

Featured Article

Rethinking Your Employee Monitoring Policies after the 9th Circuit's *Quon* Decision

Contributed by:

Amanda Witt and Jon Neiditz, Nelson Mullins Riley & Scarborough, LLP

On June 18, 2008, a panel of three judges from the Ninth Circuit held in *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008) that the Ontario, California police department, a public employer, had violated an employee's constitutional rights under the Fourth Amendment by reading the content of such employee's text messages sent by a pager supplied by the employer police department. For a further discussion of this case, see Bloomberg Law Reports — Privacy & Information, Vol. 1 No. 3 (July 2008).

Employee Expectation of Privacy

The *Quon* decision, however, was widely mischaracterized in the media as representing a holding that an employee's right to privacy in his or her text message is inviolable if such text message is sent using an outside service provider that is not owned by the employer.¹ In fact, the court notes that the specific facts of *Quon* (as more fully described below) involved employee reliance on an informal policy communicated by the employer that created a reasonable expectation of privacy in such employee's text messages. Specifically, the lieutenant in charge of collecting payments from employees for fees associated with overages for monthly text messages exceeding the permitted amount informed the employee plaintiff that the police department would not review the content of the messages if such employee continued to pay for the overages he incurred each month. In *Quon*, the plaintiff exceeded his monthly permitted allotment of characters three to four times and paid the overage each time, but the lieutenant subsequently grew weary of his fee-collecting duties and, along with others in the department, decided to review Quon's messages after requesting them from Arch Wireless, the third party service provider of the text messaging services.

Employer Privacy Policy Covers E-Mail

In *Quon*, the employer police department had a computer use policy explicitly covering an employee's e-mail and Internet use. Quon (a police officer and plaintiff in this case) was verbally informed that the department considered text messages on pagers issued to employees to be e-mails and subject to the department's computer usage policy. The text messaging services were provided by Arch Wireless. At one point, the Ninth Circuit panel stated that the employee would have no reasonable expectation of privacy if not for subsequent communications with

Quon by the lieutenant in charge of collecting the fees for messaging overages. Specifically, the Ninth Circuit panel noted the following:

The Department's general "Computer Usage, Internet and E-mail Policy" stated both that the use of computers "for personal benefit is a significant violation of City of Ontario Policy" and that "users should have no expectation of privacy or confidentiality when using these resources." Quon signed this Policy and attended a meeting in which it was made clear that the Policy also applied to use of the pagers. *If that were all, this case would be analogous to the cases relied upon by the Appellees. See, e.g., Muick v. Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002) ("[Employer] had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that [employee] might have had and so scotches his claim."); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1234–35 (D. Nev. 1996) (finding a diminished expectation of privacy under the Fourth Amendment where police department had issued a memorandum informing employees that messages sent on city-issued pagers would be "logged on the [department's] network" and that certain types of messages were "banned from the system," and because any employee "with access to, and a working knowledge of, the Department's computer system" could see the messages); see also *O'Connor*, 480 U.S. at 719 (noting that expectation of privacy would not be reasonable if the employer "had established any reasonable regulation or policy discouraging employees . . . from storing personal papers and effects in their desks or file cabinets"); *Schowengerdt v. General Dynamics Corp.*, 823 F.2d 1328, 1335 (9th Cir. 1987) ("We conclude that [the employee] would enjoy a reasonable expectation of privacy in areas given over to his exclusive use, unless he was on notice from his employer that searches of the type to which he was subjected might occur from time to time for work-related purposes.").

Quon at 7022 (emphasis added).

Because of the department's subsequent "informal" text message policy communicated by the lieutenant in charge of administering the pagers, the Ninth Circuit panel held that Quon had a reasonable expectation of privacy with respect to the content of his text messages. Consequently, the court found that the city and police department violated Quon's Fourth Amendment rights because Quon had a reasonable expectation of privacy and the department's search was not reasonable in scope. According to the court, the search was too intrusive and could have been made less intrusive by either warning the employee that he could not send personal messages for the next month or allowing the employee to review the content of the messages to determine whether

they were work-related. The department had argued that the search was legitimate and necessary to determine if the employees needed a larger character allotment for work-related messages.

Quon Applies to Public Employers

Initially, the *Quon* opinion notes the applicability of the Fourth Amendment to public employers. When the conclusions are reached toward the end of the opinion, however, there is no mention of public or private employers, so some commentators are asserting that *Quon* is unclear as to whether it is limited to public employers or applies more broadly to all employers.²

Generally, employees of public employers typically have diminished Fourth Amendment privacy protections as compared to their private sector counterparts. As established by the U.S. Supreme Court decision in *O'Connor v. Ortega*, 480 U.S. 709, 725–26 (1987), “reasonable” warrantless searches may be conducted in public-sector workplaces even if such searches violate an employee’s reasonable expectations of privacy. Such “reasonable” searches would include non-investigatory, work-related searches (e.g., entering an employee’s locked desk or file in the employee’s office while the employee is away) and reasonable investigations into a public sector employee’s alleged work-related misconduct. *Id.* In contrast to private employees, the consequences of public employee incompetence or misconduct to both the employer and the public interest can be severe. *Id.* at 724. Furthermore, a public-sector employee’s expectation of privacy would be unreasonable if the employer’s “actual office practices and procedures, or ... legitimate regulation” permit the employee’s supervisor, co-workers or public to enter such employee’s workspace. *Id.* at 717. As in the private sector context, courts have uniformly deferred to a public sector employer’s official policies that expressly address employee privacy and permit the employer to access the employee’s workspace (including computers) when holding that employees cannot retain a reasonable expectation of privacy in the workplace. See *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000); *United States v. Bunkers*, 521 F.2d 1217, 1219–1221 (9th Cir. 1975).

Employees of private sector employers, however, generally have a reasonable expectation of privacy in their workplaces. A warrantless search of a private sector employee’s workplace may only be conducted if the government officers obtain the consent of the employer or another employee with common authority over the searched area. Unless their workspace is “open to the world at large”, private sector employees retain an expectation of privacy. *United States v. Lyons*, 706 F.2d 321, 326 (D.C. Cir. 1983). Presumably, as *Quon* dealt solely with a public employer, its holding should be limited to public employees, although the court failed to address this distinction in a meaningful manner.

Arch Wireless Violated the Stored Communications Act

Lastly, although the Factual Background section of the opinion mentions that Arch Wireless (the third party wireless provider) owned the servers, network and stations through which the employee text messages were transmitted and on which such messages stored, there is no mention of that fact in the portion of the opinion dealing with the Fourth Amendment (other than that the employee had a reasonable expectation of privacy in messages archived on Arch Wireless’ servers because of the “informal” policy used by the department). Therefore, whether such messages reside on an employer’s servers was not mentioned as relevant in the court’s opinion when deciding whether *Quon*’s Fourth Amendment rights were violated by his employer. Note that because the *Quon* holds that Arch Wireless violated the Stored Communications Act when providing the messages to the police department, wireless providers may not be cooperative in responding to requests similar to the one at issue in this opinion unless an employer can demonstrate that an employee has consented to such review through an effective and consistently applied employee policy, and perhaps one explicitly applicable to text messages.

Employer Monitoring Best Practices

The Ninth Circuit’s decision in *Quon* should not change the current direction of U.S. employer policy and the surveillance approach used by U.S. employers related to messaging. The “informal policy” cited in the *Quon* facts essentially informed the employee that if he paid the police department for his messaging overages, no monitoring by the employer would take place. *Quon* is not clear enough on the distinction between Fourth Amendment protections applicable to employees of public agencies rather than of private employers to make a difference in that regard.

However, *Quon* may provide a good occasion for clarifying and updating certain employer policies and practices:

A. Note that the *Quon* court stated that the police department “had no official policy directed to text messaging by use of the pagers.” *Id.* at 896. Thus, *Quon* can provide a good reason to review and update employer policies governing an employee’s use of electronic resources (e-mail, IM, text messages, blogs, wikis, etc.) to make sure such policies are as comprehensive and specific as possible. For example, do your company’s policies clearly provide that SMS/IM platforms other than those provided by your company cannot be used for any company-related communications, and is there auditing and enforcement around those provisions? If not, is your company confident that it can restrict its monitoring to company-provided platforms?

B. By the same token, employers should review their employee monitoring policies to determine whether they include all communications:

- (1) involving company business in any messaging medium,
- (2) involving use of any company-provided messaging platform, and
- (3) involving any company-provided hardware.

C. *Quon* should prod many employers to make sure that their managers are applying policy consistently and not contradicting policy in their dealings with employees.

D. Along with all of the other new contractual assurances relating to information management, employers should get contractual assurances of future cooperation with employee monitoring by third party service providers of employee communication platforms and devices, since such third party service providers may be more uncooperative following the *Quon* decision for fear of Stored Communications Act liability.

Amanda Witt and Jon Neiditz are leaders of the Information Management Practice at Nelson Mullins Riley & Scarborough, LLP, which routinely advises companies on global employee, customer and vendor privacy, security and surveillance issues, as well as all other challenges in the management of information by organizations.

¹ See, e.g., Maura Dolan, *Your Boss Shouldn't Read Your Text or E-Mail Messages Without an OK, Court Says*, L.A. TIMES, June 19, 2008, at <http://www.latimes.com/business/la-me-text19-2008jun19,0,933444.story>; Richard Koman, *9th Circuit: Employees' Text Messages are Private*, CNET, June 20, 2008, at: <http://government.zdnet.com/index.php?p=3871>.

² See, Prof. Orin Kerr, *Ninth Circuit Finds Fourth Amendment Protection in Text Messages*, Volokh Blog, June 18, 2008, at: http://volokh.com/posts/chain_1213821576.shtml; Jennifer Granick, *New Ninth Circuit Case Protects Text Message Privacy From Police and Employers*, ELECTRONIC FRONTIER FOUNDATION, June 18, 2008 at <http://www.eff.org/deeplinks/2008/06/new-ninth-circuit-case-protects-text-message-priv>.