Employee communications

How to balance privacy with employer policies **Interviewed by Chelan David**

More than 47 billion nonspam e-mails are sent every day, and many of those pass through an employer's e-mail system or an employer-provided mobile device.

"As of mid-2010, approximately 40 percent of corporate employees used employer-provided mobile devices to send and receive electronic messages," says Andrew D. Campbell, a commercial litigation partner at Novack and Macey LLP.

Managing e-mails can be time consuming and costly for employers, says Campbell. The time and expense of regulating e-mails can be exacerbated when employees send or receive personal e-mails on employer-provided devices. Personal e-mails sent through employer-owned devices raise unique issues such as who owns these e-mails, and what, if any, expectations of privacy do employees have with respect to nonbusiness e-mails sent via corporate devices?

Smart Business spoke with Campbell about the rights of employers to access e-mail sent on company-owned devices and how an e-mail policy can help protect employers.

What are some of the issues regarding employees sending personal e-mails through their employers' devices?

Some organizations allow their employees to use employer-owned mobile devices or e-mail systems to send or receive occasional personal messages.

These organizations tend to believe that requiring an employee to use two devices — an employer-provided device for business and an employee-provided device for personal use — will result in employees opting to carry just their own device after hours and on weekends. For these employers, the benefit of greater access to their employees seven days a week outweighs the costs associated with employees sending and receiving personal messages. However, many employers prohibit employees from using employer-owned devices for personal or nonbusiness use. So why do employees continue to send personal e-mail despite these policies? Likely because they feel they can get away with it.

A recent study found that while 95 percent of organizations have policies in place for mobile devices, only 10 percent say that enforcing restrictions on their use is 'very easy.' In light of the fact that more than 47 billion e-mails are sent each day, employees may send personal e-mails believing that there is minimal chance that their personal messages will be detected.

Andrew D. Campbell
Commercial litigation partner
Novack and Macey LLP

Why would an employer want to review an employee's e-mail?

For the most part, employees use e-mail accounts as permitted by their employers. Yet, there are some who use their accounts to break the law, disparage an employer or transfer trade secrets or confidential information outside an organization. Incoming e-mails can also be a source of electronic viruses, and employers may monitor these e-mails for security purposes. Reserving the right to review an employee's company-provided e-mail can be extremely important to maintaining the security and integrity of an organization.

When is it permissible for an employer to review personal e-mails?

As with most legal questions, the answer is, 'It depends.' Among other things, it depends on whether the employer is a government entity or a private business. Government entities, even when acting in their capacities as employers, are bound by the Fourth Amendment, which prohibits the government from making unreasonable searches of people's property or effects. Private employers, while not bound by the Fourth Amendment, must still be concerned with potential claims for invasion of privacy.

While the analysis under the Fourth Amendment and privacy claims can differ, one element they share is that employees must have a reasonable expectation of privacy. If there is no reasonable expectation of privacy, an employer's review of an employee's e-mails is far less likely to be regarded as violating the law.

How do courts assess whether an employee has a reasonable expectation of privacy?

There are a number of factors that courts will consider. Four of the most common questions addressed are, does the organization maintain a policy banning personal or other objectionable use? Does the organization monitor the use of the employee's computer or e-mail? Do third parties have a right of access to the computer or e-mails? And did the organization notify the employee of, or was the employee aware of, the use and monitoring policy? The more factors that are present, the more likely it is that a court will find that an employee had no reasonable expectation of privacy in his or her e-mails.

Other factors that courts have considered — although these factors are generally not outcome determinative — include whether the employee has a password; whether anyone other than the employee knew the password; and whether the employee has a private office or a more visible workspace. The harder it is to access an employee's e-mails, the more likely it is that a court will find there is an expectation of privacy.

What provisions should an organization's e-mail policy include?

Regardless of whether an employer allows personal e-mail, to minimize the risk of liability from an employee-initiated claim for privacy violation, a policy should, among other things, be in writing; be signed by each employee to whom it applies; state that employees do not have any expectation of privacy in e-mails; notify employees that e-mails may be monitored by the employer; state that all communications sent or received through an employer's software or hardware are property of the employer; and prohibit the use of employer software or hardware for illegal or harassing purposes.

An alert, reminding employees of the policy when they sign onto their accounts, can also help shield employers from liability for claims of invasion of privacy. <<

ANDREW D. CAMPBELL is a commercial litigation partner at Novack and Macey LLP. Reach him at acampbell@novackmacey.com or (312) 419-6900.

Insights Legal Affairs is brought to you by Novack and Macey LLP