Mark Wiletsky

Partner
303.473.2864
Boulder
mbwiletsky@hollandhart.com

City Had Right To Review Employee's Text Messages

City Had Right To Review Employee's Text Messages

Insight — 6/17/2010 12:00:00 AM

If your employees send or receive text messages, e-mails, or otherwise communicate with modern technology while at work, a decision today from the U.S. Supreme Court (*City of Ontario, California, et al. v. Quon et al.*) could impact you. The U.S. Supreme Court unanimously decided that the City of Ontario, California did not violate an employee's Fourth Amendment privacy rights when it reviewed two months' worth of his text messages, many of which involved non-work related matters (Click here to see the decision on the U.S. Supreme Court's website). Although this case involved constitutional protections against unreasonable searches that apply to public employees, the decision has important lessons for private employers as well. Private employers, like public ones, can be sued if they overstep their bounds in monitoring employees' e-mails, text messages, or other communications. Most employers do not want to be sued, let alone forced to take a case all the way to the Supreme Court to prove they were right. By taking a few basic measures, employers can minimize the risk of such lawsuits.

At a minimum, the *Quon* case reinforces the importance of having a clear computer or technology resources policy in place. The policy should, among other things, state that employees have no expectation of privacy in e-mails or other communications on the company's technology resources, and that the company has the right to monitor or review any communications or content sent or received through or on its resources. Depending on where your employees are located, be careful not to overstep boundaries. For example, communications between an employee and her attorney might be privileged and confidential, even if sent or received through your computer network. Similarly, talk to your attorney before accessing an employee's personal e-mail account. Second, if you have not updated your computer use policy recently, consider doing so. Technology is rapidly evolving. The terms used in your policy from a year or two ago might not cover the technology in use today. At the same time, consider reviewing or creating a policy addressing employees' use of social media. As the use of social media becomes more prevalent, employers need to be sure they have set clear guidelines on the topic. Third, make sure the policy is distributed to all employees. Better yet, have your employees acknowledge receipt of the policy, either through an e-mail confirmation or by signing a hard copy. That way, no one can say that they were unaware of the policy or the organization's right to monitor use of its resources.

If you think that the *Quon* case is unique or would never impact your organization, read on. You might be surprised at how familiar it sounds; the situation in *Quon* is not so different from what happens in many

workplaces all over the country.

Background

The City of Ontario had a computer use policy in place. The policy clearly stated that the City had a right to monitor employee e-mail and other network activity, and that employees had no expectation of privacy when using the City's technology resources. Although the policy did not explicitly cover text messages, the City had communicated to employees - both verbally and in writing - that text messages and e-mails would be treated the same under the computer use policy. In other words, the City had a right to monitor those messages, even though they were routed through a third party (Arch Wireless) as opposed to the City's computer system.

Quon, a sergeant and member of the SWAT team, exceeded the monthly limit for his text messages, resulting in additional cost. Quon paid the extra cost, but when he continued to exceed the limit for the next three or four months, the City decided to look into the matter. The City wanted to know whether the character limit for text messages was too low. Therefore, the City obtained two months' of Quon's text message transcripts from Arch Wireless. They discovered that many of the messages were not work related, and in fact many were sexually explicit.

Out of 456 messages sent or received during work hours in one month, no more than 57 were work related. Quon sent as many as 80 text messages in a single day at work. On an average day, Quon sent or received 28 text messages, of which only 3 were work related. Not surprisingly, Quon was disciplined. He then sued the City and Arch Wireless for violating his Fourth Amendment right against an unreasonable search or seizure, and the Stored Communications Act. Arch Wireless and Quon settled, so only the claim against the City remained.

The Supreme Court's Decision

Recognizing the rapidly changing nature of technology and its use in the workplace, the Court undertook a narrow analysis. The Supreme Court concluded that the City did not violate Quon's Fourth Amendment rights by obtaining and reviewing the transcript of his text messages. Essentially, the Court concluded that the "search" or review of those transcripts was reasonable because "it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use," and the review was not "excessively intrusive." The Court went on to note that Quon's expectation of privacy was limited because he knew his messages were subject to auditing, and as a law enforcement officer, he should have known that his actions might be reviewed.

Technology can be both a blessing and a curse. But no one can deny that it is a fact of life in the modern workplace. As a result, employers should address its appropriate use, and limits, with employees, and clearly communicate guidelines to them so that the technology benefits, rather than burdens, the employer.

If you have questions about computer use or technology-related policies,

or other privacy and data security issues, feel free to contact Mark Wiletsky at 303-473-2864 or mbwiletsky@hollandhart.com.
