Volume 1 | Number 6 | September 2008

Editor: D. Reed Freeman, Jr., CIPP

Privacy TRACKER

iapp

A publication of the International Association of Privacy Professionals

Reading Your Employees' Text Messages May Get You Into Hot Water

Susan Acquista, Mary Ellen Callahan, Robin Samuel, and Laura Wilson

M. Callahan

R. Samuel

Do employees have a reasonable expectation of privacy in the content of text messages they send using equipment and service provided by their employer? The Ninth Circuit Court of Appeals recently held so in *Quon v. Arch Wireless Operating Co., Inc.*[1]. The Ninth Circuit in *Quon* determined that that the Ontario, California police department improperly invaded the privacy of one of its employee officers when it reviewed personal text messages sent by the officer using a two-way pager, even though the department supplied the pager, paid the monthly service charge for its use, and had a written policy stating that electronic devices should be used only for business purposes.

While the appellate court's decision in *Quon* most directly affects public employers because the court conducted its privacy analysis under the Fourth Amendment, which does not apply to private entities, the case nevertheless is relevant to private employers for two reasons. First, other courts likely will extend the reasoning of the *Quon* decision to private employers under state privacy laws. Many state constitutions explicitly grant their citizens the right to privacy, including California, Illinois, and Florida. Other states have common law privacy protections in place. Second, the *Quon* holding provides valuable lessons for both the public and private employment sectors about the use and enforcement of electronic communication policies. In particular, *Quon* serves as a cautionary tale for private employers who fail to heed their own written policies or whose policies and procedures may not be as up-to-date or as comprehensive as they should be.

Before delving into the facts of *Quon*, it is helpful to review the case law relied upon by the court for its important decision.

See ***Your Employees' Text Messages,*** *page 3*

[1] *Quon v. Arch Wireless Operating Co., Inc.,* No. 07-55282, 2008 WL 2440559, 2008 U.S. App. LEXIS 12766 (9th Cir. 2008).

In This Issue

Your Employees' Text Messages

continued from page 1

I. Historical Tensions

Employers have many reasons for wanting to control and monitor workplace communications. Doing so helps employers maintain a professional work environment, increase employee productivity, and control the dissemination of trade secrets or other proprietary and confidential information.

These employer interests naturally run contrary to employee privacy expectations, with the employer's desire to monitor workplace activities often frustrating perceived privacy concerns. With the advent of new communication technologies, and the integration of these technologies into the workplace, it also has become increasingly difficult for employers to protect their legitimate interests. And laws originally designed to regulate employee privacy in the "brick and mortar" world have become outdated as technology in the workplace evolves. As a result, courts are increasingly facing the tensions between employer monitoring and employee privacy in the workplace.

II. General Privacy Rights

In the public setting, the Fourth Amendment to the U.S. Constitution establishes the right to be free from government intrusion into private matters. In particular, the Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[2] An unreasonable search and seizure is one that violates a person's reasonable expectation of privacy.

Against this backdrop, courts provide guidance on when a search, and an expectation of privacy, will be deemed reasonable. In *Katz v. United States*[3] the U.S. Supreme Court held that the government's wiretapping of a telephone conversation that took place in a public telephone booth constituted an unreasonable search and seizure within the meaning of the Fourth Amendment. The Court reasoned that a person has a reasonable expectation of privacy in a public telephone booth because the person shuts the door, pays the toll, and does not expect the conversation to be broadcast to a third party. The Court also noted that using public telephone booths for private conversations had become a societal norm, and that privacy law should conform to the growing societal role that public telephone booths were playing in private communications.

While the content of a telephone conversation may be private, the telephone number that is dialed to initiate the conversation is not.[4] In *Smith*, the government used a pen register to record the telephone numbers dialed by the defendant. The *Smith* court distinguished *Katz* on the grounds that a pen register is different from a wiretap because the pen register records only the telephone number, and not the contents of the conversation. The *Smith* court noted that there is no reasonable expectation of privacy in a dialed telephone number because the number itself must be transmitted to the telephone company so that the call can be completed. Because the caller must rely on a third party, the telephone company, to complete the call, the caller cannot reasonably believe the dialed number will remain private.

The principles established in *Smith* were applied to postal mail in *United States v. Hernandez*.[5] In that case, the appellate court held that a person has a reasonable expectation of privacy in the contents of a letter or package but not in the address of the sender or recipient. Like the cases involving telephone conversations, the *Hernandez* court distinguished between the contents of a letter or package, which are concealed from third parties, and the address information on the exterior, which is not.

The Ninth Circuit recently extended the *Smith* and *Hernandez* holdings to e-mails in *United States v. Forrester*.[6] Adopting the reasoning of *Hernandez*, the appellate court held that while a person may have a reasonable expectation of privacy in the content of e-mails, there is no expectation of privacy in the "to/from" addresses of e-mail messages because the person sending the e-mail should know that this information is provided to and used by Internet service providers to route the e-mails.

---

[2] U.S. CONST. amend. IV.

[3] *Katz v. United States,* 389 U.S. 347 (1967).

[4] *Smith v. Maryland,* 442 U.S. 735 (1979).

[5] *United States v. Hernandez,* 313 F.3d 1206 (9th Cir. 2002).

[6] *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2008).

III. Electronic Privacy in the Workplace

In the seminal case of *O'Connor v. Ortega*[7] the Supreme Court addressed the reasonableness of a government worker's expectation of privacy in the workplace. The public employer in *Ortega* searched an employee's office as part of a non-criminal investigation. The search encompassed all of the contents of the employee's desk drawers and file cabinets. The *Ortega* court began its analysis by affirming that the Fourth Amendment applies to non-criminal investigations in the workplace of public employers. The Court then found that requiring employers to obtain a search warrant for such investigations presented too much of a burden for employers, thereby establishing an exception to the warrant requirement for non-criminal investigations that occur in the workplace.

The *Ortega* court ultimately constructed a two-part showing necessary to support a finding that a Fourth Amendment violation had occurred: (1) the person must have had a reasonable expectation of privacy in the area or item searched, and (2) the search itself must have been unreasonable under the circumstances. The Court held that, in this context, a search should be deemed unreasonable if there are no reasonable grounds to justify the search at its *inception*, and the *scope* of the search is excessively intrusive. The Court also held that the question of whether a person's expectation of privacy is reasonable is a factual determination that must be decided on a case-by-case basis.

Applying the two-part test, the Court found that the employee in *Ortega* had a reasonable expectation of privacy in his desk drawers and file cabinets. However, the Court acknowledged that certain "operational realities of the workplace" may render an employee's expectation of privacy unreasonable, and cited as examples workplace practices and procedures and legitimate employer regulations.

More recently, in *United States v. Ziegler*[8] the Ninth Circuit examined whether a public employee had a reasonable expectation of privacy in the contents of a work computer locked in his office, despite a company policy stating that computer usage would be monitored. As part of a government investigation into whether the employee was accessing child pornography from his workplace computer, the employer consented to and assisted a government search of the employee's computer for evidence of criminal activity. The employee claimed the government's search violated his reasonable expectation of privacy in his office computer, even though it belonged to his employer.

The Ninth Circuit concluded that the employee did indeed have a reasonable expectation of privacy in his office, but that the company could consent (on the employee's behalf) to a search of the computer within that office. The court found dispositive the fact that the employer routinely and actively monitored the computer usage of its employees and that the company had informed employees through its written policies and through training that the computers would be monitored and should not be used for personal reasons.

Muick v. Glenayre Elecs.[9] is another case that examined how employer policies can affect the "reasonableness" of an employee's expectation of privacy in employer-issued electronics. The employee in *Muick* sued his employer for seizing and holding his employer-issued laptop computer while law enforcement authorities obtained a search warrant. The employer had informed the employee, at the time it issued the laptop to him, that it reserved the right to inspect the laptop at any time. The Seventh Circuit held that the employer, by announcing its right to inspect the company-issued laptop at any time, had destroyed any reasonable expectation of privacy that the employee may have had in the laptop. The court went on to state that the employer, as owner of the laptop, had the right to attach specific conditions to its use, and therefore its policy of monitoring was not inherently unreasonable.

Bohach v. City of Reno,[10] a case involving technology similar to the two-way pagers at issue in *Quon*, also discussed how employer policies and procedures can defeat an employee's expectation of privacy in employer-issued electronics. The plaintiffs in *Bohach* were police officers who asserted that their privacy rights were being violated during an internal investigation that sought to examine messages they sent using the department's computerized paging system. The department had issued a memorandum to all of its employees informing them that messages sent to city-issued pagers would be logged on to the department's network and that certain types of messages were prohibited. It also was common knowledge that any employee with access to the department's computer system could see the messages that were sent and received. Under these facts, the court held that

[7] *O'Connor v. Ortega,* 480 U.S. 709 (1987).

[8] *United States v. Ziegler,* 474 F.3d 1184 (9th Cir. 2007).

[9] *Muick v. Glenayre Elecs.,* 280 F.3d 741 (7th Cir. 2002).

[10] *Bohach v. City of Reno,* 932 F. Supp. 1232 (D. Nev. 1996).

the plaintiff police officers had a diminished expectation of privacy and ruled against them.

These cases demonstrate that in the context of electronic communications, employees' expectations of privacy are not automatically overcome by an employer's ownership of the property or device being searched, that employee privacy expectations may be diminished through employer policies and procedures, and, most importantly, that privacy determinations are inherently factual and must be made on a case-by-case basis.

IV. The *Quon* Decision

The *Quon* case presented issues similar to those in the above cases, but unlike the prior decisions, the *Quon* court reached a different and somewhat surprising result.

The plaintiff, Sergeant Jeff Quon of the Ontario Police Department, and several persons with whom he "texted," filed suit against their employer, the Ontario Police Department and the City of Ontario (together, the "City"), and the City's wireless service provider, Arch Wireless, after Quon's supervisor at the police department obtained and reviewed the content of Quon's text messages without Quon's knowledge or consent. Quon had used a two-way alphanumeric pager issued to him by the Ontario Police Department to send and receive the text messages. His employer not only provided the pager, it also paid the bill for the text-messaging service.

In October 2001, the City and Arch Wireless entered into a contract under which Arch Wireless provided the City with two-way alphanumeric text-messaging pagers for its employees, as well as other wireless communication services incident to the use of the pagers. Under the contract, each pager was allotted up to 25,000 alpha-numeric characters per month, after which the City was required to pay overage charges.

The City distributed the pagers to members of the police department's SWAT team, which included plaintiffs Jeff Quon and Steve Trujillo. The City hoped that by providing two-way pagers capable of instantaneous communication, the SWAT team would be better able to respond to emergencies. The City did not intend that the two-way pagers would be used for personal purposes, especially while the officers were on-duty.

At the time, the City had no written policy regarding text-messaging, but the City did have a general "Computer Usage, Internet and E-mail Policy" that restricted the use of City-owned computers and all associated applications to work-related purposes. The policy also provided the City with the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Finally, the policy prohibited the use of "inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language," in e-mails. All employees of the Ontario police department, including Quon, had to review and sign a written copy of this policy before being issued any computer desktop equipment. In April 2002, the City held a staff meeting during which a supervisor allegedly informed Quon and other employees that text messages were considered e-mail, and therefore would fall under the City's auditing policy. This warning, however, was never given in writing.

Within a couple billing cycles after being issued the pager, Quon had exceeded his monthly allotment of 25,000 characters. His supervisor allegedly reminded Quon that the text messages sent using the City-owned pager were considered e-mail and therefore could be audited at any time, but Quon also was told that his messages would not be audited if he paid the overage charges himself. The City apparently had an informal practice of asking employees to pay the overage charge if their text-messaging exceeded the monthly limit of 25,000 characters. Employees were told that if they refused to pay the overage, their messages would then be audited to determine whether any were for purely personal matters. Quon exceeded the monthly character limit several times and paid the City for the overages each time without being audited.

In August 2002, Quon and another employee once again exceeded the monthly character limit. By this time, the City employee responsible for the Arch Wireless contract and for collecting the overage charges—Lieutenant Duke—had grown tired of playing the roll of "bill collector." In response, the police chief ordered Duke to obtain the transcripts of Quon's text messages, as well as those of other employees who used the pagers. Duke's task was to determine whether Quon's text messages were work-related. Quon was not informed of the police chief's decision, nor was he asked to pay the overage prior to the review.

To obtain the copies of Quon's text messages, Duke contacted an Arch Wireless representative and asked for a copy of Quon's text messages. A copy of every text message sent using the City-owned pagers was stored on an Arch Wireless server. After confirming that the pagers were owned by the City as part of its subscription and that the request came from a valid contact for the subscriber, Arch Wireless supplied Duke with the transcripts.

The transcript of Quon's text messages totaled forty-six pages in length. Many of the text messages that were sent or received on Quon's pager while he was on duty were sexually explicit in nature. Some of the messages were sent or received from Quon's wife, plaintiff Jerilyn Quon, while others were sent or received from Quon's mistress, plaintiff April Florio, a member of the Police Department's dispatch center. There were additional messages that were not sexually explicit, but nonetheless private in nature, which were sent or received from Quon's co-worker, plaintiff Sergeant Trujillo.

Quon, along with the other plaintiffs, filed suit in February 2003 against Arch Wireless, the City of Ontario, the Ontario Police Department, and members of the Police Department, asserting, among other claims, federal violations of the Stored Communications Act and the Fourth Amendment, and state law claims for violations of Article I, Section 1 of the California Constitution.

1. The *Quon* District Court Opinion

The district court divided its analysis into two parts. The court first concerned itself with the issue of whether Arch Wireless violated the Stored Communications Act (SCA) by supplying the City with the transcripts of Quon's text messages. In a complicated discussion outside the scope of this article, the district court eventually came to the conclusion that Arch Wireless was an immune entity within the definition of the SCA and therefore was not liable to the plaintiffs.

The court then turned to the question of whether the plaintiffs' privacy rights had been violated under the Fourth Amendment and Article I, Section 1 of the California Constitution. The court began by noting that it would confine its analysis to the Fourth Amendment claim because the defendants' state constitutional law claim was essentially the same as the federal constitutional claim. This is an important part of the decision for private employers; as discussed below, some state constitutional restrictions extend to private employers.

In its Fourth Amendment analysis, the district court adopted the test laid out in *Ortega*. The court first had to determine whether Quon had a reasonable expectation of privacy in the text messages sent and received from his pager. If so, the court would next have to determine whether the City's search was reasonable at its inception and in its scope.

The court began by affirming *Ortega*'s reasoning that the "operational realities" of the workplace can influence employee expectations of privacy. Had Quon been notified in writing and in person that the City regarded use of the pagers to fall within the gamut of the e-mail policy, and that the use of the pagers would be monitored and possibly audited at any time with regards to any messages sent and received, then, according to the district court, Quon would not have a reasonable expectation of privacy in his text messages. However, the court found that this operational reality was fundamentally altered by the City's informal policy of allowing employees to pay the overage fees themselves in order to avoid being audited. In fact, the court reasoned that the City's informal policy regarding the treatment of overages may actually have *encouraged* employees to use the pagers for personal messages.

As a result, the district court held as a matter of law that, in light of the informal policy giving employees the option to pay overage charges rather than having their messages audited, Quon did indeed have a reasonable expectation of privacy in the text messages sent to and from his pager, despite the City's "Computer Usage, Internet and E-mail Policy" stating to the contrary.

The fact that the City owned and provided the pager to Quon did not alter the court's holding. The court explicitly rejected a *per se* rule that public employees cannot have a reasonable expectation of privacy when using property owned by their employer. Such a rule, the court reasoned, would be at odds with prior Supreme Court precedent holding that expectations of privacy are not always related to property rights because the Fourth Amendment "protects people, not places." In support of its reasoning, the court cited the *Ortega* and *Ziegler* cases.

The court then turned to the issue of whether the City's "search" was reasonable under the circumstances. The court stated that Quon's privacy expectation could only be overcome if the City's review of the messages was reasonable both at its inception and in scope. With respect to the former, the court held that if the police chief's intent in reviewing the messages was to uncover employee misconduct, then the audit would not be reasonable at its inception. Such an audit would be an unreasonable departure from the City's past practice of not auditing pagers unless employees refused to pay overages. Under the City's informal practice, using the pagers to send personal text messages would not be considered "misconduct."

On the other hand, if the reason for obtaining transcripts of the text messages was to determine whether the City should increase the 25,000 character limit for work-related

messages, rather than to uncover employee misconduct, the district court ruled that the audit would be reasonable at its inception.

In assessing the reasonableness of the scope of the audit, the court considered the possibility of less intrusive investigative means. For example, the employer simply could have asked the employees whether some of the overages were for work-related reasons, or reviewed the telephone numbers dialed by the officers. The court found that asking the employees about their overages was insufficient because, in addition to concerns regarding the veracity of their statements, the employees may have an inaccurate recollection of the text messages. Also, reviewing the telephone numbers themselves would not be helpful because they shed no light as to the content of the text messages sent or received. All in all, the court held that there were no less intrusive means feasible for the employer to investigate the use of the pagers.

After finding insufficient evidence to adequately rule on whether the audit was to investigate employee misconduct or to determine the adequacy of the 25,000 monthly character limit, the court held a jury trial on the single issue of the police chief's intent in reviewing the messages. After the jury found that the chief's intent was to determine the efficacy of the character limit, all defendants were absolved of liability in the district court, and the plaintiffs appealed.

2. The *Quon* Ninth Circuit Decision

The Ninth Circuit affirmed in part, reversed in part, and remanded the case for further proceedings. The appellate court first disagreed with the district court's conclusion that Arch Wireless was immune from liability under the SCA. The circuit court also disagreed as to the jury trial's findings pertaining to the reasonableness of the employer audit of the text messages. Finally, the court upheld the finding that the plaintiffs had a reasonable expectation of privacy in their text messages and remanded the case for further proceedings to determine the liability of Arch Wireless under the SCA and the liability of the City under the Fourth Amendment.

In reaching its decision on plaintiffs' privacy claims, the appellate court applied *Ortega's* two-part test: (1) whether the plaintiffs had a reasonable expectation of privacy in their text messages, and (2) if so, whether the City violated their reasonable expectation of privacy by auditing the transcript of Quon's text messages.

Regarding the first test, the appellate court agreed with the district court that the plaintiffs did have a reasonable expectation of privacy in their text messages. In support of its reasoning, the appellate court cited prior decisions recognizing a reasonable expectation of privacy in e-mails and other electronic communications, such as *Katz*, *Smith*, *Forrester*, and *Zeigler*. More specifically, the court held that the *Quon* plaintiffs had a reasonable privacy expectation in the content of the text messages they sent to and received from Jeff Quon. Although they had no reasonable expectation of privacy in the information used to "address" the text messages, they did have a reasonable expectation of privacy in the content of the messages themselves.

With regards to Jeff Quon, the court held that he also had a reasonable expectation of privacy in his text messages. The court found that the City's informal practice of not auditing text messages as long as Quon paid the overages materially altered the formal policy contained in the City's "Computer Usage, Internet, and E-mail Policy." Otherwise, Quon would not have had a reasonable expectation of privacy. Therefore, the "operational reality" of the workplace rendered Quon's expectation of privacy in his text messages reasonable.

After finding that the plaintiffs all had a reasonable expectation of privacy in the content of their text messages, the appellate court next had to determine whether the audit conducted by the City was reasonable at its inception and in its scope. The search was determined to be reasonable at its inception because a jury had already found that the City's purpose for performing the audit was to determine the efficacy of the 25,000 monthly character limit, and not to uncover wrongdoing.

The appellate court then analyzed *de novo* whether the search was unreasonable in its scope. The court concluded that the scope itself was unreasonable, primarily because there were less intrusive means of conducting an audit. For example, the City could have first warned Quon that he was forbidden from using his pager for personal communication for a month, and that all his text messages would be audited at the end of the month. Alternatively, if the City wanted to review past usage, it could have given Quon the opportunity to redact from the transcript any messages that were personal in nature. Given the fact that there were less intrusive means of reviewing the text message transcript, the appellate court found the City's search to be unreasonable.

After stating its holdings, the appellate court remanded the case back to the district court for a determination of Arch Wireless' and the City's liability towards the plaintiffs.

V. How *Quon* Affects Employee Rights in the Private Sector

The *Quon* case illustrates how laws regarding employee privacy in the workplace are constantly in flux, especially with the advent of new technologies like text messaging. While the case's outcome may seem to favor employees, the decision itself is narrow in its scope. The court's decision turned on the fact that the employer's informal practice regarding the use of company-issued two-way pagers created a reasonable expectation of privacy in employee text messages. Had the City been more diligent in enforcing its right to audit messages sent using the pagers from the outset, the case would likely have had a different outcome.

Equally important is the fact that the appellate court did not disturb an employer's right to "contract away" an employee's reasonable expectation of privacy via agreements such as electronics usage policies; it only emphasized the need for employers to actually enforce and abide by these agreements, as opposed to installing contradictory informal policies in their stead.

Several aspects of the *Quon* decision may eventually reach private employers. For example, while the plaintiffs in *Quon* brought suit under both the Fourth Amendment and Article I, Section 1 of the California Constitution, this latter constitutional provision applies to both public and private entities.[11] Courts also are likely to apply the policy waiver analysis from *Quon* in future private employer cases. For these reasons alone, private employers should confirm that their practices and policies are consistent.

VI. Recommendations

The *Quon* case highlights the importance of encompassing new communication channels like text-messaging in well-written employer policies on electronic communications. Effective policies should be drafted to apply to communications generally so that they encompass evolving methods of communications, without the need for constant updating. To the extent employers want to retain their ability to monitor their employees' use of employer electronic communications, employers should clearly and prominently disclose this monitoring in a general communications policy. Employers also should require employees to affirmatively consent to such general policies in order confirm that the written policy is in force.

To be clear, a specific lesson from the *Quon* appellate court decision is that employers also should make sure that their employees understand and acknowledge any limitations on their privacy rights with regard to communications sent via company equipment or property. The acknowledgement would be accomplished through the affirmative consent from the employee, but the employer should be equally as confident that the scope of limitations are clearly and prominently disclosed to employees. Employers should take care to not allow informal policies and practices to trump written policies and codes of conduct.

In the wake of this ruling, employers should take care to:

- Ensure that the organization has an up-to-date policy covering all methods of communication generally, to avoid having to update the policy each time new technologies are introduced;
- Give employees clear notice of the company's right to audit, inspect, or otherwise monitor electronic communications, and clearly and prominently explain the methods by which such monitoring may be carried out;
- Require employees to affirmatively consent to any company policies with regard to monitoring or auditing activities;
- Train supervisors and employees to ensure compliance with the policy; and
- Consult with experienced in-house or outside counsel before reviewing the contents of an employee's text message or any other form of communication made using company-owned equipment.

The authors thank summer associate Teddie Hsu for his assistance in the drafting of this article.

MARY ELLEN CALLAHAN, Partner, Hogan & Hartson LLP, practices in the areas of privacy, data security, and consumer protection. Mary Ellen has extensive experience working with multinational companies on a variety of privacy and security issues, including companies' policies (terms and conditions, privacy policies, and security policies) and wide-scale audits of clients' privacy and security policies as they relate to relevant federal and state legislation.

This article originally appeared in ***The Privacy Tracker,*** a publication of the International Association of Privacy Professions (IAPP). If you are interested in joining the IAPP and subscribing to ***The Privacy Tracker***, please visit www.privacytracker.org. Used with permission.

[11] *Hill v. Nat'l Collegiate Ath. Ass'n,* 865 P.2d 633 (Cal. 1994), ("[t]he 'privacy' protected by [Article I, Section 1 of the California Constitution] is no broader in the area of search and seizure than the 'privacy' protected by the Fourth Amendment….").