EDWARDS ANGELL PALMER & DODGE

eapdlaw.com

Client Advisory | *June 2010*

Recent Court Rulings on Employer Review of Employees' Electronic Messages - Adjustment to Employer Policies Needed

Two recent cases, one from the U.S. Supreme Court and one from the Supreme Court of New Jersey, suggest that companies need to periodically, if not immediately, update their computer and e-mail policies in order to minimize or prevent litigation when employees use the company's systems for personal messages. Incidental personal use is commonplace, despite the fact that most companies have policies that limit employees' use of the company's communication systems and state clearly that the company may monitor or access employee use of these systems. Implications of these court rulings for employer policies and practices are listed at the end of this Alert.

Mark E. Schreiber, Partner

Barbara A. Lee, Counsel

In a victory for employers, the U.S. Supreme Court ruled that an employer had not violated an employee's Fourth Amendment privacy rights by reviewing text messages on an employer-provided pager. However, the Supreme Court of New Jersey ruled that confidential communications between an employee (or ex-employee) and the employee's attorney may be protected by the attorney-client privilege, even if the employer has notified employees that they have no expectation of privacy in e-mails sent or received by or through the use of the employer's computers, e-mail system, or internet provider. Companies should be aware of both of these rulings and review their computer use policies to make sure that they provide clear and specific notice to employees that messages sent and received by or through the use of company systems, including personal digital assistants, pagers, other ancillary devices, cell phones, text and instant messaging, Gmail, Yahoo, voice mail, etc., are subject to the employer's scrutiny.

The Supreme Court Case

The case decided by the U.S. Supreme Court involves a public sector employer, but the situation in which the employer found itself could easily occur in a private sector organization, and the Court's analysis suggests several implications for employer action. In *City of Ontario, California v. Quon,* decided on June 17, 2010, the Court ruled that a police department did not violate the Fourth Amendment's requirement that searches be reasonable when it reviewed employees' personal text messages created on pagers owned by the city. The City had issued a written policy that notified employees that any use of department computers for e-mail or other internet access must be strictly limited to official business, and that employee communications using the department's computers or internet service provider would be monitored by the department. The policy stated that internet and e-mail systems were not to be used for personal or confidential communications, and employees were told that pagers were covered by the employer's e-mail policy.

Despite these formal policies, however, the department had an informal practice of allowing employees to use their pagers for personal text messaging as long as they did not exceed the quota allotted to each pager each month by the employer's contract with

its text messaging provider. When employees exceeded this limit, they paid for the excess usage from their personal funds. After the employer decided that the bookkeeping for these transactions was too time-consuming, it decided to review the employees' text messages to ascertain the proportion of business-related messages to personal messages and to determine whether the contractual quotas should be increased. The employer found that the vast majority of the messages were not work related, and disciplined the employees who had exceeded their quotas. When the employees learned that their personal messages had been provided to their employer by the text messaging provider, they sued both their employer and the service provider.

The U.S. Supreme Court reversed the Ninth Circuit decision, which had found that the informal policy of permitting personal use created an expectation of privacy, despite the clarity of the written policy and the employer's written notice that it would monitor electronic communications. Applying the framework created by an earlier Supreme Court case, *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Court stated that the appropriate test was whether the employee had a reasonable expectation of privacy as a result of the "operational realities of the workplace" and, if so, whether the employer's intrusion on that privacy was reasonable "under all the circumstances." For purposes of this case, the Court assumed, without deciding, that the employees had a reasonable expectation of privacy in e-mail or text messages, that the City's review of their messages was a "search" for Fourth Amendment purposes, and that the principles articulated in *O'Connor* applied to searches of electronic communications—issues that the high court had not yet addressed.

The Court ruled that the search was justified because the City was concerned that these police officers were exceeding their texting quotas, which either cost the City additional money or burdened the City with the need to collect the excess costs from the employees. It also ruled that the scope was not excessively intrusive, in that only two months' worth of messages were reviewed, and only those sent and received while the users of the pagers were on duty. The Court further ruled that it was not reasonable for the employees to believe that their text messages were immune from review because of the nature of police work and the fact that such communications were subject to state open records laws. And it chastised the appellate court for ruling that the employer must use the "least intrusive" method of searching, stating that such an inquiry was too speculative. Thus, the search was reasonable and the employer's conduct was within permissible boundaries.

The New Jersey Case

In the New Jersey Supreme Court case, *Stengart v. Loving Care Agency*, 990 A.2d 650 (N.J. 2010),* the company had issued a laptop computer to the employee, which she used to exchange e-mails with her attorney using her personal, password-protected Yahoo account rather than the company's e-mail account. She was not aware that the laptop's software captured a "screen shot" of every web page accessed by any user of that computer and stored the images in temporary internet files. When the employee resigned from the company, she returned the laptop and then filed a discrimination lawsuit against the company.

As the litigation was progressing, the company discovered the e-mails between the employee and her attorney and produced the e-mails over the objection of the employee's attorney, who demanded that all copies of the messages be returned because they were protected by attorney-client privilege. The company pointed to its computer use policy, which stated that the company had the right to review, access, and disclose "all matters on the company's media systems and services at any time." The policy also stated that e-mails, Internet communications and computer files were the company's business records and "are not to be considered private or personal" to employees. The New Jersey Supreme Court ruled that the policy did not give sufficient warning to employees that it applied to personal e-mails created and sent through a personal, web-based e-mail account rather than the company's own e-mail system. Nor did the policy inform employees that the company's software system captured images of every e-mail message sent and received, allowing the company to retrieve

The New Jersey Supreme Court ruled that the policy did not give sufficient warning to employees that it applied to personal e-mails created and sent through a personal, web-based e-mail account rather than the company's own e-mail system.

such messages. Furthermore, the policy expressly allowed occasional personal use of its computers and e-mail system, which created ambiguity with respect to whether personal e-mails were personal property or company property. Finally, the court ruled that these messages were protected by the attorney-client privilege, and that the fact that they were sent and received using the company's computer did not destroy the privilege.

Third Party Providers Under *Quon*

The employees in *Quon* also sued the provider of the paging service, Arch Wireless. The provider was found liable for violation of the Stored Communications Act, 18 U.S.C. §§2701-2711, for providing transcripts of these messages to the employer without the employees' consent. That law, part of the Electronic Communications Privacy Act (18 U.S.C. §§2510 et seq.), prohibits "providers" of electronic communications services from disclosing private communications except under certain circumstances. Because the U.S. Supreme Court did not address this issue, the ruling of the Ninth Circuit still stands, but may be the law only in the Ninth Circuit. The safer course for employers would appear to be to insert an explicit statement that the employee gives permission for such disclosure by third party providers as part of the company's computer and e-mail use policy.

Practice Suggestions

Although *Quon* applies most directly to public sector employers, and *Stengart* focuses on the narrow issue of communications between an employee and her attorney, the combined result of these rulings suggests some practical lessons for employers:

1. Policies regarding employee use of electronic media operated by or through the employer's systems should ensure that all forms of such media, including personal e-mail accounts such as Gmail and Yahoo, other forms of communication technology such as personal digital assistants, pagers, text and instant messaging, cell phones, voice mail, social networking sites, etc. are covered by the policy. The policy should make it very clear that employees have no expectation of privacy and can expect their use of these systems and devices to be monitored by the employer. Policies should use words that individuals who are not knowledgeable about information systems will understand. Terms such as "media systems" may not communicate clearly to employees what is covered in the policy. The policy should also state that employees must consent to disclosure of communications stored by third-party vendors who provide communication services to the company.
2. The policy should also state that *any* messages communicated and/or stored by third-party vendors are subject to monitoring and access by the company and disclosure to the employer by the third-party vendor, and that employees have no expectation of privacy in such communications. It should also state that messages and other evidence of computer or network use may remain indefinitely either on the computer or in the network's memory and may be accessed by the employer at any time.
3. The policy should state that the employee will be required to complete an express acknowledgement that the reservation of the right to monitor or obtain messages includes any incidental personal use of these systems or devices, and that the employee specifically consents to the monitoring and disclosure of the communications transmitted or stored by a third-party vendor on behalf of the employer or otherwise.
4. Employees should be notified at least annually of this policy, or at any time that the policy is changed. Employers should require employees to expressly confirm that they have read and understand the policy, either by a personally signed acknowledgement, a "click through" link on the company's website, and/or annual reminders.
5. The policy should be reviewed and updated periodically to ensure that its scope is adequate to cover new forms of communication technology or devices that have not been included previously.
6. The policy should state that it can only be changed in writing by a high level official (stating the individual's title), and it should be enforced consistently. Employees, including supervisors and managers, should be trained about the policy and the systems that it covers, and

And finally, the court ruled that these messages were protected by the attorney-client privilege, and that the fact that they were sent and received using the company's computer did not destroy the privilege.

should be reminded periodically that this policy is a priority of the company.

7. Before reviewing allegedly "private" employee e-mail, go through the following steps:
   a. Review the actual language of the company's computer use policy.
   b. Make sure that the employee received and signed a statement acknowledging receipt and understanding of the policy and that a copy has been retained by the company.
   c. Ascertain whether the company has allowed private use of computers by employees without attempting to monitor or halt the practice.
   d. Identify whether the computer use policy has been enforced.
   e. Ensure that the reason for the review is a legitimate work-related concern, such as an investigation or evaluation of potential employee misconduct.
   f. When searching an employee's computer, care should be taken in the appropriate selection of key words, search criteria and files so that the search will be circumscribed and tailored.
   g. Consult legal counsel and forensic experts concerning the advisability of whether, how, or with what constraints e-mail or other messages can or should be reviewed.

Finally, counsel should always be mindful of ethics rules that apply when they come into possession of communications between an employee and his or her lawyer.

The policy should state that it can only be changed in writing by a high level official (stating the individual's title), and it should be enforced consistently. Employees, including supervisors and managers, should be trained about the policy and the systems that it covers, and should be reminded periodically that this policy is a priority of the company.

*The *Stengart* case is discussed more fully at http://www.eapdlaw.com/newsstand/detail.aspx?news=1896

BOSTON MA | FT. LAUDERDALE FL | HARTFORD CT | MADISON NJ | NEW YORK NY | NEWPORT BEACH CA | PROVIDENCE RI
STAMFORD CT | WASHINGTON DC | WEST PALM BEACH FL | WILMINGTON DE | LONDON UK | HONG KONG (ASSOCIATED OFFICE)

Mark E. Schreiber, Partner 617.239.0585 mschreiber@eapdlaw.com
Barbara A. Lee, Counsel 973.520.2308 blee@eapdlaw.com