Oklahoma Journal of Law and Technology

Volume 6 | Number 1

January 2010

Not So Fast: Quon v. Arch Wireless Is Not Employees' License to Text the Workday Away

Amanda R. Higgins

6 OKLA. J.L. & Tech. 48 (2010)
www.okjolt.org

NOT SO FAST: *QUON V. ARCH WIRELESS* IS NOT EMPLOYEES' LICENSE TO TEXT THE WORKDAY AWAY

Last year, the Ninth Circuit Court of Appeals decided *Quon v. Arch Wireless*,[1] a case that had privacy advocates jumping for joy, but only because they were jumping the gun. Many thought it was the beginning of a new level of privacy for employees in the workplace. One CNET blogger insisted that the *Quon* decision meant that "employees' text messages are now safe from their bosses' prying eyes."[2] Similarly, a newspaper headline shouted "Prying Bosses Get the Message," going on to claim that the ruling would affect "all employers who contract with an outside provider for messages."[3] "Bosses Can't Read Employees' Messages, Court Says" proclaimed a headline from Entrepreneur Information Management Journal in the Fall of 2008. [4] The same article goes on to quote from *Newsweek* in its conclusion that the Ninth Circuit's ruling "means that Quon's texts—and by proxy, millions of other messages from millions of other users—are protected from 'employers prying eyes.'"[5] So many were eager to report that every employee was now free to message away at any time, without their boss reading those messages. But these articles, in general, overstate the effect of the *Quon* decision, with some reactions in those early days being just plain wrong.

---

[1] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892 (9th Cir. 2008).
[2] Matthew Hirsch, *Quon v. Arch: Curb Your Enthusiasm*, GIGAOM, Jun 28, 2008, http://gigaom.com/2008/06/28/quon-v-arch-curb-your-enthusiasm/ (last visited Apr. 12, 2010).
[3] Maura Dolan, *Prying Bosses Get the Message,* L.A. TIMES, June 19, 2008, http://articles.latimes.com/2008/jun/19/local/me-text19.
[4] Nikki Swartz, *Bosses Can't Read Employees' Messages, Court Says: In a Victory for Workplace Privacy, An Appeals Court Ruling Has Made It More Difficult for Employers to Snoop in Employees' Electronic Messages,* INFO. MGMT. J., Sept.-Oct. 2008, http://www.entrepreneur.com/tradejournals/article/185428121.html (last visited Apr. 12, 2010).
[5] *Id.*

The September 2008 issue of Privacy & Data Security Law Journal asks whether "text messages . . . (are) fair game for review by employers interested in checking up on their employees . . ."[6] The same article answers its own question with a resounding "No," because of its own unequivocal interpretation that "The Ninth Circuit . . . held that an employer may not read its employees' text messages without the consent of the employees *and* the recipients of the text messages . . . (creating) a new set of challenges for employers."[7] Given the limited effect of the decision, these articles are far from the truth. Given the multitude of mistaken interpretations of the *Quon* opinion, a realistic assessment of the decision and the current state of the law in this area is warranted.

This year, *Quon* was denied rehearing en banc by the Ninth Circuit, when many thought the decision would be overturned. Despite the uproar in the period following the decision, the actual effect of the *Quon* decision is limited for two reasons. First, because the decision is limited to its facts, its effect much more narrow than it may have appeared. Second, *Quon* is limited because it fails to use the proper Fourth Amendment "search" analysis for public employees. *Quon* is a collision of dated privacy laws, the modern workplace, the latest forms of human interaction, and technology that is constantly updated. In the words of Judge Kim McLane Wardlaw, one of the Ninth Circuit panel judges in *Quon*,

> The extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet Age is an open question. The recently minted standard of electronic communications via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.[8]

---

[6] Wendy M. Lazerson & Kristen M. Pezone, *Text Messages Off Limits*, 3 PRIVACY & SECURITY DATA L.J. 825 (2008).
[7] *Id.*
[8] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904 (9th Cir. 2008).

Quon is an interesting example of the collision of the old privacy laws with the law governing electronic communications, which "is just past its infancy and undergoing significant growing pains" (Inside Counsel Article). While the opinion has caused some understandable confusion due both to the way it was written and the well-intentioned enthusiasm of privacy advocates, its effect on the future of privacy laws in the workplace is limited. Additionally, its Fourth Amendment analysis is an erroneous misstatement of the law which only serves to add confusion rather than clarify the current law dealing with employee privacy.

Part I of this paper will provide the factual and procedural background of *Quon*, a case complete with a set of juicy facts and some contemporary legal issues. Part II will review the historical framework of Fourth Amendment law leading up to the decision. Part III will highlight the Court's mistakes. Part IV predicts a limited future effect of the *Quon* decision on workplace privacy rights and some suggestions for both employers and employees in light of the current state of the law in this area.

Quon's **Facts and Procedural History**

Quon v. Arch Wireless deals with text messages, unrelated to work, sent and received by a state employee using a two-way pager issued to him by his public employer for use on the job. Jeff Quon was a Sergeant and member of the SWAT team for the City of Ontario ("the City"), located thirty-five miles east of Los Angeles in San Bernardino County, California. In 2001, the City issued twenty two-way alphanumeric pagers to its employees, including Sergeant Quon.[9] Members of the SWAT team received the pagers for the purpose of enabling better coordination and a quicker, more effective response to emergency situations.[10]

---

[9] *Id.* at 895.
[10] Quon v. Arch Wireless Operating Co. Inc., 445 F. Supp. 2d 1116, 1123 (C.D. Cal. 2006).

The City had a contract with Arch Wireless. The latter was to provide wireless text-messaging services for the City. Text messages sent from one Arch Wireless two-way alphanumeric pager were sent to another pager via a radio frequency transmission, received by a station also owned by Arch Wireless. The sent message was entered into the Arch Wireless computer network via transmission, then sent to the company's computer server. There, a copy was archived and stored in the system for up to seventy-two hours until the recipient pager was ready to receive the text message.[11]

While the city issued the pagers to employees like Quon, it had no official policy governing use of the text-messaging pagers specifically.[12] There was an official "Computer Usage, Internet and E-mail policy" ("the Policy"), which warned employees that

> [t]he use of City-owned computers and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computers is limited to City of Ontario related business. The use of these tools for personal benefit is a significant violation of City of Ontario Policy . . . [a]ccess to all sites on the Internet is recorded and will be periodically reviewed by the City. The City . . . 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 . . . [a]ccess 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 . . . [t]he use of inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail system will not be tolerated.[13]

Thus, the Policy was fairly thorough regarding computer usage, including the Internet and e-mail. Absent other facts, an employee reading and signing such a policy would have no reasonable expectation of privacy in his or her use of these particular resources. Indeed, Jeff Quon signed an "Employee Acknowledgment" in 2000 which had borrowed language from the Policy and indicated that he "read and fully [understood]" the Policy and acknowledged that the

---

[11] *Quon,* 529 F.3d at 895-96.
[12] *Id*. at 896.
[13] *Id*.

City could monitor and log all network computer and Internet activity without notice and that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[14] Additionally, in 2002, Quon attended a meeting where a Commander with OPD announced that "the pager messages 'were considered e-mail, and that those messages would fall under the City's policy as public information and eligible for auditing.'" Quon barely recalled attending the meeting and had no recollection of this announcement.[15]

While there was a clear policy governing computer, Internet and e-mail usage, there was no official policy governing use of the pagers. However, the court did find an *informal* policy governing the pagers.[16] Under the contract with Arch Wireless ("the contract"), twenty-five thousand text message characters were allotted to every pager each month, with the City liable for payment of any overage charges. OPD's Lieutenant Duke was responsible for managing the contract, paying any overages, etc. According to Duke, if there were any texting overages at the end of the month, he would notify the employee to whom the pager was assigned, and that employee would pay for that overage, usually by writing a personal check to the City. This system worked perfectly until August of 2002, when Lieutenant Duke became tired of this extra responsibility.[17]

According to a memorandum dated July of 2003 entitled "Internal Affairs Investigation of Jeffery Quon," Lieutenant Duke was interviewed by Sergeant Patrick McMahon. Duke told McMahon that he had gone to Sergeant Quon at some point and told Quon that the pagers were "considered e-mail and could be audited." Duke told Quon that "it was not his intent to audit employee text messages to see if the overage [was] due to work related transmissions." Duke

---

[14] *Id*.
[15] *Id*.
[16] *Id*. at 897.
[17] *Id*.

told Quon that he, Quon, could reimburse the City for any overages and, as a result, Duke would not need to audit the text messages to see if any were not work related. Duke later added that he recalled telling Quon "I didn't want to get into the bill collecting thing, so he needed to pay for his personal messages so we didn't—pay for the overage so we didn't do the audit. And he needed to cut down on his transmissions." Sergeant Quon only remembered being told, "If you don't want us to read it, pay the overage fee."[18]

Quon exceeded the monthly character limit three or four times prior to August of 2002, and each time he paid for the overages. When, in August of 2002, Quon and another officer went over the limit again, Lieutenant Duke complained in a meeting, at which point he was ordered by Chief Scharf to "request the transcripts of those pagers for auditing purposes."[19] So began the internal affairs investigation of Jeff Quon and the use of his work pager.[20] According to the record, the purpose behind obtaining the transcripts was to determine if the messages were exclusively work related, in which case the contract with Arch Wireless may need to be amended to increase the monthly character allowance for the pagers, or if the pagers were being used for personal reasons.[21]

City officials then e-mailed an account support specialist for Arch Wireless, Jackie Deavers. Deavers made sure the phone numbers on the transcripts matched those the City had included in its e-mail to her, and made sure the numbers actually went to pagers belonging to the City. She then placed the transcripts in a manila envelope and took them to the City. Ms. Deavers did acknowledge later that she realized the messages appeared to be sexually explicit. She also stated that only the "contact" on the account could receive the transcripts and, in this

---

[18] *Id.*
[19] *Id*. at 897-98.
[20] *Id*. at 897.
[21] *Id*. at 898.

case, the City was the account contact. Neither Quon nor any other user of the City's pagers was notified that Arch Wireless provided the transcripts. According to Chief Scharf's testimony, after receiving the transcripts, the City proceeded to audit them "to determine if someone was wasting . . . City time not doing work when they should be."[22]

However, a jury at the district court level found that the purpose of the audit, for the record, was to determine the adequacy of the monthly character limit for text messages under the contract with Arch Wireless.[23] The audit revealed that Quon "had exceeded his monthly allotted characters by 15,158 characters . . . many of these messages were personal in nature and were often sexually explicit." The messages had been sent to and received from Sergeant Quon's wife and other employees of OPD, including one officer with whom Sergeant Quon was having an extramarital affair.[24]

Sergeant Quon, along with his wife and other OPD employees ("Plaintiffs") filed suit in February of 2003 in the United States District Court for the Central District of California against Arch Wireless for alleged violations of the federal Stored Communications Act ("SCA")[25], and against the City of Ontario, OPD, Chief of Police Scharf, and internal affairs officer Glenn (collectively "Governmental Defendants") for a § 1983 Fourth Amendment claim under federal law and for violations of the California Constitution, California Penal Code section 629.86, invasion of privacy, and defamation.[26]

---

[22] *Id*.
[23] *Id*.
[24] Quon v. Arch Wireless Operating Co. Inc., 445 F. Supp. 2d 1116, 1126 (C.D. Cal. 2006).
[25] Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. Generally, the Act prohibits "providers" of communication services from revealing private communications to certain entities and/or individuals. The Act is more stringent with "electronic communication services" than with "remote computing services," the latter providing more of a computer storage function, rather than communication function.
[26] *Quon,* 445 F. Supp. at 1129.

District Judge Stephen G. Larson reviewed the factual findings outlined above and granted summary judgment for Arch Wireless on the SCA claim.[27] Congress passed the SCA because, since the appearance of the Internet, there are a multitude of potential invasions of privacy never addressed by the Fourth Amendment.[28] The SCA was created to prevent communication service providers from "divulging private communications to certain entities and/or individuals."[29] Nevertheless, Arch Wireless was victorious at the district court level.

Next, the Ninth Circuit addressed the Constitutional claim against the City. It ruled that the search was reasonable under the Fourth Amendment and granted summary judgment in favor of the Governmental Defendants. Plaintiffs appealed to the Ninth Circuit Court of Appeals, whose opinion was released on June 18, 2008.

The Ninth Circuit affirmed in part and reversed in part. It reversed the district court's SCA holding.[30] The SCA presents a different set of issues related to electronic communications which service providers must take care not to violate. It is another wrinkle in the fabric of privacy law that is beyond the scope of this paper. Next, in rather broad language, the Ninth Circuit held that "users of text messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text messages stored on the service provider's network."[31] It further ruled, in agreement with the district court, that Sergeant Quon had a reasonable expectation of privacy in the text messages he sent using the two-way pager issued by the OPD for police business, given OPD's informal policy governing the text messages.[32]

---

[27] *Quon,* 529 F.3d at 903.
[28] *Id*. at 900.
[29] *Id*.
[30] *Id*. (explaining that, since the Arch Wireless was an "electronic communication service" or "ECS" under the SCA, rather than a "remote computing service" or "RCS," the company was per se liable for knowingly providing the text message transcripts to the City (which was not an "addressee or intended recipient") and therefore had violated section 2702 of the SCA).
[31] *Id*. at 904.
[32] *Id.* at 906.

Finally, it ruled that the reading of the transcripts of Quon's text messages by OPD staff was unreasonable "given less intrusive methods" and "in light of the non-investigatory object of the search" and therefore violated Quon's reasonable expectation of privacy and the Fourth Amendment.[33]

Historical Framework

Drafted by the Framers in 1791, the Fourth Amendment was to guarantee "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . "[34] A "search" has been defined as "any intrusion with the purpose of obtaining physical evidence or information, either by a technological device or the use of the senses into a protected interest."[35] Individuals' privacy interests are protected from government intrusion via the Fourth Amendment. For a claimant to prove a Fourth Amendment violation against the government, he or she must show "a reasonable expectation of privacy in the item seized or the area searched, [and must] also demonstrate that the search was unreasonable."[36] All citizens' reasonable expectations of privacy are protected from unreasonable searches by federal and state law enforcement officials by the Constitution. Federal employees' reasonable expectations of privacy in the workplace are protected from unreasonable searches by their employers under the Fourth Amendment. State employees are protected in the same way by the Fourth Amendment, applied to states via the Fourteenth Amendment.

The Supreme Court has pronounced that the Fourth Amendment "protects people, not places," and thus does not apply only to physical intrusions.[37] In *Katz*, the Court held that there

---

[33] *Id*. at 908-09.
[34] U.S. CONST. amend. IV.
[35] Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?,* 70 ALB. L. REV. 1, 3 (2006).
[36] *Quon*, 529 F.3d at 904.
[37] Katz v. United States, 389 U.S. 347, 351-53 (1967).

was in fact a search under the Fourth Amendment when the government listened to and recorded a telephone conversation held in a phone booth by the defendant.[38] In doing so, the Court ruled that the government had violated privacy upon which the defendant had justifiably relied.[39] The Court reasoned that "one who occupies [a phone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[40] After *Katz*, the key to whether or not a government action constituted a "search" depended upon whether there was a reasonable expectation of privacy in the item or placed searched. A "reasonable" expectation of privacy was defined in *Katz* as what society is prepared to recognize as being reasonable.[41]

Twelve years later, the law from *Katz* was applied to the government's use of a pen register, a device used to record numbers dialed into a telephone.[42] The Court held that there was no reasonable expectation of privacy in the numbers a person dials into a telephone, because people knew when they dialed a telephone number that number may be recorded by a telephone company through whose switching equipment the numbers were transmitted.[43] Because the information was voluntarily provided to a third party, there was no reasonable expectation of privacy in the numbers dialed into a telephone. The Court in *Smith* also reasoned that pen registers, unlike recordings of telephone conversations, "do not acquire the contents of communications."[44]

---

[38] *Id*. at 348.
[39] *Id*. at 353.
[40] *Id.*
[41] *Id*. at 361.
[42] Smith v. Maryland, 442 U.S. 735 (1979).
[43] *Id*. at 742-43.
[44] *Id*. at 741.

In addition to telephone conversations and pen registers, the Court has analyzed whether government surveillance of physical mail constitutes a search under the Fourth Amendment.[45] The Supreme Court has held, as a general rule, the government cannot make a warrantless search of the inside contents of mail, but whatever is on the outside of mailed letters or packages can be observed, since that information is voluntarily transmitted to third parties.[46] Thus, the inside of the mailed package is akin to the private telephone conversation in *Katz* wherein there is a reasonable expectation of privacy; the outside of a mailed package is more like the pen register in *Smith*, where no government search is found because the information is voluntarily provided to third and there is no reasonable expectation of privacy. No reasonable expectation of privacy means no "search" under the Constitution.

In order for there to be a "search" under the Constitution, there is a two part requirement, according to Justice Harlan in his concurring opinion in *Katz*, another case originating in the Ninth Circuit.[47] Under the two-part test, there must first be "an actual (subjective) expectation of privacy."[48] Next, that subjective expectation "must be one that society is prepared to recognize as 'reasonable.'"[49] Unless this twofold test is satisfied, the analysis ends and the Fourth Amendment is not implicated.

Courts have used the analysis from these older cases in more recent decisions dealing with the Internet and electronic searches and surveillance. For example, in *United States v. Forrester*, the Ninth Circuit 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

---

[45] United States v. Jacobsen, 466 U.S. 109 (1984); United States v. Van Leeuwen, 397 U.S. 249, 251-52 (1970); *Ex parte* Jackson, 96 U.S. 727, 733 (1877).
[46] *Jacobsen*, 466 U.S. 109; *Van Leeuwen*, 397 U.S. at 251-52 (1970); *Jackson*, 96 U.S. at 733.
[47] Katz v. United States, 389 U.S. 347, 361 (1967) (J. Harlan, dissenting).
[48] *Id*.
[49] *Id*.

provided to and used by Internet service providers for the specific purpose of directing the routing of information."[50] Thus, the Ninth Circuit in *Forrester* "extended the *pen register* and *outside of envelope* rationales to the 'to/from' line of e-mails."[51]

The Ninth Circuit also noted that it has not yet ruled on whether there is a reasonable expectation of privacy in the content of e-mails.[52] The *Forrester* Court went on to conclude that "[t]he privacy interests in these two forms of communication [letters and e-mails] are identical, [and while] the contents may deserve Fourth Amendment protection . . . the address and size of the package do not."[53] The *Forrester* Court noted that "the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here."[54] Thus, these cases illustrate the way courts are dealing with the collision of traditional Fourth Amendment case law and modern forms of communication. The line of what is a "reasonable expectation of privacy" is repeatedly drawn between form and content, regardless of the method of communication.

Privacy in the Public Sector

As an employee of the State of California, Jeff Quon worked in the public sector. Due to the nature of jobs in the public sector, the Fourth Amendment analysis is somewhat different for government employees. The framework is the same, but the analysis changes specifically at what expectations of privacy are "reasonable" for these employees (given the nature of the public sector work environment) and what types of searches by employers are "unreasonable" (given the obvious need for efficiency in public sector workplaces). To compare, private employees aren't protected at all from searches by their employers under the Constitution. But the

---

[50] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).
[51] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 905 (9th Cir. 2008) (emphasis added).
[52] *Id*.
[53] *Forrester,* 512 F.3d at 511.
[54] *Id*. at 510.

protections afforded to both public and private employees from law enforcement searches may be greater than the protections afforded to public employees from searches by their employers. The difference comes down to the "reasonableness" analysis. This was explored more fully by the Supreme Court in *O'Connor v. Ortega* in 1987.[55] The *O'Connor* Court first discusses privacy and the workplace in general, and defines the "workplace" as

> those areas and items that are related to work and are generally within the employer's control. At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board.[56]

The *O'Connor* Court wrote that it recognized public employees may have a reasonable expectation of privacy against intrusions by police.[57] The Court noted that what is a reasonable expectation of privacy and what is a reasonable search differs according to context.[58] It went on to write (about public employees specifically),

> [Although] the operational realities of the workplace may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official and, as a result, employees' expectations of privacy in their offices, desks, and file cabinets may be reduced by virtue of actual office practices and procedures . . .[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer.[59]

As the *O'Connor* Court writes, given the wide variety of public sector work environments (some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable), the question whether a given employee has a reasonable expectation of

---

[55] O'Connor v. Ortega, 480 U.S. 709, 712-29 (1987).
[56] *Id*. at 715-16.
[57] *Id*. at 716 (citing Mancusi v. DeForte, 392 U.S. 364 (1968)).
[58] *Id*. at 715.
[59] *Id*. at 717.

privacy can only be addressed on a case-by-case basis.[60] In *O'Connor*, a physician and psychiatrist, Dr. Magno Ortega, had been Napa State Hospital's Chief of Professional Education for seventeen years.[61] He was responsible for the training of young physicians in psychiatric residency programs. Hospital officials became aware of alleged improprieties in Dr. Ortega's management of the program, including allegations that Dr. Ortega had sexually harassed two female employees and improperly disciplined a resident. Officials requested that the doctor take paid administrative leave while the charges were investigated. Ortega was to stay clear of hospital grounds throughout the investigation. During the investigation, someone entered Dr. Ortega's office.[62] The reason for the entry was disputed. At the time, there was no policy of inventorying the office of an employee on administrative leave. During the search, several items were seized from the doctor's desk and file cabinets. The items were later used in the disciplinary proceeding against Dr. Ortega.[63]

Dr. Ortega sued the hospital in Federal Court under 42 U.S.C. § 1983, alleging violations of the Fourth Amendment (applied to the State Hospital by the Fourteenth Amendment) in the search of his office.[64] The district court granted summary judgment for the hospital, calling the search proper because there was a need to secure state property in the office. On appeal, the Ninth Circuit reversed in part, ruling that the doctor had a reasonable expectation of privacy in his office. The Court explained that "[w]hile the Hospital had a procedure for office inventories, these inventories were reserved for employees who were departing or were terminated." Since Dr. Ortega was not, at that point, "departing or terminated," but merely on administrative leave, his expectation of privacy in his office, desk, and file cabinets was reasonable. Without

---

[60] *Id.* at 718.
[61] *Id*. at 712.
[62] *Id*. at 713.
[63] *Id*.
[64] *Id*. at 714.

explaining why it did so, the Ninth Circuit then held that the search of his office violated the Fourth Amendment.[65] The hospital appealed to the U.S. Supreme Court.

The Supreme Court began by stating that "searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment."[66] The Court went one to write, "[However], [p]ublic employees' expectations of privacy in their offices, desks, and file cabinets . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[67] The Court then went on to assess whether, under the facts of the case, Dr. Ortega had a reasonable expectation of privacy. This is the point at which the facts of each individual case become key. Because Dr. Ortega did not share his desk or file cabinets with any other employees, he had occupied the office alone for seventeen years and kept many public and private materials there, and there was no evidence of any policy or regulation discouraging employees from doing so, the Court agreed that the doctor had a reasonable expectation of privacy in his desk and file cabinets.[68]

Having found that, due to such reasonable expectation, there had been a "search" and the Fourth Amendment would apply, the Court began its analysis of whether the search was reasonable.[69] The Court first explained that, in assessing the reasonableness of a work-related search by a public employer of its employees' offices, desks, or file cabinets, it "must balance the invasion of the employees' legitimate expectations of privacy against the government's need

---

[65] *Id.*
[66] *Id*. at 715.
[67] *Id*. at 717.
[68] *Id*. at 718-19.
[69] *Id*. at 719.

for supervision, control, and the efficient operation of the workplace."[70] Up to this point, case law had generally held that "any 'work-related' search by an employer was reasonable."[71]

To start, the Court limited the scope of its analysis to (1) "noninvestigatory work-related intrusions" or (2) "investigatory searches for evidence of suspected work-related employee misfeasance."[72] The Court stated that a warrant requirement for public employers was unreasonable, because such a requirement would be burdensome to the conducting of public business.[73] The Court has explained that the vast majority of work-related searches are "merely incident to the primary business of the agency . . . [and] the imposition of a warrant requirement would conflict with 'the common-sense realization that government offices could not function if every employment decision became a constitutional matter."[74] The *O'Connor* Court goes on to state that requiring a public employer to show probable cause prior to conducting a workplace search would also be too burdensome in light of the public employers' interest in insuring that their agencies operate in an effective and efficient manner, free from inefficiency, incompetence, mismanagement, or other work-related misfeasance of its employees.[75] The Court adopts a standard of "reasonableness under all the circumstances" for public employer searches of the workplace.[76] Under the standard, "both the inception and scope of the intrusion must be reasonable."[77] The notions of "inception" and "scope" can be further explained:

> Ordinarily, a search of an employee's office by a supervisor will be 'justified at its *inception*' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to

---

[70] *Id.* at 719-20.
[71] United States v. Nasser, 746 F.2d 1111, 1123 (C.A. Ohio 1973); United States v. Collins, 349 F.2d 863, 868 (C.A.N.Y. 1965).
[72] *O'Connor,* 480 U.S. at 723.
[73] *Id*. at 722.
[74] Connick v. Myers, 461 U.S. 138, 143 (1983).
[75] *O'Connor,* 480 U.S. at 724.
[76] *Id*. at 725-26.
[77] *Id*. at 726.

> retrieve a needed file . . . [t]he search will be permissible in its *scope* when 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct].'[78]

Therefore, the objective or reason for the search is a crucial part of the search analysis. After announcing the law, the *O'Connor* Court goes on to remand the case because the exact reason for the search was in dispute and unclear from the record.[79] Without knowing the reason or objective for the employer's search, it is impossible to determine whether the search is reasonable. Throughout *O'Connor* is a repeated reminder of the strong need of government employers to efficiently and effectively run public workplaces. Balanced against this need are the legitimate expectations of privacy a government employee may have. *O'Connor* states the law in an understandable and objective manner, providing a clear framework for analyzing public workplace searches. *O'Connor* remains good law.

Court's Reasoning in *Quon:* A Reasonable Expectation of Privacy

The Ninth Circuit first holds that all Plaintiffs have a reasonable expectation of privacy in the text messages they sent and received using the two-way pagers.[80] The Court reiterates that whether a public sector employee has a reasonable expectation of privacy is decided on a case-by-case basis.[81] The Court goes on to liken the text messages sent and received by the Plaintiffs to the e-mails at issue in *Forrester*: "both are sent from user to user via a service provider that stores the messages on its servers. Similarly, as in *Forrester*, we also see no meaningful distinction between text messages and letters."[82] In this part of the opinion, the Court uses broad language regarding text messages in general, based on their nature. It makes no difference that Arch Wireless could have accessed the message contents for its own purposes, since Plaintiffs

---

[78] New Jersey v. T.L.O, 469 U.S. 325, 342 (1985).
[79] *O'Connor,* 480 U.S. at 729.
[80] Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 904 (9th Cir. 2008).
[81] *Id*.
[82] *Id*. at 905.

had no expectation that Arch Wireless would monitor their text messages, let alone turn over the text messages to third parties without their consent.[83]

This fairly broad language on the privacy of text messages is confusing when read alongside the Court's more narrow analysis of Jeff Quon's reasonable expectation of privacy. The Court may be saying that, absent stronger evidence of a reasonable expectation of privacy in text messages, one may still generally have a reasonable (but perhaps less compelling) expectation of privacy that text messages won't be reviewed by a governmental employer. In this same section, the Court claims not to "endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-sensitive inquiry."[84] However, the Court's discussion is quite broad and employs a general discussion of the nature of text messages.[85] Thus, although the Ninth Circuit has yet to make a judgment as to the privacy interest in the content of e-mails,[86] this portion of the opinion will likely be used in the future by parties arguing for the protected privacy interest in text messages. The main holding deals with Jeff Quon's reasonable expectation of privacy as a public employee whose workplace had an informal policy of allowing personal use of the text messaging pagers, and is therefore narrow. Yet there is this peripheral holding which could be broad and will no doubt be subject to debate in the future. After *Quon*, one could argue that the Ninth Circuit considers text message content to be like the inside of a letter, or the contents of a private telephone conversation.

After looking broadly at privacy in text messages, the Court looks specifically at Jeff Quon's own expectation of privacy in the text messages. The Court holds that Quon had a

---

[83] *Id*. at 906.
[84] *Id*.
[85] *Id.*
[86] *Id*. at 905.

reasonable expectation of privacy.[87] The expectation was not reasonable because of the lack of formal policy or because of the general nature of text messages, but because of the presence of an informal policy regarding privacy in the text messages.[88] The Ninth Circuit agreed with the district court that OPD's informal policy dictated that the text messages, if the user paid the overage charges, would not be audited.[89] This made Quon's expectation of privacy reasonable.

It is this part of the opinion which most narrows *Quon*'s result. The Court is careful to explain that OPD's general "Computer Usage, Internet and E-mail Policy"

> stated that the use of computers "for personal benefit is a significant violation of City of Ontario Policy" and that "[u]sers 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 . . . As the district court made clear, however, such was not the "operational reality" at the Department.[90]

Specifically, Lieutenant Duke made it clear that if the overages were paid, there would be no audits.[91] Duke was in charge of administering the use of the pagers, so his statements were quite meaningful. The department did not audit any text messages at any time during the eight months since the pagers were distributed.[92] Plaintiff himself had gone beyond the 25,000 character limit three or four times, and paid for the overages every time without any review of the messages.[93] Given these facts, the Court found that the OPD followed its "informal policy" and that Quon's reliance on it was reasonable.[94] The Court's finding of a reasonable expectation of privacy was

---

[87] *Id*. at 907.
[88] *Id*.
[89] *Id*. at 906.
[90] *Id*. at 906-07.
[91] *Id.* at 907.
[92] *Id*.
[93] *Id*.
[94] *Id*.

based wholly on the fact that there was an informal policy at OPD allowing personal use of the city-owned pagers.[95]

Court's Reasoning in *Quon*: An Unreasonable Search

Once a plaintiff shows a reasonable expectation of privacy such that there was in fact a "search" under the Fourth Amendment, the Plaintiff must then show that the search was unreasonable.[96] For a search to be reasonable, it must be reasonable both at its inception and in its scope.[97] If a search passes muster on both points, it is deemed reasonable under the Fourth Amendment.

The record reflected that the governmental defendants' purpose in auditing the text messages was "to determine the efficacy of the 25,000 character limit," something that amounted to a noninvestigatory work-related purpose.[98] The jury expressly rejected the other possibility: that the purpose of the audit was to uncover misconduct.[99] The Ninth Circuit was bound by this factual finding. If the scope of the search was reasonable in relation to this object, the governmental defendants would win.

In this part of the analysis, the court makes its error. Instead of sticking with the precedent in *O'Connor*, which explained that the scope of a search is reasonable when the adopted measures are reasonably related to the search objectives and not excessively intrusive . . .",[100] the court goes on to improperly narrow the test, using language from *Schowengerdt v. Gen. Dynamics Corp*, a Ninth Circuit case from 1987, and states that "[i]f less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the

---

[95] *Id.*
[96] O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987).
[97] *Id*. at 726.
[98] *Quon*, 529 F.3d at 908.
[99] Quon v. Arch Wireless Operating Co., Inc., 554 F.3d 769, 771 (9th Cir. 2009) (denying rehearing en banc).
[100] *O'Connor*, 480 U.S. at 726.

government's legitimate purposes . . . the search would be unreasonable."[101] The Court begins taking significant liberties here when it writes "there were a host of simple ways to verify the efficacy of the 25,000 character limit without intruding on Appellants' Fourth Amendment rights."[102] For example, the Court reasons that Quon could have been warned that he could not use the pager for personal communications for the following month, and that his message contents would be reviewed during that time frame;[103] he could have been asked to count the characters himself, or redact the personal content and give permission to the Department to view the redacted transcript. Because these "less intrusive alternatives" were possible, the search was unreasonable.[104]

This analysis is incorrect. First, the court's use of the more restrictive language from *Schowengert* is misplaced, considering that the *O'Connor* opinion, decided the same year as *Showengerdt*, is accepted as the correct analysis for cases regarding workplace privacy of public employees. Again, *O'Connor*'s language and reasoning shows intent to give public employers broad limits for searches of employees' work areas due to the need to run efficient workplaces.

Circuit Judge Ikuta's dissent in the *denial of rehearing en banc* goes on to state that "the Supreme Court has repeatedly rejected a 'least intrusive means' analysis for purposes of determining the reasonableness of a search."[105] In addition, Ikuta points out that seven other circuits have followed suit. The majority battles back here, pointing out that Ikuta has cited "special case" opinions for the proposition that a "least intrusive means" test should not be used.[106] However, that fact does not really help the majority's argument. Regardless of which

---

[101] *Quon,* 529 F.3d at 908 (quoting Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1336 (9th Cir. 1987)).
[102] *Id.* at 909.
[103] *Id.*
[104] *Id*.
[105] *Quon*, 554 F.3d at 778 (S. Ikuta, dissenting).
[106] *Id.* at 773.

cases Ikuta cites in his dissent, the proper analysis from *O'Connor* remains the same, and it is not a "least intrusive means" test.

The majority basically denies use of a "least intrusive means" analysis: "We mentioned other ways the OPD could have verified the efficacy of the 25,000-character limit merely to illustrate our conclusion that the search was 'excessively intrusive' under *O'Connor*, when measured against the purpose of the search as found by the jury."[107] In fact, the Ninth Circuit in *Quon* did more than "mention" other ways the OPD could have determined the adequacy of the character limit. The Ninth Circuit wrote

> The district court determined that there were no less-intrusive means . . . [w]e disagree. There were a host of simple ways to verify the efficacy of the 25,000 character limit (if that, indeed, was the intended purpose) without intruding on Appellants' Fourth Amendment rights. For example, the Department could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if the Department wanted to review past usage, it could 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. . . . These are just a few of the ways in which the Department could have conducted a search that was reasonable in scope.[108]

Whether or not the correct conclusion was reached, the Court's lip service to the district court's discussion of a "least intrusive alternative" is confusing in light of *O'Connor*'s strong language mandating that government employers should not be overly burdened in determining whether a search can be done.[109]

The proper way to analyze the search would have been a determination of whether, in light of the stated noninvestigatory, work-related purpose for the search, the act of reading the content of the text messages was reasonably related to the need to determine whether a higher

---

[107] *Id.* at 774.
[108] *Quon,* 529 F.3d at 908-09.
[109] *Id*.

character limit was needed.[110] Instead, the Ninth Circuit in *Quon* engaged in just the kind of "post hoc evaluations of government conduct [where judges can] almost always imagine some alternative means by which the objectives of the government might have been accomplished."[111] Such analysis in these cases "could raise insuperable barriers to the exercise of virtually all search-and-seizure powers."[112] Indeed, this "least-intrusive means" test defeats both the stated law of *O'Connor* and the logic behind the *O'Connor* decision: maintaining efficiency in the public sector in regard to employer searchers. This part of the Ninth Circuit opinion is somewhat cleared up by the majority in the denial of rehearing en banc. While the Ninth Circuit's improper analysis could be called a harmless error, the Ninth Circuit should have focused more on whether society is prepared to recognize Quon's expectation of privacy as reasonable, given his public position and the unique facts of the case. To focus the analysis elsewhere is less than helpful in this already murky area of law.

Regardless of how the Court decided the case, its decision is held to its facts. Jeff Quon's reasonable expectation of privacy stems from the unofficial policy in his particular workplace. The opinion goes no further. It does not speculate about varied fact patterns. As it stands, it is yet unclear whether a public employee like Quon could have a reasonable expectation of privacy in a slightly different situation, such as where there is an applicable formal policy *and* an informal policy, or where there is neither an official nor an unofficial policy in place. Because this holding is so limited, it practically begs for a new case to address the issue more broadly. One thing is certain: the opinion did not warrant the early headlines it inspired. In fact, we need

---

[110] *Id.*
[111] *Quon*, 554 F.3d at 778 (S. Ikuta, dissenting) (citing Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989)).
[112] *Id.*

not wait long for *Quon* to be looked at again.[113] Perhaps the Supreme Court will provide some much-needed guidance. Although *Quon* could be overturned next year, the danger to public employers is right now, and it is very real.

Future of *Quon* Decision and Practical Advice for Employers

It is important to remember a few things about this opinion. First, Jeff Quon was a state employee and therefore protected by the Fourth Amendment from unreasonable searches by his public employer. The holding does not apply to private employment situations wherein the Constitution does not apply. Therefore, private employees cannot depend on cases like *Quon* for privacy protection. Had Jeff Quon been a private employee, there would have been no Constitutional claim against his employer.

Second, the *Quon* Court brings text message content into the fold alongside the content of a mailed letter and a private telephone conversation as something in which users generally have a reasonable expectation of privacy. The Court also has excluded the "address" to or from which a text message is sent from Fourth Amendment protection, grouping this information with the to/from line of e-mails in *Forrester*, the information located on the outside of a mailed envelope or package from *Jacobsen*, and the information obtained by pen register in *Smith*. Therefore, although the Ninth Circuit has yet to rule on the content of e-mail messages sent using an employer's network, it appears that it has now ruled that the content of text messages are something in which an employee, or anyone else, has a reasonable expectation of privacy.[114]

---

[113] On December 14, 2009, the U.S. Supreme Court announced that it would take up the case of Quon v. Arch Wireless. The Court will hear arguments in Spring of 2010. See City of Ontario, Cal. v. Quon, -----S. Ct. ----- (U.S. Dec. 14, 2009).

[114] *Quon,* 529 F.3d at 904.

Third, although not emphasized in the opinion, the Court's finding that the Government Defendants had a noninvestigatory work-related purpose for conducting the search ended up harming the government's cause in the end. Had there been a finding that OPD had a legitimate purpose of investigating workplace misconduct, the Ninth Circuit may have ruled that reading the content of the messages without permission was not unreasonable in light of the object of the search. This serves as a cautionary tale for future public employers forced to litigate a case like *Quon*. Public employers will want to get on the court record that their search was for some purpose that will not only pass as reasonable at its inception under the facts of the case (for example, by appearing responsive to an apparently justified need to search) and will also allow the court to find that the actual method was not excessive in relation to the purpose. Since the Ninth Circuit was bound by the factual finding as to the object of the search, the actual method of searching did appear to be unreasonable in light of that object.

Finally, and most importantly for public employers, is the formal/informal policy issue. This employer not only lacked a formal policy specifically for use of the pagers, but there was an informal policy that the text messages would not be read by the employer. Lack of a formal policy by itself will not create a reasonable expectation of privacy. However, the presence of the informal policy was enough to create a reasonable expectation of privacy in the text messages, at least where there is no formal policy. Public employers must create a formal policy and live by it. Simply having a formal policy in place may not be enough if the actual practice in your workplace is such that the form of communication will be free from the eyes of employers. While the facts of *Quon* were that there was no formal policy regarding the text messages, other areas of law involving employers and employees, such as workplace discrimination and civil rights litigation, provide sound examples that informal policies can overcome the presence of

opposing formal policies. In light of the *Quon* opinion, one would not want to be an employer arguing in court that the formal policy regarding text messaging on the employer's electronic device, signed off on by every employee at the beginning of his or her employment, is enough to protect said employer from a Fourth Amendment cause of action for invading employee privacy.

While it isn't explicit, the *Quon* decision asserts that society is prepared to recognize as reasonable a public employee's expectation that the personal texts he or she sends using a device belonging to, issued by, and issued to forward the business of a public employer will remain free from the prying eyes of that employer, if the employee is given any reason to believe the messages will not be seen. Therefore, a wise employer can avoid this type of pitfall by updating workplace policies each and every time a new form of communication arrives in the workplace. Each update must expressly include the specific type of technology it seeks to cover. Once the policy is in place, the employer must strictly monitor the workplace to be sure the policies are being followed without deviation.

This may be a tall order, for a number of reasons. The busy nature of public work environments and the constant evolution of communication technology mean that there is always danger of employers' lagging behind the times. The natural desire of humans to communicate at home and work, coupled with the modern ability to do so swiftly and easily, often has the consequence of blending public and private communications. However, in this dangerous area of law for public employers, prevention is the soundest cure.