Client Alert

pillsbury

Privacy, Data Security & Information Use

Employment | Communications

June 22, 2010

U.S. Supreme Court Reminds Employers to Update E-Communication Privacy Policies

by Christine Nicolaides Kearns and Rebecca Carr Rizzo

On June 17, the U.S. Supreme Court unanimously upheld the legality of the Ontario, California Police Department's audit of police Sgt. Jeff Quon's text messages on his department-issued pager, in City of Ontario v. Quon. *Declining to issue a broad holding on employee privacy rights in electronic communications, the Court decided the case on the narrow point that, even assuming that Quon had a reasonable expectation of privacy in his text messages, the search was reasonable because it was motivated by a legitimate work-related purpose and was not excessive in scope. Nonetheless, the opinion emphasized the importance of well-crafted employer privacy policies, noting that "employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."*

In *Quon*, the City of Ontario had issued pagers to Quon and other SWAT team members. Before distributing the pagers, the City provided a "Computer Usage, Internet and E-Mail Policy." This policy stated, in part, that the City "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." The policy did not apply to text messages specifically, but the City made clear to its employees during a staff meeting and then later in a written memorandum that text messages sent on the department-issued pagers were to be considered e-mails subject to this policy.

After Quon initially exceeded his monthly text message character allotment, his lieutenant reminded him that text messages could be audited pursuant to the policy, but told Quon that was not his intent. Quon then reimbursed the City for the overage free. However, after Quon repeatedly exceeded his character limit, the department chief decided to determine whether the existing character limit was too low or whether these overages were the result of the pagers being used for personal messages.

The department requested transcripts from the service provider of the text messages sent during August and September 2002 by Quon and another employee who had exceeded the character allowance. Many of Quon's messages were not work-related and some were sexually explicit. The department's Internal Affairs division conducted a review limited to Quon's messages sent during work hours in August and September 2002. Internal Affairs determined that Quon had violated the department's rules, and Quon was reportedly disciplined for this misconduct.

Quon filed suit alleging violations of the Fourth Amendment, the Stored Communications Act, and California law.

In deciding this case, the Court specifically declined to issue any broad pronouncements regarding the privacy rights of employees, stating:

"The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear . . . Prudence counsels caution before the facts of the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."

Preferring to dispose of the case on more narrow grounds, the Court assumed that Quon had a reasonable expectation of privacy in his text messages and assessed the specific facts of the case to analyze whether the search was reasonable. The Court found it was reasonable because (1) the City "had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand that the City was not paying for extensive personal communications" and (2) the scope of the search 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 was not "excessively intrusive."

Finally, the Court held "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."

The *Quon* decision contained a few additional noteworthy comments by the Court:

- The Court acknowledged but did not resolve the parties' disagreement over whether the lieutenant's initial comments that Quon's text messages would not be audited overrode the department's policy, creating a reasonable expectation of privacy in his test messages;

- The Court, in light of the department's policy in this case, highlighted the distinction between e-mails that are transmitted through a company's own server and text messages that are transmitted through a wireless provider's network, but ultimately concluded that the policy covered both;

- The Court noted that the department's audit of Quon's text messages on his employer-provided pager was "not nearly as intrusive as a search of his personal e-mail account or page, or a wiretap on his home phone line";

- In overruling the Ninth Circuit's finding that the search was unreasonable, the Court made clear that it has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."

While the Court's opinion was fact-specific and decided on narrow grounds, it provides useful guidance to employers on how to handle privacy policies. Based on the *Quon* decision, employers are advised to:

- Implement a well-crafted and up-to-date written policy covering electronic communications that is widely distributed, and require written acknowledgements of receipt by employees. This policy should clearly state that employees do not have an expectation of privacy in electronic communications sent or received on any employer-provided device and that the employer may monitor and review such electronic communications. This policy should extend to all electronic communications sent or received from employer-provided devices, not just those sent through the employer's server. The policy should also clearly establish that it can only be altered in writing by certain specified individuals with proper authority. Finally, the policy should alert employees that violations of the policy may lead to discipline up to and including termination.

- Provide training regarding the electronic communications policy to employees and supervisors and managers;

- Ensure that investigations into potential misconduct are conducted only for a legitimate work-related purpose and are properly limited in scope; and

- Stay abreast on changes in the technological and legal landscape and consult with counsel when implementing such policies and when possible violations of the policies arise.

If you have any questions about the content of this client alert, please contact the Pillsbury attorney with whom you regularly work or the authors below.

Christine Nicolaides Kearns (bio)
Washington, DC
+1.202.663.8488
christine.kearns@pillsburylaw.com

Rebecca Carr Rizzo (bio)
Washington, DC
+1.202.663.9143
rebecca.rizzo@pillsburylaw.com