

U.S. Supreme Court Rules in *Quon*: Employee Text Messages Not Shielded from Employer Review

June 18, 2010

In a much-anticipated opinion in the *Quon*¹ matter, on June 17 the U.S. Supreme Court declined to set precedent on broad issues of employee privacy expectations in workplace communications. Instead, the unanimous Court ruled narrowly, reversing the decision of the Ninth Circuit by holding that the review of an employee's text messages sent using employer-issued electronic devices did not, under the circumstances in that case, violate traditional Fourth Amendment reasonable search standards.²

Acknowledging that it was in sensitive and uncharted territory and, therefore, should "proceed with care," the Court noted that it "risked 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 communications devices." Nevertheless, the Court's analysis and dicta suggest factors that may be weighed by future courts in addressing these issues.

***Quon* Facts**

In *Quon*, the City of Ontario (the City) acquired two-way pagers for use by Ontario Police Department (OPD) SWAT team members, including Sergeant Quon, to assist with responding to emergencies. Under the City's contract with service provider Arch Wireless, each pager was allotted 25,000 characters per month, after which overage fees would accrue. When it issued the pagers, the City did not have in place a formal pager-use policy. It did, however, have a computer usage, Internet, and email policy which warned that all network activity might be monitored and that users had no expectation of privacy or confidentiality when emailing or when using network resources. Quon signed an acknowledgment of this policy.

¹ *City of Ontario, Cal. v. Quon*, No. 08-1332 (2010), issued June 17, 2010.

² For a fuller exploration of the underlying facts and lower court rulings, see the eData LawFlash, "Ninth Circuit Ruling: Employee Text Messages Shielded from Employer Review," June 26 2008, available at: http://www.morganlewis.com/pubs/eData_LF_TextMessagesShielded_26jun08.pdf.

Once the pagers were in use, the City made clear to employees, including Quon, that it would treat text messages in the same way as email messages. Some City employees also developed an informal policy concerning fees for exceeding the monthly character limit, allowing individual users to pay overage charges with the understanding that if they paid, their usage would not be audited.

The OPD later opened an internal investigation to establish the adequacy of the character limit. As part of this investigation, the department obtained transcripts of Quon's text messages from service provider Arch Wireless for two of the several months in which Quon exceeded the character limit. Messages sent outside of work hours were redacted. Review of the transcripts revealed that most of Quon's work-hours communications were personal and included sexually explicit messages, some of which he sent to coworkers within the department.

Procedural Issues and Legal Analysis

Quon and others implicated by the transcripts, including coworkers and Quon's then-wife, sued Arch Wireless and the City, claiming that Arch had violated the Stored Communications Act (SCA)³ and that the City had violated their Fourth Amendment rights. On a motion for summary judgment, the district court held that Arch had not violated the SCA and that, although Quon had a reasonable expectation of privacy, neither the City nor the OPD had violated the Fourth Amendment.

On appeal the Ninth Circuit reversed. While agreeing that Quon had a reasonable expectation of privacy in his text messages, the court found that the search was unreasonable and listed less intrusive means that could have been used to determine the reason for the overages, including warning Quon or allowing him to redact the transcripts. The court also held that Arch violated the SCA.

Having granted certiorari only on the Fourth Amendment issues, the Supreme Court reversed the Ninth Circuit. Previously in *O'Connor*⁴ the Supreme Court majority held that "special needs, beyond the normal need for law enforcement," can make warrant and probable cause requirements impracticable for government employers, and developed a two-part test for determining whether a Fourth Amendment right has been violated. First, a court must decide if the employee has a reasonable expectation of privacy, considering the "operational realities of the workplace," to determine if privacy rights are implicated. If a legitimate privacy expectation is found, the court proceeds to the second part of the test to determine if, under all of the circumstances, the intrusion into that right is reasonable.

Rather than deciding whether Quon had a legitimate privacy expectation, the Court focused on the reasonableness of the City's text message review. Assuming, *arguendo*, that Quon did have a reasonable expectation of privacy in the text messages, that the City's review constituted a search under the Fourth Amendment, and 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, the Court still found that the City's actions were reasonable.

In *O'Connor*, the plurality reasoned that when conducted for a "non-investigatory, work-related purpose" or for the "investigation of work-related misconduct," a government employer's warrantless

³ 18 U.S.C. §§ 2701-2711.

⁴ *O'Connor v. Ortega*, 480 U.S. 709, 711 (1987).

search is reasonable if it is “justified at its inception” and “the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in life of the” the circumstances giving rise to the search. Here, the City sampled Quon’s messages, redacting those which occurred while not on duty. Moreover, the Court held that the review was the most efficient way for the City to assess whether the messages were professional or personal. The City was furthering a legitimate work-related purpose by ensuring that employees were not being required to pay work-related expenses out of their own pockets, and that the City was not paying for employee personal communications.

Finally, the Court reasoned that as a law enforcement officer, Quon should have known that his communications could be subject to legal scrutiny and audit. Because they were predicated solely on the search’s unreasonableness, the privacy violation claims of those with whom Quon communicated also failed.

Lessons from *Quon*

The Court decided *Quon* under the Fourth Amendment of the U.S. Constitution, which only regulates the conduct of governmental actors. Consequently, the decision technically applies only to public employers. Nonetheless, the decision ultimately could have broader implications for private employers as well. Private employees have privacy protection under some state constitutions, statutes, and the common law. In defining the scope of this protection in the future, lower courts may be influenced by some of the Supreme Court’s observations about the reasonableness of the City’s conduct in *Quon*. The Court’s overall approach suggests that the practices listed below will help reduce the potential exposure to any employer facing similar issues.

Though the opinion does not address head-on the issue of employee privacy expectations in workplace communications, there is still much in the Court’s analysis and overall approach that may serve to curb a proliferation of privacy claims in the private sector.

The Morgan Lewis team can help clients with developing policies and procedures that take advantage of the Supreme Court’s guidance, positioning an employer to face these issues by establishing the following practices:

- Establish and clearly disseminate formal, written electronic communications and systems usage policies, broad and flexible enough to cover emerging technologies, and update them regularly as the practical implications of new technologies become clear
- Establish and disseminate explicit statements that employees have no privacy, confidentiality or ownership expectations in data stored on company systems or in any communications generated using employer provided devices
- Formally disseminate, and require an acknowledgement for, all policies and modifications
- Provide clear notice that communications and systems usage may be monitored and audited
- Put in place monitoring practices, including taking measures to detect and eradicate informal policies and workarounds that may contradict or undercut company policies

If you have any questions or would like more information on any of the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

Dallas

Ann Marie Painter 214.466.4121 annmarie.painter@morganlewis.com

New York

Denise E. Backhouse 212.309.6364 dbackhouse@morganlewis.com
Christopher A. Parlo 212.309.6062 cparlo@morganlewis.com

Palo Alto

Melinda S. Riechert 650.843.7530 mriechert@morganlewis.com

Philadelphia

Stephanie A. “Tess” Blair 215.963.5161 sblair@morganlewis.com
Jacquelyn A. Caridad 215.963.5275 jcaridad@morganlewis.com
Scott A. Milner 215.963.5016 smilner@morganlewis.com
Michael J. Ossip 215.963.5761 mossip@morganlewis.com
Gregory T. Parks 215.963.5170 gparks@morganlewis.com

San Francisco

W. Reece Hirsch 415.442.1422 rhirsch@morganlewis.com
Renée T. Lawson 415.442.1443 rlawson@morganlewis.com

Washington, D.C.

Matthew A. Verga 202.739.5886 mverga@morganlewis.com

About Morgan, Lewis & Bockius LLP

With 23 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, Minneapolis, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.

This LawFlash is provided as a general informational service to clients and friends of Morgan, Lewis & Bockius LLP. It should not be construed as, and does not constitute, legal advice on any specific matter, nor does this message create an attorney-client relationship. These materials may be considered **Attorney Advertising** in some states. Please note that the prior results discussed in the material do not guarantee similar outcomes.

© 2010 Morgan, Lewis & Bockius LLP. All Rights Reserved.