



City of Ontario v. Quon: The U.S. Supreme Court Weighs in on Employee Privacy Issues

By Don Phin, Esq.

This is an article about a case I have been following through the courts for quite a while: *City of Ontario v. Quon* (see www.supremecourt.gov/opinions/09pdf/08-1332.pdf). For the first time, the U.S. Supreme Court was confronted with the all-important question of workplace privacy rights in the context of today's electronic communications. Regrettably, the Court failed to address the issue directly. Rather than unequivocally stating that employees do or do not have a right to privacy in such matters, it instead examined the narrower question of whether, given the specific circumstances of the case, the employer had reasonable grounds in conducting a search of the employee's text messages, the act that produced the lawsuit.

But despite its inability to squarely examine this central question in its written opinion, the Court did provide a number of useful guidelines for delineating the boundary between what, on one hand, constitutes an employer's unlawful violation of an employee's privacy rights and, on the other hand, what information an employer must legitimately have about an employee's workplace activities to operate its business successfully.

The Circumstances That Gave Rise to the Lawsuit

Jeff Quon was hired as a SWAT officer by the City of Ontario in California. At the time of his hire, he received a “Computer Usage, Internet

and E-Mail Policy” (Computer Policy) that applied to all employees. Among other provisions, it specified that 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.” In March 2000, Mr. Quon signed a statement acknowledging that he had read and understood the Computer Policy.

In October 2001, the City acquired 20 alphanumeric pagers capable of sending and receiving text messages. Arch Wireless Operating Company provided wireless service for the pagers. Under the City's service contract with Arch Wireless, each pager was allotted a limited number of characters sent or received each month. Usage in excess of that amount would result in an additional fee. The City issued pagers to Mr. Quon and to other SWAT team members, in order to help the SWAT team mobilize and respond to emergency situations.

Importantly, the Computer Policy did not, on its face, apply to text messaging. Text messages share similarities with e-mails, but the two differ in one significant way. In this case, for instance, an e-mail sent on a City of Ontario computer was transmitted through the City's own data servers. In contrast, a text message sent on one of the City's pagers was transmitted using wireless radio frequencies from an individual pager to a receiving station owned by Arch Wireless.

Although the Computer Policy did not cover text messages by its explicit terms, the City made it clear to employees, including Mr. Quon, that the City would treat text messages the same way as it treated e-mails. Officers were told that messages sent on the pagers “are considered e-mail messages. This means that [text] messages would fall under the City’s policy as public information and [would be] eligible for auditing.” This policy was eventually put in writing in a memorandum sent to Mr. Quon and other City personnel, but such personnel were never required to acknowledge it in writing.

Mr. Quon exceeded his allotted limits for several months in a row. As a result, the officer in charge of assessing costs for overage minutes “grew tired of being a bill collector.” When the officer in charge complained to his superior about having to collect monies in this way, the officer was asked if the message limit was set too low. It was then agreed to audit the records of Mr. Quon and another officer to see if a different limit should be set. Mr. Quon made but lost the argument at trial that the real purpose of the arrangement was to “nose” into his personal business rather than to assess the adequacy of monthly overage limits.

The officer in charge of the audit was told to redact any messages that were sent outside of work hours.

When the officer reviewed the text transcripts, lo and behold, he discovered that the vast majority of the personal messages on Mr. Quon’s phone, a number of which were sexually explicit, were sent during the regular work day. Many were to/from a coworker with whom he was having an affair, during a separation from his wife. (Whoops!) According to the report, Mr. Quon received 456 messages during work hours in the month of August 2002, of which no more than 57 were work-related. He sent as many as 80 messages during a single day at work, and on an average workday, Mr. Quon sent or received 28 messages of which *only* 3 involved police business. As a consequence of this discovery, it was determined that Mr. Quon had violated the employer’s rules and he was allegedly disciplined. (Let’s hope so!)

The Lawsuit

Apparently, Mr. Quon was so offended by having his misdeeds brought to light that he filed suit against both Arch Wireless and the City of Ontario. His lawsuit alleged that (a) Arch wrongfully provided the department with his text transcripts without a subpoena under the Stored Communications Act, and (b) that the City of Ontario had violated his privacy rights by reading the contents of the text messages. At the Ninth Circuit Court of Appeals level, he prevailed on his SCA case against Arch (which was not reviewed by the U.S. Supreme Court), and the outcome now stands as law in the Ninth Circuit. The only matter decided by the Supreme Court was related to his privacy claim against his employer, the City of Ontario.

The Supreme Court’s Ruling

Much of the majority’s decision centered on how to formulate a “bright-line” legal approach that would effectively analyze, and ultimately determine the appropriate result in, future privacy violation cases. Indeed, it was readily apparent in reading the case that the Court members grappled with creating a unified definition of what, exactly, constituted a privacy violation, compared to what did not. But despite such efforts, the Court stopped short of issuing specific rules delineating the privacy right boundaries as respects workplace electronic communications. And, as concurring Justice Scalia wrote, “The majority court spent a great deal of time agonizing over how to approach privacy claims generated in the context of today’s new technologies *without* providing any firm legal guidelines (emphasis added).”

Instead, the Court “punted” and simply jumped to the conclusion that in this situation it was reasonable to search the officer’s text messages—regardless of whether he had a right to privacy in the first place. Thus, by an 8–1 majority, it ruled that the City of Ontario had a valid justification for searching the officer’s text messages and, given this rightful exercise, whatever inappropriate conduct the search revealed—even if uncovering such conduct was

not the goal of the investigation—was fair game for the investigation to reveal.

Nevertheless, the majority decision did provide a bunch of valuable information within the dicta portion of its decision. (“Dicta” refers to commentary in a court’s written decision or opinion that is offered for explanatory purposes yet is not binding in future cases.)

What Employers/Risk Managers Need To Know about the Ruling

Here is what employers and the risk management community must learn from this decision.

Privacy Violations Remain a Case-by-Case Issue

The question of whether an employee has a reasonable expectation of privacy and whether that privacy was, in fact, violated will continue to be examined on a case-by-case basis. As with most employment cases (think: disability, sexual harassment, etc.), there are numerous *guidelines* but as was also true in this case, the Court provided no hard-and-fast *rules*. Justice Scalia did, however, cut right to the chase regarding public employers when he said that any search is regarded as reasonable and normal if allowable in the private-employer context. He simply noted that in both the private or public context, this search should not violate the Fourth Amendment against “unreasonable” searches and seizures.

Operational Realities Are Critical

So instead of hard-and-fast rules, the majority of the Court preferred to use a murky “operational realities” test in evaluating the appropriateness of an intrusion. They reminded us that the intrusion has to be reasonable but not necessarily the “most reasonable” way of doing things. This helps prevent “second-guessing” of management decisions (a theme consistent with the Court’s recent discrimination rulings related to the hiring of firemen; i.e., *Ricci v. DeStefano* and *Lewis v. City of Chicago*).

Put the Policy in Writing and Have It Acknowledged by the Employee

The Court made it clear that its decision would have been easier had Mr. Quon been explicitly told that he had no right to privacy in his text messages and that they might be reviewed in a manner similar to his e-mail. Of course, it would have helped to have had a signed copy of a policy acknowledging this assertion. (According to the facts, Mr. Quon *was* told just that; which seems to contradict the Court’s assertion here.) Unfortunately, his superior also told him not to worry about an audit, as long as Mr. Quon was willing to pay any overage charges.

Clearly Notify Employees of the Employer’s Right To Monitor Electronic Communications

The Court noted that various states have begun passing statutes requiring employers to notify employees when their electronic communications are being monitored. The fact is employment lawyers like me have been recommending that employers do exactly this for the last decade.

Employers Must Decide *Exactly* How To Handle Personal Communications

Many employers provide employees with cell phones, pagers, and other communication devices, explicitly instructing the employees not to use them for any reason other than business purposes. In such instances, employers should simply arrange to have the devices turned off from 5 p.m. until 8 a.m. Or, they should instruct employees to do so.

But on the other hand, for customer service purposes, some employers like it when employees are “tethered” to their cell phones and other communication devices. For the sake of enhanced customer service, these employers have determined that they can “live with” having employees use the equipment for personal, as well as for business, purposes.

Interestingly, many of the billing concerns that drive this division between the “tight” (first paragraph, above) and “loose” (preceding paragraph) personal usage policies are quickly disappearing from the landscape. This is especially true, now that unlimited use plans are routinely being provided by carriers. Accordingly, the only question becomes: how much of the worker’s day is being taken up by personal communication activities? One benefit of allowing limited personal use of company devices is that it affords an employer the ability to determine precisely how much of each employee’s day is being consumed in this manner. Conversely, if employees use their own cell phones, pagers, or computers, the employer has no way of tracking such information.

Yet another employer perspective on this matter comes from those who instruct their workers: “If you’re going to do any personal communication, do it on your own cell phone or computer.” Given the extent to which pricing has come down in recent years, nowadays, nobody really needs to use the office computer or cell phone to communicate with their friends/family, or visit porn/gambling sites. They can simply use their own.

Distinctions as to the Purpose of a Search

The Court reminded us that there is a distinction between, on one hand, breaches of privacy done for “non-investigatory work-related purposes” (such as determining a reasonable usage limit) and “investigation of work-related misconduct,” on the other. In either case, a government employer’s warrantless search (and you may be able to simply say that *any* employer’s search) is reasonable if it is “justified at its inception” and if “the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of” the circumstances giving rise to the search.

Employer Efforts To Lessen the Intrusiveness of an Investigation

The Court stated that the City had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets

for work-related expenses; or, on the other hand, that the City was not paying for extensive personal communications. It made a point of noting that during the investigation, the City redacted all messages sent while off-duty—a measure that reduced the intrusiveness of the investigation. Again, the Court provided guidelines—but not rules, once more emphasizing the case-by-case/operational realities of the privacy issue.

Reasonableness of Employee Privacy Expectations

The Court noted that it would not have been reasonable for Mr. Quon to conclude his messages were, in all circumstances, immune from scrutiny. This is especially true, in light of the fact that he was a SWAT officer! On the other hand, a more important question is whether this justification can be extended to, for example, a teacher, a day care employee, a nurse, or even a clerk.

Are the Justices of the U.S. Supreme Court That Disconnected from Today’s Reality?

The following quote from the Court would be amusing if it wasn’t so wrong: “That the search did reveal intimate details of Mr. Quon’s life does not make it unreasonable, for under the circumstances *a reasonable employer would not expect that such a review would intrude on such matters.*” (My emphasis.) Just how disconnected from the realities of daily life in 2010 are these justices? In my mind, an employer would be unreasonable to think that people *don’t use* electronic communication devices for personal reasons, as did Mr. Quon. Of course, they would certainly hope an employee didn’t use them as often as Mr. Quon did. But to be *surprised* that someone sends salacious e-mails or texts shows a certain degree of detachment from real life. In fact, I have seen a number of sources cite the statistic that the vast majority of pornography usage occurs between 9 a.m. and 5 p.m.!

And if you closely analyze the subtext of the Court’s opinion, what it really grappled with but couldn’t bring itself to state directly was this: “Hey, you’re a SWAT officer. Who are you kidding? You’re spending excessive amounts of on-the-job time sending these ridiculous sex-based

texts while you're supposed to be out there protecting people. Don't whine about the fact that you got found out!"

Lastly, if you want to amuse yourself, read Justice Scalia's concurring opinion. Not only does he use words like "agnostic" and "expatriation," he takes a parting shot at the minority's paranoia and reluctance to create clear guidelines when it comes to privacy and electronic technology.

My Own Take on the Case

I believe the decision was a correct one. The Ninth Circuit, in its ruling, basically said that the City did not have to read the content of Mr. Quon's personal e-mails to meet its objective of assessing the extent to which he was generating overage charges by text messaging. But who really knows if that is, in fact, true? The fact that the jury believed the City was reading it to find out if its monthly text message limits were too low was all the Court needed to make this case a simple one to decide. Maybe

it's just the skeptic in me, but I have to believe that, at some level, the City expected there was misuse of the program and it was, in part, curious as to the exact nature of that misuse.

Conjecture aside, in the end, the safe route for an employer is as follows.

- ◆ Have a clearly communicated policy that unequivocally puts to rest any notions that employees have a right to privacy when using company-provided equipment.
- ◆ Obtain a signed acknowledgment of that policy.
- ◆ Realize that the boundaries between people's work and personal lives have all but vanished and that if you're going to give employees electronic equipment, be crystal clear about the exact extent to which they can use it for personal matters—if at all.
- ◆ If you are going to monitor employees, do it in the least intrusive manner possible.

If you would like a copy of a sample privacy policy, send me an e-mail at don@hrthatworks.com.

EPLiC

Donald A. Phin, Esq., has been an employment law attorney since 1983. He developed the HRThatWorks.com program used by agencies and their clients nationwide. Mr. Phin is a highly rated speaker and author of Building Powerful Employment Relationships; LAWSUIT FREE! How to Prevent Employee Lawsuits; and Victims, Villains and Heroes: Managing Emotions in the Workplace. His articles have appeared in The Risk Report, Business Insurance, CFG Update, HR.com, EPLiC, and other industry publications. He can be reached at (800) 234-3304 or by e-mail at don@hrthatworks.com.