

June 30, 2010

## U.S. Supreme Court Upholds Employer Searches and Underscores Importance of Electronic Communications Policies

Technology, the final frontier. These are the voyages of the U.S. Supreme Court. Its current mission: to explore strange new electronic communication devices; to boldly go where no court has gone before.

In its pioneer voyage into the perilous realm where workplace monitoring of a new technological device meets an employee's reasonable expectation of privacy, the United States Supreme Court issued a unanimous decision that provides guidance on steps employers can take to reduce an employee's privacy expectations and emphasizes the importance of having a clear, well-defined privacy policy. The Supreme Court decided *City of Ontario v. Quon* on June 17, 2010, holding that the City of Ontario did not violate an employee's Fourth Amendment privacy rights when it reviewed personal text messages that the employee sent and received on his employer-owned and issued pager.<sup>1</sup>

While *Quon* is the first case in which the Supreme Court had an opportunity to address a public employee's expectation of privacy in the workplace concerning text messaging and electronic communication devices, such as pagers and PDAs, the Court declined to set precedent on the issue of employee privacy expectations in workplace communications. The Court leapfrogged the question of whether the employee had a reasonable expectation of privacy in his text messages by instead focusing on the purpose and scope of the search, namely, whether the search was reasonable. Given the uncertainty in workplace norms and the role emerging technology plays in society, the Court limited its holding to the specific facts of the case. The Court left unresolved the question of how much discretion a public employer has to review an employee's workplace electronic communications, but the *Quon* decision has important implications for private sector employers and the implementation and use of search policies.

### Background of Quon

The City of Ontario issued pagers capable of sending and receiving text messages to Jeffrey Quon and other SWAT Team members to help the SWAT Team respond to emergency situations. Arch Wireless provided wireless service for the pagers, and under the City's service contract with Arch Wireless, each pager had a monthly allotment on the number of characters sent or received. If an employee exceeded the monthly allotment, Arch Wireless charged the City overage charges.

The City had a written electronic communications policy that warned employees of the City's right to monitor computer, internet, and e-mail usage. The policy further informed employees that they did not have an expectation of privacy or confidentiality in these electronic communications. Although the policy did not expressly apply to text messages or pagers, the City made clear to employees that it would treat text messages in the same manner as e-mails – meaning that the City could also audit text messages. Despite the City's policy, Lieutenant Steven Duke, the Ontario Police Department officer responsible for the City's contract with Arch Wireless, told Quon that he did not intend to audit text messages for personal use if the officer reimbursed the City for the overage fee. Quon exceeded his character limit several times and each time paid the overage charges.

<sup>1</sup> *City of Ontario v. Quon*, 560 U.S. \_\_\_ (2010).

When Lt. Duke eventually grew tired of being a “bill collector,” the City decided to review the officers’ text messages to determine whether the existing character limit was too low, namely, whether officers were paying overage fees for work-related messages or if the overages were for personal messages. Arch Wireless provided the City with transcripts of the text messages of Quon and another employee who exceeded the monthly character allowance. The review revealed that the vast majority of Quon’s messages were personal and some were sexually explicit. After Quon was disciplined for violating police department rules, he filed a lawsuit, alleging that the City violated his privacy rights under the Fourth Amendment and the California Constitution by reviewing his personal text messages without his consent.

The U.S. Court of Appeals for the Ninth Circuit held that Quon had a reasonable expectation of privacy in his text messages based on the “operational realities” of the police department. Conceding that the City’s search was conducted for a legitimate work-related purpose, the Ninth Circuit nevertheless concluded that the search was unreasonable because the City could have used less intrusive means to determine the reason for the overages, such as warning Quon or allowing him to redact the personal messages from the transcripts.

### **U.S. Supreme Court Analysis**

The Supreme Court reversed the Ninth Circuit, holding that the City’s review of the text messages did not violate Quon’s Fourth Amendment privacy rights. Recognizing that its earlier opinions had not clarified the threshold test for determining the scope of a public employee’s Fourth Amendment privacy rights, the High Court nonetheless declined to address more broadly the privacy expectations of employees when using employer-issued communication devices. Instead, the Court assumed: (1) that Quon had a reasonable expectation of privacy in his text messages; (2) that the City’s review constituted a search under the Fourth Amendment; and (3) that the principles applicable to a government employer’s search of an employee’s physical office also apply to the search of an employee’s electronic communications.

Disposing of the case on narrow grounds, the Supreme Court warned that “[p]rudence counsels caution before the facts in 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.” The Court explained that the “judiciary risks error” by addressing the Fourth Amendment implications of emerging technology given the uncertainty of what society accepts as proper behavior concerning electronic communications in the workplace. The Court also feared that a broad holding concerning employees’ privacy expectations vis-à-vis employer-provided technological equipment might have unpredictable repercussions for future cases, thus warranting a holding based on the specific facts of the case.

Turning to the “reasonable” search issue, the Supreme Court found that the City’s search was motivated by a non-investigatory, work-related purpose because the City sought only to determine whether the employees had been provided with an adequate limit on the number of text message characters. The Court agreed that the City had a legitimate interest in ensuring that it was not forcing employees to pay for work-related expenses or, alternatively, that it was not paying for employees’ personal communications. The Court determined that the scope of the search was reasonably related to its objective because reviewing the transcripts was an “efficient and expedient” method for determining the source of Quon’s overages. Moreover, the search was not excessive because the City had limited its review to two months, even though Quon had gone over his monthly allotment a number of times. The Court additionally rejected the Ninth Circuit’s least intrusive means approach, stating that the search was not unreasonable merely because the City could have employed less intrusive means.

The Supreme Court also explained that the extent of Quon's expectation of privacy was relevant to assessing whether the search was too intrusive. The Court reasoned that Quon should have known his communications were not immune from scrutiny based on the following factors: (i) the City told him that his messages were subject to auditing; (ii) as a law enforcement officer he should have known that his actions were likely to come under legal scrutiny; and (iii) given the purpose behind the pagers, Quon should have known that the City may audit pager messages to assess the SWAT Team's performance and proper use of the pagers. The Court also noted that the City's audit of messages on Quon's employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager.

In summary, the *Quon* decision stands for the proposition that even if an employee has a reasonable expectation of privacy in the physical place, object, or electronic communication searched, the government employer does not violate the Fourth Amendment if the search is reasonable – meaning that it is conducted for a legitimate work-related purpose and is not excessive in scope. Nevertheless, the Court expressly narrowed its holding to the specific facts of this case; therefore, sweeping generalizations regarding an employee's privacy expectations and Fourth Amendment law on electronic communications should be avoided.

### Lessons for Private-Sector Employers

Despite the Supreme Court's reticence to voyage into the broader issue of a public employee's reasonable expectation of privacy in the workplace and, in particular, electronic communications, the dicta in the *Quon* opinion suggests certain practices that employers can implement to help reduce potential exposure to similar employee privacy claims. While the Fourth Amendment only regulates the conduct of governmental actors and, thus, *Quon* technically applies only to public employers, the decision has implications for private-sector employers, as private employees may have privacy protection under certain state constitutions, statutes, and common law.

To safeguard against privacy claims, employers should ensure that they have appropriate policies in place to apprise employees that electronic communications transmitted on employer equipment, systems, or networks are not private or confidential and are subject to monitoring:

- First and foremost, employers should establish a formal, written electronic communications and privacy policy and make it broad enough to cover emerging and evolving technologies.
- The written policy should explicitly state that employees have no expectation of privacy when using any of the employer's electronic communication equipment, systems, or networks, and that the employer has the right to monitor, audit, and search employee communications and systems' usage.
- Employers should clearly communicate their workplace policy to all employees and require each employee to sign an acknowledgment form, acknowledging the employee's review and acceptance of the policy.
- The policy should also stress that it can only be modified by a written document issued or signed by the President, CEO, or Director of Human Resources.
- Employers should ensure that managers and supervisors consistently communicate the policy and do not alter it by verbal assurances.

- Employers should provide training to employees, managers, and supervisors regarding the privacy policy.
- Employers should consider issuing policy reminders to provide repeat notice and inform employees of any changes or updates to the policy.
- If a need for an employee search arises, employers should make certain that the search is legally defensible – it is for a legitimate work-related purpose and reasonably tailored to that purpose.
- Finally, employers should monitor changes in technology or the legal landscape regarding an employee's expectation of privacy at work and consult with counsel if a question arises or if a possible violation occurs.

*Quon* underscores the importance of preparing for the next frontier by crafting employment policies that eliminate employee expectations of privacy in communications made on employer-issued devices or network systems. The Labor and Employment Practice Group of Haynes and Boone, LLP has significant experience in drafting employment policies on electronic communications and assisting employers to address employee privacy concerns.

For more information, please contact the Haynes and Boone attorney with whom you work or any of the following attorneys in the firm's [Labor and Employment Practice Group](#):

[Arthur T. Carter](#)  
214.651.5683

[arthur.carter@haynesboone.com](mailto:arthur.carter@haynesboone.com)

[Matthew T. Deffebach](#)  
713.547.2064

[matthew.deffebach@haynesboone.com](mailto:matthew.deffebach@haynesboone.com)

[Felicity A. Fowler](#)  
713.547.2072

[felicity.fowler@haynesboone.com](mailto:felicity.fowler@haynesboone.com)

[Melissa M. Goodman](#)  
214.651.5628

[melissa.goodman@haynesboone.com](mailto:melissa.goodman@haynesboone.com)

[Meghaan McElroy](#)  
713.547.2082

[meghaan.mcelroy@haynesboone.com](mailto:meghaan.mcelroy@haynesboone.com)

[Brenna G. Nava](#)  
210.978.7430

[brenna.nava@haynesboone.com](mailto:brenna.nava@haynesboone.com)

[Dean J. Schaner](#)  
713.547.2044

[dean.schaner@haynesboone.com](mailto:dean.schaner@haynesboone.com)

[William C. Strock](#)  
214.651.5623

[bill.strock@haynesboone.com](mailto:bill.strock@haynesboone.com)

[Jonathan C. Wilson](#)  
214.651.5646

[jonathan.wilson@haynesboone.com](mailto:jonathan.wilson@haynesboone.com)