New York Law Journal
TECHNOLOGY TODAY
TUESDAY, AUGUST 26, 2008

An incisivemedia publication

Reasonable Expectations of Privacy Expand

• ELECTRONIC DISCOVERY •

A recent decision from the Ninth Circuit teaches that employees may have greater expectations of privacy in their personal e-mail, text messages, file downloads and other electronic communications if employers fail to enforce their electronic communication policies. Consequently, existing policies may not adequately shield some employers from liability.

BY H. CHRISTOPHER BOEHNING AND DANIEL J. TOAL

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person. ...Numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[1]

Samuel D. Warren and Louis D. Brandeis wrote those words back in 1890, noting with dismay the unauthorized circulation of "instantaneous photographs" and urging privacy protection. The sentiment still resonates more than a century later, although the unauthorized access that exercises hearts and minds today is access to personal electronic communications.

Over the last decade, as technology has become increasingly sophisticated and widespread, courts have continually re-examined the extent to which employees have a reasonable expectation of privacy when using office equipment to surf the Internet for personal reasons, to send and receive personal e-mail and to transmit personal text messages. The U.S. Court of Appeals for the Ninth Circuit's recent decision in *Quon v. Arch Wireless Operating Co. Inc.*, 552 F.3d 892 (2008), demonstrates the fragility of judicial consensus on this subject and the need to stay abreast of new developments.

In *Quon*, the Ninth Circuit considered whether a public employee may prevent his employer from reading text messages sent from an office pager but stored on an independent service provider's computer network. The City of Ontario, Calif., had entered into a contract for text-messaging services, and had provided pagers to officers of the Ontario Police Department to assist in their work. The text messages themselves were stored on the servers of Arch Wireless, an independent service provider. Sergeant Jeff Quon regularly exceeded the monthly character limit for text messaging, which caused the department to incur overage charges. Quon's superior advised him that he could pay the overage charges or, if he was unwilling to do so, the department would have to audit the text messages to ensure all were work-related. Quon opted to pay the overcharges. Eventually, however, the department decided it needed to review the messages, purportedly to ensure the overcharges Quon paid were not work-related. The department therefore obtained the transcripts of his text messages from Arch Wireless. Upon review, the department found many of the messages to be non-work-related, even sexually explicit, and opened an internal investigation.

Quon responded by suing Arch Wireless, the city, and the police department. First, he alleged that Arch Wireless had violated the Stored Communications Act, 18 U.S.C. §§2701-2712, by sending the city transcripts of his text messages without his consent. The Ninth Circuit agreed, holding that Arch Wireless was an "electronic communication service" within meaning of the act because it "provide[d] users…the ability to send or receive wire or electronic communications." As a result, Arch Wireless was prohibited from disclosing the contents of text messages—even to the subscriber of its services—without the consent of the sender or intended recipient of the message.[2] As neither Quon nor his co-respondents had consented here, the Ninth Circuit ruled that Arch Wireless had violated the Stored Communications Act.

Additionally, Quon asserted claims against the department and city for violations of the Fourth Amendment to the U.S. Constitution. In analyzing this claim, the court recognized the need to assess how Fourth Amendment jurisprudence—originally developed to address physical spaces and tangible objects—applies to "the contents of electronic communication in the Internet age," which the court called "an open question."

The court began the Fourth Amendment analysis with "the threshold question": whether Quon had "a reasonable expectation of privacy" in the contents of his text messages. The circuit clarified that the reasonableness of such expectation "turn[ed] on" his employer's electronic communications policy. The court made several findings toward that end.

First, it found the police department had instituted a formal "Computer Usage, Internet and E-mail Policy," and that the policy had been expanded to include pagers, as communicated in a meeting attended by Quon. Second, the policy made clear not only that use "for personal benefit is a significant violation of City of Ontario Policy," but also that "[u]sers should have no expectation of privacy or confidentiality when using these resources" and that "[t]he City of Ontario reserves the right to monitor and log all network activity." Finally, the circuit noted that Quon had signed the policy.

But the court did not stop there. It found that the department's informal policy was, in fact, the reverse: the department did not monitor text messages for personal use. Citing *O'Conner v.*

H. Christopher Boehning *and* **Daniel J. Toal** *are litigation partners at Paul, Weiss, Rifkind, Wharton & Garrison LLP.* **Layaliza K. Soloveichik,** *an associate at the firm, assisted in the preparation of this article.*

Ortega, 480 U.S. 709, 718-19 (1987), the circuit reasoned that "the operational realities of the workplace may make some employees' expectations of privacy unreasonable."

In *Quon*, the "operational reality" upon which the court focused was that, although a policy existed, it was not enforced and employees were aware of this failure to implement the policy. The circuit pointed to the department's complete failure to audit pager use during the entire period pagers were utilized.

The court also observed that the formal policy had been replaced by an "informal policy," whereby the department agreed not to audit text messages as long as officers paid for their overages. The court noted that it sufficed that this "informal policy" had been set by an officer who was in charge of the pagers, rejecting as irrelevant that this officer was neither a "final" nor "official" policy-maker.

The Ninth Circuit concluded that these "operational realities" meant that, the department's formal policy notwithstanding, Quon had a "reasonable expectation of privacy in [his] text messages."

Having established that Quon had a reasonable expectation of privacy, the circuit continued to the second prong of the test for determining whether a search in a government workplace violates the Fourth Amendment. Specifically, the court examined whether the search either lacked "justifi[cation] at its inception" or, though justified, was not "reasonably related in scope to the circumstances which justified the interference in the first place."

The court reasoned that the department's search was "justified at its inception" because there was a work-related purpose in reviewing the messages—assessing the character-limit policies to ensure the employees were not paying for work-related messages. But the court also found that the police department could have achieved this end less intrusively, without reviewing the content of the messages. Therefore, the court concluded that the police department's review of Quon's text messages had violated his Fourth Amendment rights.

Efficacy of Policies

The holding in *Quon* has potentially disturbing implications for the efficacy of workplace policies in shielding public employers from Fourth Amendment violations.

In reaching the holding, the Ninth Circuit announced that "protection for the contents of electronic communications in the Internet Age is an open question" and that "electronic communication via e-mails, text message, and other means opens a new frontier in Fourth Amendment jurisprudence."

However, insofar as *Quon* addressed the effect an electronic communication policy has in connection with a "reasonable expectation of privacy," the case did not venture into entirely uncharted territory. Earlier decisions from the Fourth, Seventh, Eighth and Ninth circuits, for example, had already examined the significance of such policies, and had concluded that the institution of formal policies tended strongly to undercut employees' reasonable expectation of privacy in the contents of their electronic messages and files stored on, transmitted by, or accessed through office equipment.[3]

Nevertheless, *Quon* does reflect an important change. In *Quon*, the Ninth Circuit concluded that the existence of an electronic communications policy, standing alone, might be insufficient to strip an employee's expectation of privacy. In the view of the Ninth Circuit, the manner in which such a policy has been enforced may bear upon whether employees have a reasonable expectation of privacy in electronic communications despite a formal policy of their employer insisting that they do not. It is in this manner that *Quon* parts company with the earlier cases.

One ramification of *Quon*, therefore, is that public employers desiring to be shielded from Fourth Amendment claims may not be able to rely solely on the existence of an electronic communications policy. Formerly, practitioners advised their clients seeking to avoid claims premised on "a reasonable expectation of privacy" to be sure to craft workplace policies mentioning the employer's intent to monitor electronic communications made through third-party service providers.[4]

In light of *Quon*, however, public employers would be well served by actively enforcing such electronic communication policies.[5] Permitting the search of downloaded files, e-mail, and text messages accessed through workplace equipment may turn not only on whether policies exist, but also on whether such policies have actually been policed.

Moreover, because policies containing absolute bans on personal use may be difficult to enforce, another implication of *Quon* may be that employers should tailor their bans to an extent that can be practically implemented. At least some courts in the Second Circuit have found that employees had a reasonable expectation of privacy in the personal use of office equipment where their employers' absolute ban on the personal use of office equipment had been sporadically applied.[6]

Private Sector

Finally, the significance of *Quon* is not limited to the government context. It may also be instructive in cases where private sector employees store or access e-mails or text messages using workplace equipment.

Numerous courts have concluded that the privacy right given expression in the Fourth Amendment exists also as a common law doctrine. Courts that have examined that doctrine have concluded that a "reasonable expectation of privacy" is one of the factors for demonstrating that the common law tort applies.[7] If *Quon* becomes the standard going forward, then enforcing compliance may be relevant in cases brought under the common law against private employers.

Additionally, *Quon* may apply in instances where private sector employees assert a privilege, such as the attorney-client or marital communication privileges, as a basis for withholding the production of e-mail. Courts assessing whether such privileges are waived as to e-mail transmitted on office equipment have borrowed the "reasonable expectation of privacy" analysis from Fourth Amendment cases, and have examined the private employer's electronic communication policies for the purpose of that analysis.[8]

If *Quon* gains currency in Fourth Amendment jurisprudence, the enforcement of electronic communication policies may become an issue in the privilege cases as well. Absent policing, employees may be able to assert a privilege, despite their employer's institution of a comprehensive electronic communications policy.

Conclusion

Quon teaches that employees may have greater expectations of privacy in their personal e-mail, text messages, file downloads and other electronic communications if employers fail to enforce their electronic communication policies. Consequently, existing policies may not adequately shield public employers from liability.

In addition, if *Quon* carries over to the privilege waiver cases, then employers in both the public and private sectors will either need to accept that their employees may be deemed to have a legitimate expectation of privacy in such electronic communications sent over their systems or, if they are determined to avoid that result, may need to enforce their policies. As *Quon* makes clear, having a policy may no longer be enough.

1. Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," 4 Harv. L Rev. 193, 195 (1890).

2. By contrast, the Stored Communications Act imposes less stringent restrictions on "remote computing services," which provide "computer storage or processing services by means of an electronic communications system," 18 U.S.C. §2711(2). Remote computing services may release private information with the lawful consent of either an addressee of a communication or the subscriber.

3. See, e.g., *Biby v. Board of Regents of the Univ. of Nebraska*, 419 F.3d 845, 846, 849-50 (8th Cir. 2005); *Muick v. Glenayre Electronics*, 280 F.3d 741, 742-43 (7th Cir. 2002) (Posner, J); *United States v. Simons*, 206 F.3d 392, 398-99 (4th Cir. 2000); *Thygeson v. U.S. Bancorp.*, No. CV-03-467-ST, 2004 WL 2066746, at *19-20 (D. Or. Sept. 15, 2004).

4. See, e.g., Victor Schachter, "Privacy in the Workplace," 828 Practicing Law Institute 153, 210-11, 214 (May-June 2005) (model policy).

5. Note that, in order for an employer to conduct such enforcement, it may be necessary for the employer first to secure its employees' consent to review their electronic communications. This is because, consistent with the *Quon*'s discussion of the restrictions the Stored Communications Act imposes on third-party service providers, employers have no automatic right under the act to access their employees' electronic communications on such a network. See also *Hone v. Presidente U.S.A. Inc.*, No. C08-80071, 2008 U.S. LEXIS 55722, at *4 n.3 (N.D. Cal. July 21, 2008). One method of satisfying the act's consent requirement may be to require that employees consent to the release of such communications as a condition of employment.

6. See, e.g., *Leventhal*, 266 F.3d at 74, 75; *Curto v. Medical World Communications Inc.*, No. 03CV6327 (DRH), 2006 WL 1318387, at *8 (E.D.N.Y. May 15, 2006).

7. See, e.g., *Muick*, 280 F.3d at 743-44; *Kelleher v. City of Reading*, No. CIV.A. 01-3386, 2002 WL 1067442, at *7, *8 (E.D. Pa. May 29, 2002); *White v. White*, 344 N.J. Super. 211, 223 (Ch. Div. 2001); see also Restatement (Second) of Torts §652 (1977).

8. *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 257-58 (Bankr. S.D.N.Y. 2005); see also *Sprenger v. Rector and Bd of Visitors of Va. Tech*, No. 7:07cv502, 2008 WL 2465236, at *3, *4 (W.D. Va. June 17, 2008); *Curto*, 2006 WL 1318387, at *7.