

Torys on Litigation and Dispute Resolution

L&DR 2008-4
June 24, 2008

U.S. Employers May Need to Revise Their Computer and Internet Policies

By [Christopher Caparelli](#)

A noteworthy decision from the U.S. Court of Appeals for the Ninth Circuit last week, *Quon v. Arch Wireless Operating Company*,¹ counsels employers to review, and perhaps revise, their computer and Internet policies.

Although *Quon* concerned a public employer subject to the Fourth Amendment, the court's reasoning indicates that all employers should review their computer, Internet and email usage policies because courts often employ the same "reasonable expectation of privacy" analysis in private contexts. And employers who contract outside service providers to host electronic communication services, including email, text messaging and proprietary systems such as Bloomberg, must give special attention to this ruling.

The court's decision yields two important results. First, the court concluded that providers of wire and electronic communication services may not provide the contents of those communications to the service "subscriber" without the consent of the "addressee or other intended recipient." Second, the court held that an employer may not be able to rely on its formal computer and Internet usage policies if these policies are not enforced.

Quon arises out of a program run by the City of Ontario, California, in which it distributed to its employees, including its police officers, two-way text-messaging pagers. The City contracted with Arch Wireless to provide wireless text-messaging services for the pagers, but the plan limited each user to 25,000 characters per month. Overages on the character limit incurred additional fees. Because several officers in the Ontario Police Department regularly went over the limit, the department undertook an inquiry to determine whether the overages were the result of work-related or personal messages. The department requested, and received, from Arch Wireless the transcripts of archived messages of several officers, including Jeffrey Quon. As it turned out, many of Quon's messages were personal in nature and often sexually explicit.

The City had no official policy regarding text-messaging pagers, but did have a general policy governing computer, Internet and email usage applicable to all employees. The policy stated, among other things, that employees' use of email and other City computer systems was limited to City-related business and that the use of such tools "for personal benefit is a significant violation of the City of Ontario Policy." The policy further stated that employees' emails and Internet use were not confidential; employees should not expect privacy when using such resources; the contents of electronic transmissions were City property; and the City could review them at any time. Although the policy did not expressly refer to wireless text

To discuss these issues, please contact the author.

For media calls, please contact [Stuart Wood](#), Director, Marketing & Business Development, 416.865.8205.

To contact us, please email info@torys.com.

Torys' bulletins are available on our website at www.torys.com, under Publications.

This bulletin is a general discussion of certain legal and related developments and should not be relied upon as legal advice. If you require legal advice, we would be pleased to discuss with you the issues raised here in the context of your particular circumstances.

© 2008 by Torys LLP.
All rights reserved.

messaging, Quon attended a meeting at which the officers were informed that the pager messages were considered email, which would fall under the City's email policy, and they too could be reviewed at any time. In practice, however, the commanding officer responsible for the police department's pagers told officers, including Quon, that their text messages would not be audited if they paid the overage fee.

The Ninth Circuit first considered whether Arch Wireless violated the federal Stored Communications Act of 1986 (SCA) when it turned over the contents of Quon's text messages to the City. The court held that it did. In the court's view, Arch Wireless is an "electronic communication service" (ECS) that "provides to users thereof the ability to send or receive wire or electronic communications." The SCA prohibits an ECS from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service" unless that person or entity is "an addressee or intended recipient of such communication." Because the City was neither an "addressee" nor an "intended recipient" of Quon's messages, Arch Wireless violated the SCA when it disclosed Quon's messages to the City.

The court then considered whether the City, as Quon's employer, engaged in an unlawful search and seizure of his text messages in violation of the Fourth Amendment to the U.S. Constitution. To make this determination, the court evaluated Quon's reasonable expectation of privacy in the text messages, "which turns on the Department's policies regarding privacy in his text messages." The court acknowledged the City's computer usage, Internet and email policy, observed that Quon had signed a written acknowledgment of the policy and accepted that the policy applied to the text messages. But that did not end the court's inquiry because the formal policy was not the "operational reality" at the police department. Instead, Quon's supervisor had told him that he would not audit the text messages if Quon paid the overage fees; furthermore, the department had not audited any employee's use of the pagers for the eight months the pagers had been in use. According to the court, these facts demonstrate that the department followed an "informal policy" and that Quon reasonably relied on it. He therefore had a reasonable expectation of privacy in the text messages, and the department's review of their contents was improper.

The *Quon* decision has significant implications for employers and providers of electronic communications.² Employers that contract with third-party providers of electronic communication services are likely to be hindered in monitoring these communications. Before a service provider discloses the contents of such communications, it is now likely to require the consent of the recipient (who may not even be an employee) or the consent of the employee who sent the message. If the communications are to be reviewed for purposes of investigating the employee, this consent requirement could greatly compromise the efficacy of such an investigation. Accordingly, employers using third-party service providers may wish to consider migrating their communications systems in-house.

Employers should consider revising their communications policies – or the more comprehensive employee manuals that typically contain these policies – to state that a policy cannot be modified by "informal" practices. For example, the formal policy should state that it can only be modified through a written amendment acknowledged by both employer and employee. *Quon* further suggests that employers maintain a regular practice of monitoring or auditing employee communications to preserve the right to do so when necessary, such as when litigation with the employee arises. While privacy advocates are hailing the *Quon* decision as a landmark ruling, it is likely to add to employers' compliance burdens. **1**

¹ ___ F.3d ___, No. 07-55282, slip op. (9th Cir. June 18, 2008).

² Technically, the *Quon* decision applies only to public employers located in the states covered by the Ninth Circuit: Alaska, Arizona, California, Hawaii, Idaho, Nevada, Oregon and Washington. Its reasoning, however, may be persuasive to other courts in the United States and in the context of private employers.