WSGR ALERT

JUNE 2010

U.S. SUPREME COURT UPHOLDS EMPLOYER'S INSPECTION OF EMPLOYEE'S TEXT MESSAGES—*CITY OF ONTARIO V. QUON*

On June 17, 2010, the United States Supreme Court issued its opinion in the closely watched case *City of Ontario v. Quon*. Before the Court was the question of whether a public-sector employer violated an employee's Fourth Amendment privacy rights when it reviewed personal text messages sent and received by the employee on a pager issued by the employer. As discussed below, the Court held that employer's inspection of the text messages was reasonable under the Fourth Amendment and did not violate the employee's privacy rights. The case, though brought against a public-sector employer, provides important guidance for employers in both private and public sectors on the law governing the use of communications technology in the workplace.

Underlying Lawsuit

The underlying case was brought by Jeff Quon, a former sergeant and member of the Ontario Police Department's SWAT team, who was disciplined after an audit of text messages sent and received by him on his employer-provided pager uncovered numerous unofficial, and some sexually explicit, text messages transmitted while Quon was on duty. Quon filed a lawsuit against the City of Ontario, alleging that the city had violated his privacy rights under the California constitution and the Fourth Amendment. He further alleged that the wireless provider had violated the federal Stored Communications Act by disclosing his text messages to the city.

Applicability of an Electronic Resources Policy to Communications Transmitted through a Third-Party Provider

The law is fairly settled that private employers can review employee communications stored on company servers when the employer has provided notice of such monitoring, typically through an electronic resources policy. In *Quon*, the Supreme Court addressed for the first time whether this same right is available to an employer when the employee's communication is transmitted through a third-party provider, such as a wireless telecommunications provider.

The Ontario Police Department had a "Computer Usage, Internet, and E-Mail Policy," in which the city reserved the right to monitor and log network activity. The policy, which was implemented prior to the city's acquisition of the pagers, stated that employees had no expectation of privacy when using the employer's electronic resources, but did not address pagers specifically. At a staff meeting less than six months after the pagers were purchased, however, the officer responsible for the city's contract with Arch Wireless (the third-party wireless provider) made clear to the employees that text messages transmitted on the employer-provided pagers would be treated the same as emails under the computer usage policy, and would therefore be eligible for auditing. The chief of police then distributed a memorandum to the employees formalizing this extension of the computer usage policy to the pagers.

While not making a definitive finding, the Supreme Court suggested that the city's computer usage policy, and therefore the ability of the city to monitor and audit employee communications, extended to the messages sent and received on Quon's employer-issued pager because the city clearly established the extension of the policy to the pagers. Private employers can therefore potentially extend their electronic resources policies to include employee communications transmitted through a third-party service provider, such as a wireless phone provider or a third-party email provider.

To ensure that a company has an unfettered right to review information contained on and transmitted through its electronic systems and devices, including those stored on a third-party server, a company's electronic resources policy should clearly cover not only the use of employer-provided wireless devices, but also communications transmitted to or from employer-provided electronic resources and stored on third-party servers (such as emails sent from the employee's personal email account). If a company's electronic resources policy already has been issued to employees, as in *Quon*, the employer still may be able to extend the policy to cover these third-party stored communications by clarifying that they are subject to the terms of the policy.

Continued on page 2...

U.S. Supreme Court Upholds Employer's Inspection . . .

Continued from page 1...

Ability of a Company Employee to Undermine a Company's Well-Crafted Electronic Resources Policy

The *Quon* case was closely followed by employers, both public and private, because it raised an interesting issue of whether managerial statements could negate the employer's right to inspect information transmitted using employer-provided equipment and resources. In *Quon*, following the city's written extension of its computer usage policy to text messages sent or received on employer-issued pagers, Quon's supervisor told employees that he did not intend to audit the text messages. The Ninth Circuit found these statements created an expectation of privacy on the part of employees and eroded the city's position despite its written policy. The Supreme Court declined to address this issue, noting that "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted." Accordingly, the Supreme Court assumed for the purposes of its analysis that Quon had a reasonable expectation of privacy in the text messages transmitted on his employer-provided pager. However, the Court then concluded that the search was reasonable for business reasons and therefore there was no invasion of privacy.

While the issue of whether an employee has an expectation of privacy in text messages sent and received on an employer-issued device remains open, the Ninth Circuit's holding should serve as a caution to employers that even a clear written policy could be undermined by inconsistent practices. Consequently, employers should take appropriate steps to ensure the electronic resources policy—which, as discussed above, should contain language allowing monitoring of communications stored on third-party servers—is not being undermined by contrary statements made by company employees, particularly supervisors or those employees with apparent authority to make such statements.

If you need assistance creating or updating your electronic resources policy, contact Kristen Garcia Dumont, Cathy Kirkman, Tonia Klausner, Lydia Parnes, Matthew Staples, Gerry Stegmaier, or another attorney in the firm's employment law, media, or consumer regulatory and privacy practice.

WSGR

Wilson Sonsini Goodrich & Rosati

PROFESSIONAL CORPORATION

This WSGR Alert was sent to our clients and interested parties via email on June 21, 2010. To receive future WSGR Alerts and newsletters via email, please contact Marketing at wsgr_resource@wsgr.com and ask to be added to our mailing list.

650 Page Mill Road
Palo Alto, CA 94304-1050
Tel: (650) 493-9300 Fax: (650) 493-6811
email: wsgr_resource@wsgr.com

www.wsgr.com