N.J. Appellate Court's Groundbreaking Decision Gives Employees A Limited Right to Privacy When Using Company Computer

Articles

07.06.2009

For the first time, a New Jersey court has ruled that an employee has a limited right to privacy when using his/her employer's computer for personal matters. In Stengart v. Loving Care Agency, Inc. et al., New Jersey's Appellate Division found that the employee had a legitimate expectation of privacy when she accessed her personal e-mail account from the company computer in order to communicate with her attorney. The Court reached this holding despite the employer's broad electronic communications policy, which disclaimed any expectation of privacy and stated that communications using the company computer became company property.

As a result of this decision, employers need to revisit their employee handbooks and electronic communication policies, and likewise may need to exercise restraint in monitoring employee use of electronic equipment in the workplace.

In this case, the employee ultimately resigned her job and filed a discrimination lawsuit against her employer. But, before she quit, the employee had already hired an attorney, whom she communicated with through e-mail. These e-mail communications related directly to her discrimination claims, and several were sent from the company laptop computer assigned to her. However, the e-mail exchanges were through a personal, web-based, password-protected Yahoo e-mail account which she was able to access from her company-assigned computer. After the lawsuit began, the company's attorneys did a forensic scan of the laptop, and found these e-mails, which it hoped to use during the litigation.

In the litigation, the company argued that these e-mails were not protected by the attorney-client privilege because the e-mails had been sent using the company computer. The company relied on language in its Employee Handbook, which among other provisions: (1) reserved to the company the right to review and intercept all matters passing through it servers; (2) stated that all e-mail communications and Internet use were not "private" but rather would be considered "company property," and; (3) stated that the principal purpose of the company

hardware and software was for business communications, permitting only occasional personal use. The trial judge agreed with the employer, finding no privilege and holding that the employee waived any right to privacy by virtue of the express language in the Employee Handbook.

On appeal, however, the Appellate Division reversed the trial court's decision completely. The Court found numerous grounds to conclude that these e-mail exchanges were purely private and that the employee had a legitimate expectation of privacy that forbade the employer (or its attorneys) from accessing them. The Court initially found the Employee Handbook language to be confusing and ambiguous, given that it sought to claim all computer use as "company property" while expressly allowing personal use of that same computer. But, the Court did not stop there. Rather, the Court found that employees have a legitimate expectation of privacy in these e-mail communications, and analogized the employer's inspection of these e-mails to an employer who "rifles through a folder containing an employee's private papers or reaches in and examines the contents of an employee's pockets." Finally, the Court also faulted the company attorneys for reading and reviewing these e-mails and not seeking Court intervention when it became obvious that these were attorney-client communications.

In reaching its holding, the Court acknowledged the broad company policy in the Employee Handbook, yet found that it simply went too far. Noting its belief that employers have been given too much leeway in this area, the Court formulated a new rule that employers can only access employee personal e-mail communications and internet usage if there is a legitimate business reason to do so. The Court also stated that courts should balance the import of the company's claimed legitimate business interest against the employee's confidentiality interest in determining whether employer access to the employee's personal communication is appropriate. In this case, the employee's interest in the confidentiality of her communications with her lawyer trumped any employer interest in reviewing them.

The Appellate Division opinion provides very little guidance to employers on what is or is not going to be considered proper monitoring and access by employers to employee personal communications. The Court expressly stated that it would "make no attempt to define the extent to which an employer may reach into an employee's private life or confidential records through an employment rule or regulation," suggesting this was best left to the Legislature. And while the Court, by way of example, indicated that an employer may monitor whether an employee is distracted from the employer's business and take appropriate disciplinary action, that "right to discipline or terminate…does not extend to the confiscation of the employee's personal communications."

This decision may still be appealed to the New Jersey Supreme Court, so this case may not be the final say on this matter. Yet, for the time being, all New Jersey employers will need to take two steps in response to this decision.

First, all New Jersey employers should examine the current language in their Employee Handbook and/or electronic communications policy. The policies must be clearly expressed and unambiguous that the company computers are for company business and that all communications made using the company computer are accessible to the company and will not be considered "private." Moreover, given that the employer in the reported case was also disadvantaged by its acknowledgement that employers could "occasionally" use the

computer for personal business, employers need to consider whether to expressly forbid any personal use of company computers. This is not likely going to be practical for many employers, given the realities of the workplace and historical practices, which, if changed, will create a new series of morale issues. But it would be practical, if not cost prohibitive, to upgrade filters to prevent employee access to personal e-mail accounts, thereby assuring that any "personal" e-mails which are sent will be on the company's network, rather than the employee's personal account. Certainly, the Appellate Division's opinion did focus on the fact that the employee e-mails here were made on the employee's personal website, albeit accessible to the employer because they were imaged on the company computer's hard drive.

Second, regardless of the language of the company policy, employers need to exercise caution when monitoring and accessing employees' personal use of company computers. There are certainly legitimate business reasons to do so, and employers may continue to check employee computer usage to see if the personal use is excessive, but this interest recognized by the Appellate Division does not necessarily provide a basis for the employer to review the content of the communications. There may be instances, such as in employee breach of loyalty cases, where the content of the employee's conduct may be legitimately reviewed. The problem is that, with such limited guidance from the Appellate Division, it becomes difficult to discern when it is legitimate to monitor only as opposed to accessing the content of the communications and retaining them. This will become a case-by-case consideration, and will likely compel more access to legal advice before employers unilaterally access these personal communications.

If you have any questions about this new decision, or any revisions that may be needed to your company handbook or electronic communications policy, please contact a member of Archer's Labor and Employment Department at (856) 795-2121.

Printer Friendly View

Related Services

- Labor & Employment