How Private is Private? Employee Communication in the New Digital Age

8/12/2010

Tara M. Kennedy

Most employers have long had a policy in place governing how employees can use company computers. The policy was probably drafted when all the employer had to worry about was e-mail and maybe access to the Internet. One thing we can be sure of in this technological era is that we can't keep up with how quickly things change.

Today, not only do employers need to worry about e-mail and the Internet, but there is instant messaging, access to personal e-mail accounts from work computers and text messaging from company-owned phones. In fact, "texting" has become so prolific that some states, including Michigan, have passed laws to keep people from texting while driving.

This new technology raises all kinds of issues for employers. Problems like "textual harassment," violations of company EEO policies via Internet access and even something as basic as so-called "cyber loafing." What might get lost in all of this is the employee's right to privacy.

Most employees are entitled to privacy when they have what is commonly called a "reasonable expectation of privacy." If you are sitting in your office with the door closed and locked, you generally have a reasonable expectation of privacy. On the other hand, if you work out in the open, you might not have the same expectation of privacy.

That, of course, is why most employers include in their computer use policies a statement that says the company owns the computer and everything on it, and that the company can look at an employee's computer or e-mail or Internet use, whenever it wants. With all of this new technology, employers may be wondering how far this reasonable expectation of privacy goes. A couple of recent case have helped define the boundaries.

In *Quon v. City of Ontario*, the Supreme Court of the United States set out to determine whether searching an employee's text messages was reasonable. The case involved a police officer who frequently exceeded the text-message limit on his work-issued pager. As a result, he constantly had to pay overage charges to his employer. The employer grew tired of being a bill collector and decided to conduct an audit to determine whether the existing character limit was too low for work purposes. The audit revealed that only a fraction of the messages sent and received by the officer were work related – out of 456 messages, 400 were personal and the majority of the personal texts were sexually explicit conversations with the police officer's wife or girlfriend.

The city's computer policy stated: "Users should have no expectation of privacy or confidentiality when using city computers." Additionally, employees had been told that the city considered pager messages the same as e-mail messages. However, a supervisor had told the offending police officer that the city did not intend to audit his text messages. Nevertheless, the city disciplined the officer for violating its computer policy by sending the sexually explicit messages. He sued.

In declining to take a broad stance on an employee's privacy expectation, the Supreme Court determined that because the employer had a legitimate motive to search the employee's messages, the search was reasonable and the employee had no reasonable expectation of privacy. Even though the case involved public employees, the reasoning seems equally applicable to private employees.

But not all cases are going the employer's way. In *Stengart v. Loving Care Agency, Inc.*, the plaintiff filed a discrimination lawsuit against her employer who, in anticipation of litigation, "hired a computer forensic expert to recover all files stored on the laptop." The files recovered included e-mails the employee exchanged with her attorney through her personal e-mail account. The New Jersey Supreme Court held that the employee could reasonably expect that "e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney-client privilege."

The Court reached its decision by analyzing the adequacy of the notice provided by the company policy. The specific language of the policy gave the employer the right to review and "access all matters on company computers, media systems and sertices at any time." In addition, e-mail messages are plainly "considered part of the company's business . . . records." The Court determined that because the policy used general language; never defined the terms "media systems and services;" and did not address personal e-mail accounts, "employees did not have express notice that messages sent or received on a personal, Web-based e-mail account [were] subject to monitoring if company equipment [was] used to access the account."

Additionally, the Court also pointed out that the computer policy contained some ambiguities, such as stating: "e-mails are not to be considered private or personal to any individual employee…[however,] occasional personal use [of e-mail] is permitted." An employee's reasonable expectation of privacy is determined on a case-by-case basis. The Court determined that the combination of the ambiguous language in the policy, the steps the employee took to protect her privacy by using a personal, password-protected e-mail and not saving the account's password created an expectation of privacy for the employee.

What both of these cases make clear is that it is vitally important for employers to revisit their computer use policies on a periodic basis to at least try to keep up with technology.