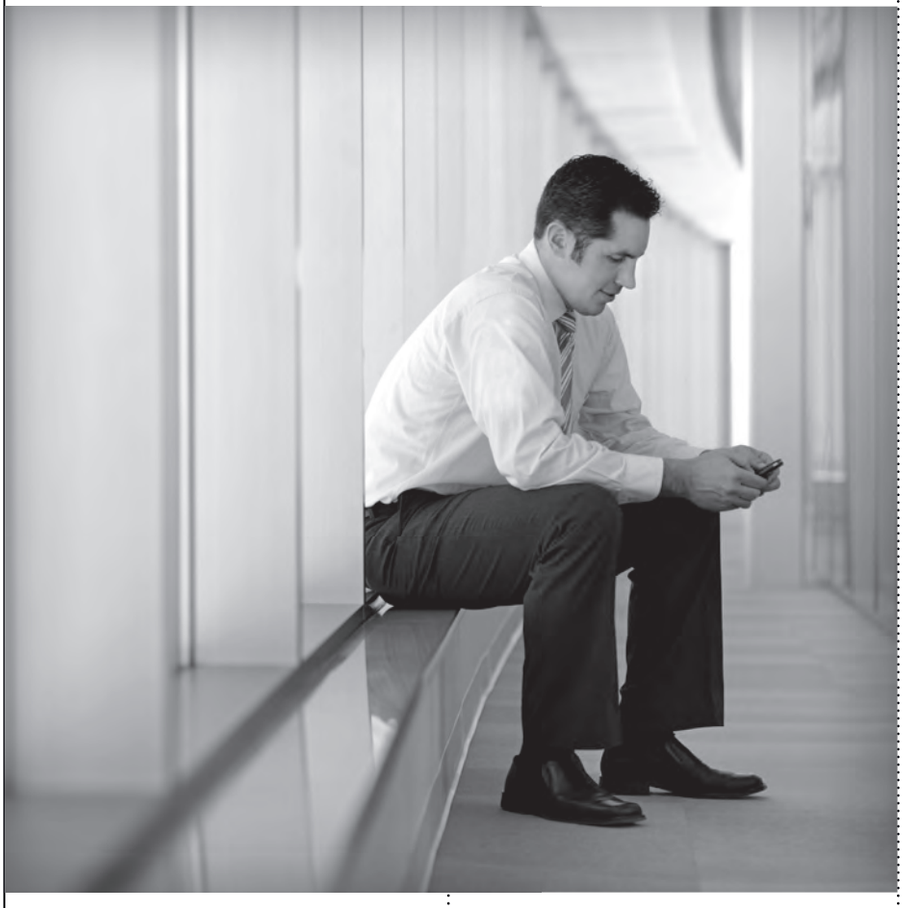
Opening Pandora's Box: Employee Communications in the Digital Age

by Sophia M. Stadnyk



The U.S. Supreme Court reached a milestone of sorts with this year's ruling on workplace privacy and employee monitoring. The decision, *City of Ontario v. Quon*,[1] is the first time the Court addressed whether a reasonable expectation of privacy exists in the personal text-messages employees send on city-owned or issued pagers. On the plus side, a unanimous Supreme Court upheld the City's search of the employee's personal messages, finding the warrantless search was reasonable and did not violate the employee's Fourth Amendment rights. On the minus side, the ruling is structured along the lines of less is more: pointing to rapid changes in the state of technology, the Court shied away from providing a clear answer on the issue of employee communications and privacy, leaving employers with not much of a framework to go on for dealing with this difficult issue.

Background

Ontario, California had adopted a formal policy on employee use of designated electronic communication devices. City computers "and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computers [were] limited" to City business, and the use of "inappropriate, derogatory, obscene, suggestive, defamatory, or harassing" language was prohibited.[2] The written policy expressly provided that:

> Access to all sites on the Internet is recorded and will be periodically reviewed by the City. The City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.
>
> Access to the Internet and the e-mail system is not confidential; and information produced either in hard copy or in electronic form is considered City property. As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.[3]

Jeff Quon, a SWAT team police officer, signed an "Employee Acknowledgment" that borrowed language from this policy, indicating that he had "read and fully under[stood]" the policy.[4] Subsequently, Quon and other employees were issued with two-way pagers pursuant to a contract between Arch Wireless and the City for wireless text-messaging services. Unlike computers, the pagers operated through the use of radio frequency transmissions sent to and from receiving stations operated by Arch Wireless, with the messages being stored on the company's server. The City had no separate policy specifically addressing text-messaging and the pagers, although in 2002, Quon attended a meeting at which Lieutenant Duke (a non-policy-making employee responsible for the department's electronic equipment) advised that pager messages were considered to be e-mails, and would fall under the City's policy as public information and would be eligible for auditing.[5] This statement was also circulated to Quon and others as a written memo from Police Chief Scharf.[6]

Each pager had an allotted 25,000 character limit, and the City had to pay extra for anything over this threshold (the "overage"). In actual practice, as decided on and administered by Duke, if an employee promptly reimbursed the overage charge, Duke would not inquire further into the excess or have the messages audited to see if the use was non-work-related.[7] Significantly, though, it was not possible for any supervisory employee to view the content of the messages without contacting Arch Wireless. Quon

went over the monthly character limit three or four times and paid the City for the overages.

Chief Scharf ordered an audit of the messages of Quon and another officer. Scarf indicated that one reason for the audit was to see if there was a need to increase the amount of monthly characters allotted to the officers.[8] The City, as the subscriber, requested that Arch Wireless provide the message transcripts. These revealed that most of Quon's messages were personal (and often sexually explicit) and Scharf determined that Quon's pager was being misused. Of the 456 texts Quon sent *while on duty* in one month, only 57 were for work-related purposes; on an average workday, Quon sent or received 28 messages, of which only three were related to police business.[9]

Quon and several message recipients (including Quon's then wife, his mistress, and his co-worker on the SWAT team) sued the City, claiming that the City and the service provider had violated their Fourth Amendment rights and their rights under the Stored Communications Act (SCA).[10] This prohibits any "person or entity providing" either "an electronic communication service" or a "remote computing service" to "the public" from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service," or "divulg[ing] a record or other information pertaining to a subscriber or customer of such service."[11]

The Rulings Below

The district court ruled that neither the City nor the provider was liable under the SCA, and that, while Quon had a reasonable expectation of privacy in the text messages, genuine issues of fact as to Scharf's actual purpose in having the audit done precluded summary judgment as to the reasonableness of the search for Fourth Amendment purposes.[12] Key to the district court's conclusion was the department's handling of the overages: the express but unwritten "policy," known to Chief Scharf, of turning a "blind eye" to the actual use of the pagers so long as the overages were paid. This countermanded and vitiated the official policy, and "effectively provided employees a reasonable basis to expect privacy in the contents of the text messages."[13]

On appeal, the U.S. Court of Appeals for the Ninth Circuit affirmed the finding of a reasonable expectation of privacy and found that the search was unreasonable.[14] For Fourth Amendment purposes, there was no meaningful distinction between text/pager messages, e-mails, or letters. This court, too, concluded that, although the City had established various written policies, the "operational reality" for employees was that the policies would not be enforced. It was immaterial that Duke was "not the official policymaker, or even the final policymaker," because he "was in charge of the pagers, and it was reasonable" for Quon to rely on the policy—formal or informal—that Duke established and enforced.[15] Accordingly, Quon had a reasonable expectation of privacy in his messages.

The Ninth Circuit held that the search of the messages was unreasonable because, even though the employer's purpose was legitimate and work-related (to ensure that officers were not being required to pay for work-related expenses), its scope far exceeded that objective, and the purpose would have been met through less intrusive means. Instead of a non-consensual review of all of the messages, the department could, for example, "have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to the Department to review the redacted transcript."[16] Scharf, however, was entitled to qualified immunity because, at the time of the search, there was no clearly established law regarding whether users of text-messages that were archived, however temporarily, by an outside service provider, had a reasonable expectation of privacy in the messages.[17] Lastly, the Ninth Circuit reversed the finding on the SCA, ruling that Arch Wireless had violated the SCA by releasing the content of the messages without the sender's or recipient's consent.

The Supreme Court

The petition for certiorari filed by Arch Wireless, challenging the Ninth Circuit's ruling that it violated the SCA, was denied.[18] The only issue before the Supreme Court was the Fourth Amendment claim.

The Court, in a unanimous decision authored by Justice Kennedy, reversed and remanded. It began its analysis with the two-step inquiry established by the plurality in *O'Connor v. Ortega*[19]— namely, that a court must consider "[t]he operational realities of the workplace" in order to determine whether an employee's Fourth Amendment rights are implicated. If this case-by-case inquiry determines that the employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness."[20] (Justice Scalia outlined a different approach, dispensing with the "operational realities" inquiry, but agreed that government searches for work-related materials or to investigate workplace rule violations were generally not violative of the Fourth Amendment.[21])

Here, the employer had "at the outset" made it "clear that pager messages were not considered private,"[22] and it would not have been reasonable for Quon to conclude that his messages were, in all circumstances, protected from employer review. Further, being a law enforcement officer who served on a SWAT team, he should have been aware that his actions were likely to come under public or legal scrutiny[23]—by an investigating board, during litigation, or by the media. The Court declined to go further and address whether Duke's conduct negated or amended the employer's official policy, and instead assumed, for the sake of argument, that Quon had a reasonable expectation of privacy in the text messages.[24] Using the approach of the *O'Connor* plurality — a search conducted for a non-investigatory, work-related purpose or to investigate work-related misconduct was "reasonable if it was 'justified at its inception'" and if

continued on page 16

Sophia M. Stadnyk is the Senior Associate Counsel with IMLA. She is the editor of the *Municipal Lawyer*, and writes about the U.S. Supreme Court for the American Bar Association's *State & Local Law News*, and for IMLA. She has an LL.B. (University of Alberta) and LL.M. (Cambridge University), and is admitted to practice law in Alberta, Canada and in New York State.

The *Quon* Case *continued from page 15*

"'the measures adopted [were] reasonably related to the objectives of the search and not excessively intrusive in light of'" the circumstances giving rise to the search, the Court concluded that the search here satisfied the standard.[25] The search had been ordered because the police chief wanted to determine if the existing character limit was adequate to meet the department's needs, and reviewing the transcripts was reasonable and not excessively intrusive because it was an "efficient and expedient way to determine whether Quon's overages" were work-related or due to personal use.[26] The fact that the search unearthed intimate details about Quon, or the likelihood that Arch Wireless violated the SCA by turning over the transcripts, did not serve to make the search unreasonable.[27]

In summary, the search was reasonable under both *O'Connor* approaches, the plurality's and Justice Scalia's, and no Fourth Amendment violation had occurred.[28]

The difficulty with the ruling is the reluctance with which the Court looked at the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. Peeping through its fingers, as it were, the majority referred to the ongoing "changes in the dynamics of communication and information transmission"[29] and emphasized the need to proceed with care:

> The judiciary risks 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 in 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 communication devices.[30]

Thus, it was "preferable to dispose of this case on narrower grounds."[31]

Although the Court declined to establish any broad guidelines regarding the existence and extent of employee privacy expectations in employer-provided electronic communication devices, the decision did provide a few helpful guideposts for employers. First, the "principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere;"[32] second, the Court expressly rejected the Ninth Circuit's "least intrusive search" requirement in determining if a search was reasonable. Third, an employer's use policies should make clear that no informal practices are to be construed as acceptable deviations from the formal policy. Last, but less clear, the ruling seems to indicate that an employer's use policy need not specifically mention every form of possible electronic communication device.

Now What?

It's clear that a boxful of other complicated issues remains, issues that the courts are just beginning to address.

Blogs. Last year, in *Richerson v. Beckon,*[33] the Ninth Circuit ruled that a government employer did not violate the First Amendment when it transferred an employee based, in part, on comments that the employee had posted on her personal Internet blog. Richerson was employed as a "curriculum specialist" and "instructional coach," but was transferred to a classroom teaching position after the details of her publicly-available blog—one that included "several highly personal and vituperative comments about her employers, union representatives, and fellow teachers"[34]—came to the attention of the school district, her employer. Richerson's position required that she cultivate "trusting mentor relationships" with teachers where she could give honest and private feedback. The employer correctly determined that Richerson's speech had a significantly deleterious effect on her ability to do her job, particularly since several employees had refused to work with her, and others had complained about the blog. Since it was clear that the legitimate administrative interests of the employer outweighed Richerson's First Amendment rights, the employee's Section 1983 lawsuit claiming retaliation was dismissed.

Workplace Computer, Personal Account. Stengart's employer issued her with a laptop computer and a work e-mail address. She used that computer to communicate with her lawyers about her anticipated lawsuit against her employer, using her personal, web-based, password-protected Yahoo e-mail account. She never saved her Yahoo ID or password on the laptop, but browser software automatically made a copy of each web page she viewed and saved it on the computer's hard drive. After Stengart filed a discrimination suit against her employer, the company hired an expert to create a forensic image of her laptop's hard drive and accessed the e-mails. Her attorney objected on the basis of attorney-client privilege; the employer asserted that Stengart had no reasonable expectation of privacy in files on a company-owned computer in light of the company's policy on electronic communications. This stated that the company expressly asserted and would "exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice," that e-mails were "not to be considered private or personal," and that "[o]ccasional personal use" of the computers was permitted.

The trial judge denied the motion, noting that the company's policy put the employee on sufficient notice that her e-mails would be viewed as company property and that, as a result, Stengart waived any privilege. Stengart appealed, arguing that the policy failed to provide adequate warning that the employer would save on a hard drive, or monitor the contents of, e-mails sent from a personal account. Earlier this year, the Supreme Court of New Jersey held that Stengart had a reasonable expectation of privacy in the personal e-mails (she took steps to protect her password) and that sending and receiving them using a company laptop did not eliminate the attorney-client privilege that protected them. The policy, the court noted, did "not address the use of personal, web-based e-mail accounts accessed through company equipment. It [did] not address personal accounts at all. Nor [did] it warn employees that the contents of e-mails sent via personal accounts [could] be forensically retrieved and read by the company."[35]

"Authorized Access"? In *LVRC Holdings LLC v. Brekka*,[36] an employer sued a former employee, Brekka, alleging that he violated the Computer Fraud and Abuse Act (CFAA)[37] by accessing a company computer "without authorization" while he was employed. Brekka was assigned a computer at work, but e-mailed documents he obtained or created in connection with his work to his personal e-mail account or his wife's computer. This, the company claimed, violated the Act's prohibition on accessing a protected computer without authorization, or exceeding authorized access. The company had no guidelines that would prohibit employees from e-mailing documents to their homes, but it claimed that, since Brekka had accessed a company computer and obtained confidential information to further his own interests, rather than the interests of his employer, such access was "without authorization." The court disagreed. There was no liability under the Act, as Brekka had permission to access the computer and the documents he had e-mailed, and was still employed by the company when he sent the documents to himself and to his wife.

Social Networking: Another Minefield. In 2009, police officers of the Town of Harrison, N.Y. were suspended after the inappropriate comments they posted to a Facebook page (including comments about the town's mayor) came to light. According to a news story, the officers believed the page to be password-protected.[38] In a recent ruling involving a plaintiff who claimed an accident left her largely confined to her bed and home, a New York court granted the defendant's motion for production of materials from the plaintiff's social networking website accounts, on the basis that the plaintiff did not have a reasonable expectation of privacy in that information:

> Indeed, as neither Facebook nor MySpace guarantee complete privacy, Plaintiff has no legitimate reasonable expectation of privacy. In this regard, MySpace warns users not to forget that their profiles and MySpace forums are public spaces ... Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy.[39]

The law in this area continues to evolve. While *Quon* may be the Court's first pronouncement on employee communications and new technology, it surely will not be the last.

As these examples show, the law in this area continues to evolve. While *Quon* may be the Court's first pronouncement on employee communications and new technology, it surely will not be the last.

Notes

1. 130 S.Ct. 2619.
2. 529 F.3d 892, 896 (9th Cir. 2008).
3. *Id.*
4. 130 S.Ct at 2625.
5. 529 F.3d at 896.
6. 130 S.Ct at 2625.
7. 529 F.3d at 896.
8. As indicated in the district court ruling, this apparently coincided with an investigation into whether police dispatchers were improperly providing information to the Hell's Angels on police investigations. At the time, Quon was having an affair with one of these dispatchers. 445 F.Supp.2d 1116, 1122 (C.D. Cal. 2006).
9. 130 S.Ct. at 2626.
10. 18 U.S.C. §§ 2701-2711 (1986) ("SCA").
11. 18 U.S.C. § 2702(a). The Act provides for a private right of action to any "person aggrieved by any violation of this chapter." *Id.*
12. Quon v. Arch Wireless Operating Co., Inc., 445 F. Supp.2d 1116, 1138, 1146 (C.D. Cal. 2006).
13. *Id.* at 1141.
14. 529 F.3d 892 (9th Cir. 2008). (A divided Ninth Circuit declined to reconsider the case *en banc*. Quon v. Arch Wireless Operating Co., Inc., 554 F.3d 769 (9th Cir. 2009)).
15. *Id.* at 907.
16. *Id.* at 909.
17. *Id.* at 910.
18. USA Mobility Wireless, Inc. v. Quon, 30 S.Ct. 1011(2009).
19. 480 U. S. 709, 711 (1987).
20. 130 S.Ct. 2619, 2628.
21. *Id.* at 2634.
22. *Id.* at 2629.
23. *Id.* at 2631.
24. *Id.* at 2630.
25. *Id.*
26. *Id.* at 2631.
27. *Id.* at 2632.
28. *Id.* at 2629-33.
29. *Id.* at 2629.
30. *Id.* Justice Scalia, however, had no such qualms: "Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice." *Id.* at 2635.
31. *Id.* at 2630.
32. *Id.*
33. 337 Fed. Appx. 637 (9th Cir. 2009).
34. *Id.* at 638.
35. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 663 (N.J. 2010).
36. 581 F.3d 1127 (9th Cir. 2009).
37. 18 U.S.C. § 1030 (West 2010).
38. Dionne Searcey, *Employers Watching Workers Online Spurs Privacy Debate*, Wall Street Journal Online, April 23, 2009 at http://online.wsj.com/article/SB124045009224646091.html. And on November 03, a blog post indicated that the National Labor Relations Board had filed a complaint against an employer that allegedly fired a worker over the negative comments she posted about her supervisor on her personal Facebook page. *See* Jenna Greene, *NLRB Sues Company for Firing Worker Over Facebook Post*, The BLT: The Blog of Legal Times, Nov. 03, 2010 at http://www.typepad.com/services/trackback/6a00d83451d94869e20133f58ec3f0970b.
39. Romano v. Steelcase Inc., 907 N.Y.S. 2d 650, 656-57 (N.Y. Sup. 2010). ML