or sites are subject to these measures.

Provide Notice of any Intent To Monitor Employee Use of Employers' Computer Systems: Employers who intend to monitor employee e-mail communications, either sporadically or routinely, should fully inform employees of this intent in their policies. The policies should not only advise of the employer's intent to monitor Internet-based e-mail accounts, but should also include monitoring of employee activity on social networking sites such as Facebook or MySpace, which has become increasingly at issue in employment-related litigation.

Time and Location Issues: In *Stengart*, the Court noted the fact that the communications were sent during nonworking time and from the employee's home. In the absence of a policy provision addressing those factors, the Court observed that an employee could reasonably expect communications sent over a company-provided laptop during "private" time and from nonwork locations to be private. Employers should include provisions in their electronic communications policies that address those issues.

Be Consistent: It is almost impossible in this day and age to expect that employees will not use company-issued computers for some type of personal use. In fact, *Stengart* warned that a zero-tolerance policy regarding personal e-mails can be "unworkable and unwelcome" and was not encouraged. However, employers are advised to be clear and consistent when defining the terms and conditions of the use of personal e-mails at work. The Court in *Stengart* faulted the company for the ambiguity contained in the policy that boldly declared e-mails were not to be considered private or personal, while simultaneously permitting "occasional use" of e-mail. Any provision allowing for the personal use of e-mail also should state whether those e-mails are considered company or private property and whether they are subject to monitoring or not.

Be Aware of Attorney-Client Privilege Limitations: *Stengart* also serves as a warning to employers who stumble across e-mails between employees/former employees and their attorneys. If an employer uncovers such information, they should immediately turn the documents over to its attorneys who should either promptly notify their adversary of discovery of these e-mails or seek direction from the court before reading further.

We anticipate that this case is only the beginning of a string of litigation that will result from employee use or misuse of employer's computer systems. Employers should be sure to review their current policies, to ensure they comply with the standards articulated in *Stengart*. ■