

The Employer as Big Brother

Are Text Messages and Emails Private?

by Maureen S. Binetti

In this electronic age, employers often provide their employees with computers, cell phones and other electronic devices to aid the employee and employer in efficiently performing their work. Does the employee have a reasonable expectation of privacy regarding the content of emails and text messages routed through service providers, for example that an employer may not attempt to obtain them from the provider, absent consent of the employee?

The Ninth Circuit recently answered that question in favor of a public employee in *Quon v. Arch Wireless Operating Co., et al.*¹ In *Quon*, the court found the provider of wireless text messaging services, defendant Arch Wireless, violated the Stored Communications Act (SCA),² and that the city of Ontario, California, the public employer of one of the plaintiffs, violated the plaintiffs' Fourth Amendments rights to be free from unreasonable search and seizure pursuant to 42 U.S.C. Section 1983³ and the California Constitution.

In *Quon*, a SWAT team member for the Ontario Police Department (OPD) sued his employer and his wireless pager carrier, Arch Wireless, after the carrier released private records of his text messages from his pager to his employer. The recipients of his text messages (his wife, a fellow SWAT sergeant, and another person) were also plaintiffs. The SWAT team members had been issued pagers because they were required to be on call 24 hours a day, seven days a week, and were not paid for standing by. The pagers were not regulated, and the SWAT members' text messages themselves were not reviewed. Because the city was charged for all characters in excess of 25,000 per month, the total number of characters produced and message content were reviewed to determine whether the overage was work-related. However, as long as the troopers stayed within their 25,000-character limit, there was no review.

Sergeant Quon frequently went over the 25,000 character limit. However, Lieutenant Duke, the officer in charge of the pagers for the OPD, told him that as long as he paid the overage charges, the content would not be examined. Sergeant Quon went over the limit three or four times, by substantial margins, but always paid the overages, without incident. When he once again went over the limit, a frustrated Lieutenant Duke complained of having to collect overage charges. The chief of the department then ordered Lieutenant Duke to ascertain why Sergeant Quon and others were going over the allowance limit, even though overages had not, up until that point, cost the department any money, since Sergeant Quon and the others always paid the overage charges.

There was a dispute over whether the reason for the resultant search was to investigate Sergeant Quon and other employees' usage to determine if they were using the service excessively for personal reasons, or simply to determine if the 25,000 limit should be raised, in order to not charge the officers with overages for work-related text messages.

There was no dispute that the employer was interested in the content of the messages, at least in order to determine if they were work-related or personal communications. The employer asked for and acquired from Arch Wireless, the service provider for the pagers, transcripts of Sergeant Quon's text messages. It found that Sergeant Quon's messages often were

personal communications to his wife, one of his fellow officers, and another person. The communications sometimes were sexually explicit.

Sergeant Quon and the recipients of his messages sued for violations of the SCA and the Fourth Amendment's prohibition against unreasonable search and seizure. The district court found that the Stored Communications Act did not apply, because Arch Wireless's pager and text-messaging services were remote computing services (RCS), not electronic communications services (ECS). This distinction is significant, as the SCA distinguishes between the persons/entities that are permitted to obtain such information from the service providers, depending upon the characterization of the providers.

The Ninth Circuit reversed the district court on this issue, holding that it erred in determining that Arch Wireless was an RCS, not an ECS. In so holding, the court first noted the purpose of the SCA:

The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address. See Orin S. Kerr, *A User's Guide to the Stored Communications Act and a Legislator's Guide to Amending It*, 72 *Geo. Wash. L. Rev.* 1208, 1209-13 (2004). Generally, the SCA prevents "providers" of communication services from divulging private communications to certain entities and/or individuals. *Id.* at 1213.⁴

Section 2702 of the SCA governs liability for both ECS and RCS providers.⁵ The nature of the services provided determines whether a provider such as Arch Wireless is an ECS or an RCS. Arch Wireless provided the employer in *Quon* with a service that allowed communication between two pagers—text messaging over radio frequencies.

Both an ECS and an RCS can release private information to, or with the lawful consent of, "an addressee or intended recipient of such communication,"⁶ but only an RCS can release such information "with the lawful consent of...the subscriber."⁷ In *Quon*, it was undisputed that the employer was a "subscriber," but was not an "addressee or intended recipient" of the released messages.⁸

Thus, the characterization of the service provided by Arch Wireless was critical to its liability. If, as the district court found, it was an RCS, it had no liability; if it was an ECS, liability was established as a matter of law.⁹

The Ninth Circuit held that although Arch Wireless's service involved some "computer storage or processing services" by electronic means (the definition of an RCS), the definition of an ECS clearly described the text-messaging pager services it provides: "any service which provides to users thereof the ability to send or receive wire or electronic communications."¹⁰ Neither its temporary storage, incidental to such communications, nor its storage for backup protection, altered its essential character as an ECS.¹¹

As there was no dispute that Arch Wireless "knowingly" provided text-messaging transcripts to the city/employer, the Ninth Circuit entered judgment in the plaintiffs' favor on this claim as a matter of law.¹²

The court then turned to the claims against the employer under the Fourth Amendment. It applied the two-prong test well-established by the Supreme Court in *O'Connor v. Ortega*.¹³ The first prong is that the employee must have a reasonable expectation of privacy. The district court determined that Sergeant Quon had such an expectation, since the pager effectively was his private property and there was no practical system for regulating his text usage before that property was accessed without his consent.

Regarding the second prong—that the search itself was unreasonable—the lower court concluded that a trial was necessary, as an issue of material fact existed regarding whether the search's purpose was for determining if the over-ages were caused by work-related messages, and thus the limit had to be increased, or whether the search was investigatory in nature. The district court held that if the jury found the search to be the latter (investigatory), it was unreasonable, but if it was for the former (administrative purposes), it would be reasonable, and thus the claim would fail. The jury found that the purpose of the search was to determine the proper character limit for its officers (administrative), and thus the court entered judgment for the defendants.¹⁴

The Ninth Circuit reviewed and confirmed the lower court's finding that Sergeant Quon and his associates had a reasonable expectation of privacy. Significantly, the employer had a very clear computer usage, Internet and email policy that warned employees they "should have no expectation of privacy or confidentiality when using these resources."¹⁵ Moreover, Sergeant Quon attended a meeting in which it was made clear that the policy applied to use of the pagers.¹⁶

The court noted that if that were all, the cases holding that there is no reasonable expectation of privacy in electronic communications where the employer has a policy warning employees of this consequence would be dispositive, and the plaintiffs' claims would fail.¹⁷ However, despite the official policy of the defendant employer in *Quon*, Lieutenant Duke, the point person for the policy in question, had made it clear that he would not audit the employees' pagers as long as the over-ages were paid. Indeed, the department did not audit the pagers for the eight months they had been in use, and Sergeant Quon himself had exceeded the 25,000 character limit three or four

times before, and paid for the overages each time, without anyone reviewing the text messages.¹⁸

The court held that because Sergeant Quon abided by these rules, he had a reasonable expectation of privacy.¹⁹ Since Sergeant Quon's associates had a reasonable expectation that Sergeant Quon's employer would not surreptitiously review their messages, absent proper consent, they too had a reasonable expectation of privacy as a matter of law.²⁰

With respect to the second element of the test, the court disagreed with the lower court's holding that there was an issue of material fact regarding whether the search was reasonable, based upon the intent of the searchers. The Ninth Circuit found the search was unreasonable as a matter of law, and thus granted summary judgment to the plaintiffs on their Fourth Amendment claims.²¹ The court found that assuming, as the jury found, the search was for non-investigatory purposes, it was unnecessary to achieve the stated non-investigatory goals of determining whether the text character limits were being overrun consistently because of work-related or personal messages. The court found that less intrusive means could have been used to garner the information easily, and that the failure to do so was patently unreasonable, and thus inconsistent with the Fourth Amendment.²²

The city requested a rehearing *en banc*, which was denied earlier this year.²³ While orders denying rehearings *en banc* are usually *pro forma*, this one clearly was more controversial, as two opinions were issued in connection with it. A dissent, in which seven judges joined, argued that the panel's decision should be overturned by the entire court because it contradicted *O'Connor v. Ortega*²⁴ and other Supreme Court precedents. Judge Sandra Segal Ikuta's dissent argued that the decision amounted to a "less intrusive means test," whereby an

employer or government official is precluded from any search where a less intrusive means is available, and that this approach has been rejected explicitly by the Supreme Court.²⁵

A concurrence on the denial of a rehearing *en banc* (essentially a reaffirmation of the first opinion) argued against the dissent, stating that such a test was never applied by the panel in the first decision. Instead, the finding was that the search itself was excessively broad and intrusive, given its non-investigatory purpose. Weighing the governmental interest against the individuals' privacy interests, the concurrence argued that the panel properly held that the extremely intrusive nature of the search, where there were many less intrusive ways to easily accomplish the same ends, given the totality of the circumstances, constituted an unreasonable search and seizure. The panel, the concurrence stated, rendered a decision consistent with *O'Connor*.²⁶

The *O'Connor* decision itself, upon which both sides of this case relied, is a core Supreme Court decision on the Fourth Amendment from 1987. Often cited as limiting Fourth Amendment litigants' rights, the decision, based upon a plurality, held that while public employees' expectations of privacy can exist, when a search or seizure is performed in the workplace by a supervisor rather than a law enforcement official, some expectations of privacy may be unreasonable. Moreover, given the variety of work environments in the public sector, this question must be addressed on a case-by-case basis.²⁷

In *O'Connor*, a physician who was an employee of a state hospital brought suit under Section 1983, alleging that a search of his office, including seizure of items from his desk and file cabinets, violated the Fourth Amendment. Although finding that the employee had a reasonable expectation of privacy in his office, desk, and filing cabinet,

the Court held that summary judgment for the employee on liability for the search was improper, as the issue of the reasonableness of the search under the circumstances was a fact issue.²⁸

The interpretation of *O'Connor* in *Quon* focused on the reasonableness issue, but determined as a matter of law that the search was unreasonable.²⁹ The court similarly distinguished the Supreme Court's opinion in *Smith v. Maryland*,³⁰ the "pen register" case, and other similar cases holding that the "search of identifying information (phone numbers dialed in *Smith*, outside of envelopes in *United States v. Hernandez*"³¹ is not violative of the Fourth Amendment. Noting it had held that "e-mail users have no expectation of privacy in the to/from addresses of their messages...because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information,"³² the court stated that these email addresses, like envelopes containing letters, involve the "address and size of the package," which do not deserve Fourth Amendment protection; however, the *contents do* deserve that protection.³³

Like the maker of a telephone call who has a reasonable expectation of privacy in his or her conversation (but not the number called), the *Quon* court concluded text messages on a cell phone, information stored on computers, and Quon's wireless text messages involved *content*, and were protected.³⁴

Thus, the *Quon* court's holdings are seen as a victory for the privacy rights of employees; however, several serious cautions must be given. First, the case involved a public employer, thus Fourth Amendment rights not present in the private employment context were invoked. However, particularly in a state such as New Jersey, which affords generous privacy protections, the arguments accepted in *Quon* may very well be utilized.³⁵

It should be further noted that *Quon* rested upon potentially unique facts. What normally would satisfy an argument that an employee had a reasonable expectation of privacy in using electronic equipment belonging to the employer—a clear, unambiguous warning in a policy distributed to all employees that *no* such privacy expectation may be had—was defeated by a contrary course of conduct that obviated that policy. Thus, a clear policy that is *not* contradicted by practice should protect employers (although not necessarily service providers under the SCA).

Finally, the court's factual determination, *as a matter of law*, that the search was unreasonable as there were less intrusive means available to make the desired determination of work-related or personal use, as criticized in the dissent on the rehearing *en banc* decision,³⁶ is subject to attack. Indeed, a *writ of certiorari* to the Supreme Court was filed on April 27, 2009.

Thus, it may be argued that the law in this area remains unsettled, particularly regarding private employers, on the privacy issue. However, service providers should be wary of providing such information, given the strictures of the SCA, as interpreted by *Quon* to apply to text (and email) messages. ☞

Endnotes

1. 529 F.3d 892 (9th Cir. 2008), *rehearing en banc denied*, 554 F.3d 769 (9th Cir. 2009).
2. 18 U.S.C. §§ 2701-2711.
3. 42 U.S.C. § 1983.
4. 529 F.3d at 900.
5. 18 U.S.C. § 2702(a)(1)-(2).
6. *Id.*, § 2702(b)(1), (b)(3).
7. *Id.*, § 2702(b)(3).
8. 529 F.3d at 900.
9. *Id.*
10. 18 U.S.C. § 2510(15).
11. 529 F.3d at 902. *See also Theofel v. Farey-Jones*, 359 F.3d 1066, 1070 (9th Cir. 2004) (provider of email

services is an ECS, even though it stores emails on its servers for backup protection).

12. *Id.* at 903.
13. 480 U.S. 709 (1987).
14. 529 F.3d at 899.
15. *Id.* at 906.
16. *Id.*
17. *Id. Compare Cowles Publishing Co. v. Kootenai County Board of County Commissioners*, 159 F.2d 896 (2007) (policy not contradicted by practice meant no reasonable expectation of privacy in employee emails).
18. *Id.* at 907.
19. *Id.* at 906-08.
20. *Id.* at 906.
21. *Id.* at 908-09.
22. *Id.*
23. 554 F.3d 769 (9th Cir. 2009).
24. 480 U.S. 709 (1987).
25. 554 F.3d at 774.
26. *Id.* at 769-73.
27. 480 U.S. 709.
28. *Id.*
29. 529 F.3d at 908-09.
30. 442 U.S. 735, 742 (1979).
31. 313 F.3d 1206, 1209-10 (9th Cir. 2002).
32. *U.S. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008).
33. *Quon, supra*, at 905, *citing Forrester, supra*, at 511.
34. *Id.* at 905-906 (citations omitted).
35. *See, e.g., Hennessey v. Coastal Eagle Point Oil Company*, 129 N.J. 81 (1992); *Slohoda v. United Parcel Service*, 193 N.J. Super. 586 (App. Div. 1984). *But see Weigand v. Motiva Enterprises*, 295 F. Supp. 2d 465 (D. N.J. 2003) (employer properly terminated employee for operating white supremacist mail order business outside of work).
36. 554 F.3d at 774.

Maureen S. Binetti is a shareholder with Wilentz, Goldman & Spitzer, P.A. in Woodbridge, and chairs its employment law department, which represents both

employers and employees. A certified civil trial attorney and member of the College of Labor and Employment Lawyers, she handles all types of employment law advice, litigation and investigation matters, and has mediated over 200 employment law cases. The author gratefully acknowledges the assistance of Christopher R. Binetti, paralegal/intern, in the preparation of this article.