U.S. Supreme Court Supports Employer's Right to Review Employee's Text Messages Made Using Employer's Property

Jun 22 2010

Posted By: Kyle J. Gulya

Practice Area: Labor and Employment & County and Municipal Governance

In a much-awaited U.S. Supreme Court decision, the Court, in a narrow but unanimous conclusion, upheld a municipal employer's right to search and review the content of text message communications made by employees using the employer's property. In *City of Ontario v. Quon*, No. 08-1332 (2010), the Supreme Court concluded the City of Ontario Police Department and the Police Chief did not violate an employee's Fourth Amendment right to privacy by reading the employee's private text messages made while using City property.

I. APPLICABLE FACTS

The City of Ontario established a "Computer Usage, Internet and Email Policy" addressing "[t]he use of any City-owned computer equipment, computer peripherals, City networks, the Internet, e-mail services or other City computer-related services" and explicitly reserved the City's rights to monitor use with or without notice. The Policy also informed users that they should have "no expectation of privacy or confidentiality when using these resources . . . [and] as such, these systems should not be used for personal or confidential communications." The Policy acknowledgement form was signed by Plaintiff Jeff Quon.

Following the implementation of that Policy, the City assigned pagers to Quon and other Department employees. Each pager was allotted 25,000 characters per month, after which the City paid overage charges. The City's Policy did not expressly address the use of the pagers or wireless text messages. However, the Police Department's Commander held a meeting where he informed Quon and other officers that text messages were "considered e-mail messages" and that those "messages would fall under the City's policy as public information and [be] eligible for auditing." This statement was later memorialized in a memorandum and sent to City employees. The Lieutenant in charge of the pagers, however, collected overage charges from each employee who went over the allotted character amount, and as long as the employee agreed to pay for the charges, the Lieutenant would not audit the content of the text messages. Quon went over the monthly character limit on several months and paid the City for the overages each time rather than having his messages audited.

After a sensitive internal investigation involving the use of pagers by Department dispatchers, the Chief commenced an audit of the pager use of employees with overages. The Chief wanted to determine the efficacy of the existing character limits in order to ensure that officers were not paying for work-related expenses. The ensuing audit of Quon's transcript revealed significant personal and sexually explicit messages. In one month, Quon had sent or received 456 text messages during work hours but only 57 were work related.

Quon argued the search was unlawful because he and the other plaintiffs had a reasonable expectation of privacy in the text messages based on the Lieutenant's informal, unwritten policy that the text messages would not be audited if the employee paid the overages. The City argued the Lieutenant was not a policymaker, and therefore his informal policy could not create an objectively reasonable expectation of privacy, especially since the City's Policy and the statements and meetings of the Commander notified the employees that they should have no expectation of privacy in the contents of the text messages made using Department property.

II. THE SUPREME COURT'S DECISION

The Supreme Court began its analysis by identifying the narrowness of its decision and minimized any far-reaching premise regarding employee expectations of privacy when using employer-provided communication devices. The Court treated electronic communications no differently than it did an inspection of physical property in the workplace. The Court found that where an employee has a legitimate privacy expectation, a public employer's intrusion and search "for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct" is permissible if the search is "'justified at its inception'" and if "'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of'" the circumstances giving rise to the search. The "operational realities" of the workplace can diminish an employee's privacy expectations and is considered when assessing the reasonableness of a workplace search.

The Department's review of the text messages was justified at its inception because there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose." The Chief ordered the search in order to determine whether the character limit was sufficient to meet the City's needs—a "legitimate work-related rationale." The Department had legitimate interests in ensuring that employees were not being forced to pay for work-related expenses and the City was not paying for extensive personal communications. Reviewing the text messages 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. The search was not excessively intrusive, because the Department only reviewed two months of messages where overages occurred. The Court even noted the search could have been broader when it said, "it may have been reasonable as well for [the Department] to review transcripts of all the months in which Quon exceeded his allowance."

The Court also noted that public employees, and particularly law enforcement officers, cannot illicitly claim privacy and immunity for their actions. The Court stated:

it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing. As a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. Given that the City issued the pagers to Quon and other SWAT Team members in order to help them more quickly respond to crises—and given that Quon had received no assurances of privacy—Quon could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team's performance in particular emergency situations.

Even though there were less intrusive ways to conduct the search of the text messages, the Court reiterated that it has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."

III. DISCUSSION

There are several lessons that employers should learn from *Quon*. First, while the Court reminded employers that the *Quon* decision is unique to the facts of that case and is to be treated narrowly, the Court did identify several purposes for searches of the content of employee text messages that may be appropriate. These purposes include inspection of the employer's property for "performance evaluations, litigation concerning the lawfulness of police actions, and perhaps compliance with state open records laws." The Court, however, hinted that it may find some searches even more intrusive than the review of text messages, such as a search of an employee's personal email account or a wiretap on the employee's phone line.

More importantly, the Supreme Court's decision reinforces the need for well-crafted and consistently enforced policies. The Court identified this need when it stated "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated." Even the best-crafted policy can be less useful if the policy is not enforced.

Employers can learn from the problems the City of Ontario faced. The City's electronic communications policy was narrow and outdated because it did not affect all forms of electronic communications and only stated that it applied to use of the employer's network and not networks of other entities used by the employer. Through meetings and written memoranda, the City attempted to clarify its position without revising its policy by notifying employees that pager messages would be treated as email communications and that employees should not have any expectation of privacy. Another supervisor, however, then developed his own plan for managing the pagers.

The resulting direction for employers is to be clear and unequivocal in policy development, implementation and enforcement. Now is the time for employers to develop or revise and properly implement and enforce "use of property" policies, "computer and network use" policies and general "workplace communication" policies to address cutting-edge technological changes and to address the communication habits of employees. As you develop, implement and enforce policies, keep in mind the following important guidance:

- Remind employees, in writing, that they should have no expectation of privacy nor any confidentiality in any communications made while using the employer's property and employer-provided resources unless those communications are otherwise protected by law. These communications include any communications made on-duty or off-duty and over any private email system or other private communication system like Facebook or chat functions.
- Remind employees that they need to always use the employer's property in furtherance of the interests of the employer and in compliance with all applicable laws including record retention laws.
- Remind employees that management will monitor all use of its property and may do so at any time.
- Establish professional use expectations and consequences for improper use of employer property.
- Train supervisors to effectively and consistently enforce policies and procedures. Policies are policies of the employer, not of the individual supervisor. A policy should reaffirm that no individual supervisor has the authority to change policy of the organization without approval and action of the governmental body or chief policy maker adopting the policy.
- Require employees to sign a form acknowledging receipt of the policy and a statement of understanding the policy with the affirmative duty of the employee to ask questions of a specific supervisor who is qualified to answer such inquiries.
- Enforce the policies, and monitor enforcement to ensure compliance and effective and consistent enforcement.

Employers should take other preventative measures to minimize the risk of liability similar to that in *Quon*. For example, when new communication devices or systems are implemented, require employees to provide written acknowledgment of their understanding of the business use of such devices or systems, the employee's understanding that they have no expectation of privacy in the use or contents of these devices or systems, and the employee's consent to full release and disclosure of the contents of the device or system, regardless of whether the contents are stored in the device or on a provider's network and regardless of when such information is requested or accessed by the employer.
