SOCIAL NETWORKING AND THE PUBLIC EMPLOYEE: THE FIRST AND FOURTH AMENDMENTS MEET FACEBOOK

Presenter
PAMELA HUTSON JOHNSON
Assistant City Attorney
City of Arlington, Texas

Author
MELINDA H. BARLOW
Assistant City Attorney
City of Arlington, Texas

State Bar of Texas
23rd ANNUAL
ADVANCED SUING AND DEFENDING GOVERNMENTAL ENTITIES COURSE
July 21-22, 2011
Austin

CHAPTER 8

PAMELA HUTSON JOHNSON is employed with the City of Arlington as an Assistant City Attorney and engaged in the practice of municipal law, focusing on counseling and litigation of employment law as well as open records litigation. She is also experienced in providing counsel to investigators during Police and Fire internal affairs investigations and advises on employee disciplines. She has represented the city in numerous employee Arbitrations and currently serves as legal counsel for management during the city's Meet and Confer Sessions with both Police and Fire Employee Associations.

Mrs. Johnson is originally from Midland Texas and received her B.A. from The University of Texas at Dallas and her J.D. from Southern Methodist University. She is a member of the College of the State Bar of Texas and is licensed and admitted to practice in Texas, Northern District of Texas, the Fifth Circuit Court of Appeals and the U.S. Supreme Court. She has lectured numerous times on EEOC and the Law, Discipline Done Right, Workplace Harassment, and ethical issues in local government employment representation.

Her other activities have included serving as an Adjunct Instructor for Everest University, University of Phoenix, and University of North Texas Professional Development Institute where she developed and/or instructed paralegal and general courses on Legal Ethics & Professional Responsibility, Real Estate Law, Criminal Law, Business Organizations, Criminal Procedure and Business Writing. Her prior legal experience with the City of Arlington also includes serving as the Assistant Police Legal Advisor and as a Municipal Prosecutor. While working as a Staff Attorney in Housing and Consumer Protection with Legal Services of North West Texas, she also hosted a weekly radio talk show on legal topics of interest to the community.

TABLE OF CONTENTS

I. INTRODUCTION 1

II. FIRST AMENDMENT SPEECH REGULATION BY PUBLIC EMPLOYERS 2
A. First Amendment Tests as Applied to Social Networking 3

III. FOURTH AMENDMENT CONSIDERATIONS FOR PUBLIC EMPLOYERS 4
A. Stored Communications Act 5
B. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir.), *reversed* No. 08-1332, 2010 U.S. LEXIS 4972 (June 17, 2010) 5

IV. WHAT SHOULD OUR POLICY SAY ANYWAY? 6

SOCIAL NETWORKING AND THE PUBLIC EMPLOYEE: THE FIRST AND FOURTH AMENDMENTS MEET FACEBOOK

I. INTRODUCTION

In today's legal environment, the most certain thing that can be said about law and technology is that technology is progressing faster than the common law, statutes and many personnel policies designed to address them. In particular, the explosion of social networking and PDAs into the general population has created whole new issues regarding forums, speech, and privacy, both in and outside the workplace. As technology and ease of access grows, employers are finding that the same technology designed to increase opportunities for communication can also have a negative effect on employee productivity and increase the risk of liability related to harassment and invasion of privacy claims. "The *New York Times* reported recently that even commanders in our Armed Forces have expressed concern about troops playing with iPhones and BlackBerrys when they should be working. Because the law has not caught up with the use of social media, navigating through issues raised by this technology can be a difficult, complicated and frustrating process for employers." Pilar Morin, *10 Things Employers And Employees Should Know About Social Media* (March 7, 2011) http://www.calpublicagencylaboremploymentblog.com/privacy/10-things-employers-and-employees-should-know-about-social-media/ (last visited June 3, 2011) The cyber world opens a Pandora's Box of privacy and search issues never addressed by the Supreme Court while governmental entities, like private industry, propel forward utilizing these e-tools to not only market programs and their organization but to create forums of discussion and connections with citizens and stakeholders. The implications of all this activity will not likely be realized for some time. However, governmental entities acting as employers must get ahead of the potential negative fallouts by educating employees and preparing legally defensible policies to avoid risk and liability in an unclear new frontier. One study identifies three distinct ways that government employees are using social media tools while at work. Generally, employees use social media for official agency interests, professional interests, and personal interests. Jana Hrdinová, Natalie Helbig & Catherine Stollar Peters, *Social Media Policy for Government: Eight Essential Elements* (May 12, 2010), http://www.ctg.albany.edu/publications/guides/social_media_policy (last visited June 16, 2010). The problem, as employers, is that the lines between professional/official use and personal use are increasingly fluid and blurred. Thus, striking a balance among such uses while taking into consideration security, legal, and managerial implications, becomes uncharted territory for many organizations.

As government employers, we are particularly concerned with controlling and maintaining discipline within the workplace while being mindful of violating state or federal constitutional rights. Many of the questions that arise when reviewing an employee's e-mails, text communications or social networking activities simply do not have definitive answers and will not likely have definitive answers for some time as the natural progression and resolution of these issues through the court system tends to be slow. The U.S. Supreme Court's decision in *City of Ontario v. Quon* provides the first glimpse of insight into management of the cyber world as a government employer. No. 08-1332, 2010 U.S. LEXIS 4972 (June 17, 2010). The case was heard in April 2010 and Justices struggled with some of the very thorny issues discussed herein, such as whether it is reasonable for a government employee to expect his text communications are private and, even stickier, whether it is reasonable for someone communicating with a government employee to expect their text communications are private? However, those two issues were specifically left undecided. Recognizing the new frontier, the Supreme Court rationalizes its decision to skirt the issue by stating:

> "The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on Fourth Amendment implications of emerging technology before its role in society has become clear." Id. at *10.

Thus, the Supreme Court in its first decision with opportunity to addresses privacy in the new cyber world recognized the far-reaching significance of the issue but concluded the matter before them should be decided upon settled principles regarding when a search is reasonable. *Id.* at *1.

Unfortunately, awaiting further direction from the high courts is not an option for public employers as these issues are arising daily and demand attention now. As such, this paper focuses on the existing case law and how it may be reasonably extrapolated to apply to cyber situations for government employers with regard to government employees' communications. The issues that arise most

commonly with regard to an employee's conduct or speech via a social technical medium are 1) whether the employer's restriction or reaction is a violation of the employee's First Amendment rights to free speech and 2) whether the employer's review of certain employee speech is an unwarranted search pursuant to the Fourth Amendment. Additionally, this paper makes recommendations regarding implementing personnel policies that address government employees' expectations and hopefully provides government employers a layer of defense when examining employees' cyber activities that violate policy.

II. FIRST AMENDMENT SPEECH REGULATION BY PUBLIC EMPLOYERS

Can an employee face an adverse employment action based on language posted on a social networking site? The answer, of course, is it depends. If an employment action is taken against an employee based on speech, it is possible the employee may file a Section 1983 suit against the employer claiming infringement of the right to free speech under the First Amendment. However, case law addressing public employer infringement of speech is nuanced and when social networking is added to the equation the issue becomes even more abstract.

Governmental employers may place more restraints on employee speech than is placed on the general public. *City of San Diego v. Roe,* 543 U.S. 77, 80 (2004). The Supreme Court summarized the precedent for free speech protection of government employees as follows:

> "To prevail, an employee must prove that the conduct at issue was constitutionally protected, and that it was a substantial or motivating factor in the termination. If the employee discharges that burden, the government can escape liability by showing that it would have taken the same action even in the absence of the protected conduct. And even termination because of protected speech may be justified when legitimate countervailing government interests are sufficiently strong. Government employees' First Amendment rights depend on the 'balance between the interests of the [employee], as a citizen, in commenting upon matters of public concern and the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees.' In striking that balance, we have concluded that '[t]he government's interest in achieving its goals as effectively and efficiently as possible is elevated from a relatively subordinate interest when it acts as sovereign to a significant one when it acts as employer.' We have, therefore, 'consistently given greater deference to government predictions of harm used to justify restriction of employee speech than to predictions of harm used to justify restrictions on the speech of the public at large.' " *Citing Bd. of County Comm'rs v. Umbehr,* 518 U.S. 668, 675-76 (1996).

Back when rotary phones were still the norm, the Supreme Court established the two-prong *Pickering* test to evaluate the protection afforded to speech by public employees. The first prong requires a determination of whether the employee spoke as a citizen on a matter of public concern. *Pickering v. Bd. of Educ.,* 391 U.S. 563, 568 (1968). If the employee did not speak as a citizen on a matter of public concern, then the evaluation ends, for the employee has no claim of First Amendment infringement. *Connick v. Myers,* 461 U.S. 138, 147 (1983). The Constitution will not shield employee comments from employer discipline. *Garcetti v. Ceballos,* 547 U.S. 410, 421 (2006). If the employee was speaking on a matter of public concern, there is a possible First Amendment claim. The content, form, and context of the speech must be analyzed when determining if it is a matter of public concern. *Connick,* 461 U.S. at 147-48.

There is no bright line rule as to what the judicial system considers a matter of public concern. Courts have held that statements criticizing public policy, such as the statement, "if they go for him again, I hope they get him," referring to an assassination attempt on the President, constitutes a matter of public concern because it encouraged public discourse and debate. *Rankin v. McPherson,* 483 U.S. 378, 387 (1987), *citing New York Times Co. v. Sullivan,* 376 U.S. 254, 270 (1964). Additionally, it has been held that a teacher publicly criticizing a school board and its funding of the school district is protected as a matter of public concern because it was directed at the public more than at any close coworker of the employee's, did not impede the daily functioning of the school, and involved a matter of public debate. *Pickering,* 391 U.S. at 569. Also, the Court holds that speech regarding racial discrimination is inherently a matter of public concern. *Givhan v. W. Line Consol. Sch. Dist.,* 439 U.S. 410 (1979).

The Supreme Court found an employee's speech was not a matter of public concern in *Connick.* In that case, an assistant district attorney ("ADA") who was about to be transferred to a different area of the court wrote a pamphlet for distribution among the other

ADAs regarding topics such as the office transfer policy, office morale, and the need for a grievance committee. *Id.* at 140-41. The District Attorney, upon learning of the pamphlet, felt the pamphlet caused a "mini insurrection" and terminated the employee construing her actions as declining the transfer. *Id.* The Court held the pamphlet's generally narrow focus and specific audience (the other district attorneys) demonstrated that the speech contained within was not a matter of public concern. *Id.* at 148.

In *Garcetti*, deputy district attorney Ceballos testified on behalf of the defense at a motion's hearing involving a warrant affidavit he believed to be defective after he informed his superior of his opinion but was told the case would proceed. 547 U.S. at 414. After the court rejected the challenge to the warrant, Ceballos claimed he was subjected to retaliatory employment actions based on his involvement with the warrant affidavit. *Id.* at 415. The Court held Ceballos's statements were made pursuant to his prosecutorial duties. *Id.* at 421. "The fact that his duties sometimes required him to speak or write," the Court held, "does not mean his supervisors were prohibited from evaluating his performance." *Id.* at 422.

If analysis under the first prong of the *Pickering* test deems the speech a matter of public concern, then the speech must be evaluated under the second prong. The second prong questions whether the employer had appropriate justification for treating the employee differently from any other member of the general public. *Pickering*, 391 U.S. at 568. The test balances the interests of the employee in commenting upon matters of public concern and the employer in promoting the efficiency of the public services it performs through its employees. *Id.* If the scale tips in favor of the employee's free speech, then the employee has a possible First Amendment claim based on the employment action. If the scale tips in favor of the employer's interest, then a First Amendment claim is less likely to prevail. Examples of appropriate considerations for an employer include whether the statement impairs discipline by superiors or undermines relations with the community. *See Weicherding v. Riegel*, 160 F.3d 1139, 1143 (7th Cir. 1998). Further, the employer may avoid liability even if the speech is protected if it can demonstrate by a preponderance of the evidence that the disciplinary action would have been taken even if the employee had not engaged in the speech. *Mt. Healthy City Sch. Dist. Bd. of Educ. v. Doyle*, 429 U.S. 274, 287 (1977). This defense is really premised on the notion that it wasn't the speech at all but rather the employee attempting to shield itself through the First Amendment.

A. First Amendment Tests as Applied to Social Networking

The Supreme Court has not heard any cases involving social networking and a public employee discipline. However, when a case is finally heard, the *Pickering* test is sure to be applied presenting some interpretative challenges. What comments from an employee constitute matters of public concern? Surely comments about racial discrimination, comments related to political issues, and comments that might constitute whistleblower actions. Conversely, comments that relate directly to the employee may be considered matters not of public concern, like "I hate my job," "My boss is lazy," etc.

Further, the issue of whether social network forums are private or public should reasonably bear upon whether the speech is a matter of public concern. Forums like Facebook allow users to limit their audiences to a degree by adjusting privacy settings. Chatrooms may also be restricted so that only certain members may enter the room. An expression to a limited audience arguably bears weight on whether the information is a matter of public concern. However, the scope of the audience, as in *Connick*, is clearly a factor but may not be dispositive. Matters of public concern may still be discussed among a small group. Additionally, even though a Facebook user may have privacy settings, many users have 500 plus "friends." Under that scenario, is the message really intended to reach only a small, private audience?

The *Garcetti* case adds an interesting dimension to the analysis. When is a comment posted done in a manner that is pursuant to an employee's job duties? A prosecutor commenting on a MySpace page regarding the status of his ongoing criminal trial may be an example of speech that is not a matter of public concern; however, it is also likely an ethical violation for the attorney. What about the police officer that makes a post on Facebook on his personal PDA while on duty regarding an ongoing incident? The incident may be a matter of public concern but is it a reasonable extension of his job duties to capture it on Facebook?

If speech is deemed to be a matter of public concern, the second prong of the *Pickering* test must be considered. Employers will have to argue persuasively that the content of the speech is outweighed by a need to efficiently provide public services. If a post disrupts the workplace, even if it was composed on the employee's free time or outside of the office, the court may find for the offended employer. Finally, employers who act pursuant to specific policies regarding use of PDAs and social networking sites while "on the clock" have a strong

argument that efficient operations is the impetus for the restrictions rather than suppression of speech.

III. FOURTH AMENDMENT CONSIDERATIONS FOR PUBLIC EMPLOYERS

Social media will surely present unique issues of workplace privacy and thus courts will likely hear Section 1983 claims stemming from Fourth Amendment arguments against unreasonable searches and seizures by government employers associated with information from social networking sites. The Court has already held that searches by government employers of their employees offices are subject to the Fourth Amendment. *O'Connor v. Ortega*, 480 U.S. 709, 721 (1987). But, it remains unclear how far Fourth Amendment protections extend into the cyber-world.

Pursuant to *O'Connor,* and as recently reiterated by *City of Ontario,* the Supreme Court has fashioned a two prong analysis for Fourth Amendment claims in the government employer context. *O'Connor,* 480 U.S. at 718-26; *City of Ontario*. First, is the determination whether the employee has a reasonable expectation of privacy? If no, then the courts must analyze on a case by case basis whether an employee's Fourth Amendment rights are implicated. If yes, then the employer's intrusion for non-investigatory, work-related purposes, as well as investigation of work-related misconduct is judged based upon the reasonableness under the circumstances. In the concurrence of *O'Connor*, Scalia advocated that government searches to retrieve work-related materials or to investigate violations of workplace rules if considered reasonable and normal in the private employer context would not violate the Fourth Amendment in the public employer context. *O'Connor,* 480 U.S. at 732. The Supreme Court in *City of Ontario* determines that under its facts, even if the employee had a reasonable expectation of privacy, a violation of his Fourth Amendment rights did not occur under either *O'Connor* approach. *City of Ontario,* 2010 U.S. LEXIS 4972, at *9.

When reviewing a search, the reasonableness of a search is determined by assessing the degree to which it intrudes on the individual's privacy and also the degree to which it is needed to promote a legitimate governmental interest. *United States v. Knights,* 534 U.S. 112, 118-19 (2001). Naturally, government employees do not lose their expectation of privacy because they work for the government. *O'Connor,* 480 U.S. at 717. However, the Court in *O'Connor* held that because of the great variety of work environments in the public sector, the question of privacy must be addressed on a case-by-case basis. *Id.* at 718.

When does an employee have a reasonable expectation of privacy in regards to a social networking site? Suppression of evidence under the Fourth Amendment requires the showing that the defendant had a legitimate expectation of privacy in the place searched or item seized, and the subjective expectation of privacy was objectively reasonable. *Rakas v. Illinois,* 439 U.S. 128, 143 (1978). When information is posted to a public forum such as Facebook (with no privacy settings enabled), there is likely no expectation of privacy. What a person exposes to the public is not protected by the Fourth Amendment. *Katz v. United States,* 389 U.S. 347, 351 (1967). Additionally, an employer policy may outline when an employee should have an expectation of privacy or not. *See United States v. Simmons,* 206 F.3d 392 (4th Cir. 2000) (denying an employee's motion to suppress files accessed by his employer on his computer when employee had been provided warnings that data stored on company computers was not private). If an employee is notified in the policy handbook that all internet access is monitored at work, they should have no expectation of privacy in the content of the information they post while at work. Other factors courts might consider when determining if an employee has a reasonable expectation of privacy in IT systems at work:

- Does the employer ban personal/objectionable use of computer equipment?
- Does the employer monitor the use of the equipment?
- Do third parties have a right of access to the information under open records laws?
- Was the employee aware of the open records law applicability and the employer's policies related to computer use and monitoring?

However, the use of electronic equipment outside of the governmental entity's IT system such as personal smart phones, cell phones, Ipads, etc., makes it more difficult to formulate constitutionally sound policies that address such "private" usage. Because of the proliferation of personal devices such as the Iphone, employees may, while at work, engage in many computer activities outside of city systems. Some employers may also draft policies making employees aware that social networking sites may be reviewed for content, putting the employee on notice that those sites may be subject to search by the employer. However, if social network sites have privacy settings

which are activated by the employee, does the employee have a legitimate expectation of privacy?

Courts typically have not found a reasonable expectation of privacy in communications on websites, email, or chatrooms since the individual is posting material on the internet and generally takes no steps to limit access or otherwise protect the communication. However, large sites such as Facebook have privacy settings so information posted on such a website is not transmitted to the general public; rather, it is typically published to the group of "friends" a user has on the account (those with access to view the profile). This muddies the waters even more as to how much of an expectation of privacy exists with a social networking site that has privacy safeguards.

The Court has held, by plurality, that government employers may conduct warrantless searches of employees where the employer's search is to further the investigation of workplace misconduct, not criminality; when there are reasonable grounds to suspect evidence of the misconduct will be located; and the scope of the search is reasonably related to its objectives and not overly intrusively. *O'Connor,* 480 U.S. at 719-23. The same principle could be applied to employers searching social networking sites, as they do already in many hiring instances, but under the same guidelines as outlined in *O'Connor*. An employer must decide under what circumstances social networking content will be searched, and what information constitutes reasonable grounds for a search. The employer must also decide if it will conduct the search or hire out the task. It is not advisable to create a "dummy profile" in an attempt to access a social networking site and collect information through deception.

A. Stored Communications Act

Employers must also consider statutory privacy protections, such as the Stored Communications Act ("SCA"), 18 U.S.C.A. §§ 2701-2708. Section 2701 of the SCA creates a criminal offense for whomever "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility," and by doing so "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C.A. § 2701(a)(1-2). Further, a private cause of action for "any…other person aggrieved" by a violation of the SCA allows a district court to award equitable or declaratory relief, reasonable attorney's fees and other costs, and damages. 18 U.S.C.A. § 2707(a)-(c). Punitive damages are available if the violation is willful or intentional. 18 U.S.C.A. § 2707(c).

Importantly, in the *Quon v. Arch Wireless Operating Co., Inc.* case, the Ninth Circuit reversed the district court's summary judgment in favor of Arch Wireless (the pager provider for the City of Ontario) and held that the company violated the SCA for turning over the transcripts of the text messages from its pagers to the City. 529 F. 3d 892, 909 (2008). Additionally, the Supreme Court denied Arch Wireless' petition for certiorari. *USA Mobility Wireless, Inc. v. Quon*, 2009 U.S. LEXIS 9132 (2009). Thus, even though the City was the customer and paid for the pagers, it appears that providing the transcripts of the texts to the organization may have been a violation of the SCA. In other words, good luck cities on obtaining such information from cell phone and pager providers in the future.

Types of electronic communications that courts have found are covered by the SCA include e-mail accounts, text messages, and social networking pages. *See Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009); *Pietrylo v. Hillstone Rest. Group d/b/a Houston's,* 2009 U.S. Dist. LEXIS 88702 (Sept. 25, 2009) (unpublished); *Quon*. The SCA does allow a person to authorize access to electronic communications if the person is the user of the service and the communication in question is from or is intended for the user. 18 U.S.C.A. § 2701(c). So, while this implies the employee could allow the employer to view their social networking posts with their permission, this exception should not be abused and an employer should be mindful that the permission should be voluntary.

B. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir.), *reversed* No. 08-1332, 2010 U.S. LEXIS 4972 (June 17, 2010)

The *Quon* case held such promise as to how the Supreme Court would address privacy expectations in this new technical world thus warranting its own discussion section. Sadly, the Supreme Court dodged the issue for another day leaving practitioners to tackle meatier issues on their own for a while longer. However, the *Quon* case still serves as a valuable lesson on 1) what are the issues of the future and 2) how can policies help/harm legal defenses.

Quon arises from a suit brought by a City of Ontario officer and his wife and girlfriend after the messages on Officer Quon's city-issued pager were read and reviewed by the police department in an effort to determine his usage amount. *Id.* The Ninth Circuit Court held that Officer Quon did have a reasonable expectation of privacy based on his reliance on the representations ("informal policy") of the lieutenant who administered the pager program. *Id.* at 908. The Court further held that reading Quon's

messages constituted an unreasonable search because the search's scope exceeded the objectives of the search, which was to ensure that employee's were not paying for work related expenses (pages). *Id.* at 909. The Court determined there were other ways to determine the usage amount of the pager without actually reading the pages. *Id.*

The Supreme Court's opinion, hot off the presses, reversed the Ninth Circuit and held that the search of Quon's text messages was reasonable and thus no violation of his Fourth Amendment rights. *City of Ontario,* 2010 U.S. LEXIS 4972, at *9-17. In doing so, the Supreme Court specifically does not analyze whether Quon had a reasonable expectation of privacy in his text messages but assumes that even if he did, the search was reasonable under either approach presented in *O'Connor's* plurality decision because it was motivated by a legitimate work-related purpose. *City of Ontario,* 2010 U.S. LEXIS 4972, at *9-17. Additionally, because the search was reasonable as to Quon, it was reasonable as to the wife and girlfriend as well. *Id.* at *16-17.

From the practitioner standpoint, several lessons can be learned from the Ninth Circuit decision in *Quon* regardless of the Supreme Court's ruling. First, even though there is a great chasm of conflict over whether or not the City of Ontario had "official" or "unofficial" policies regarding the pager use, the dispute is one that the city created for itself. The City of Ontario did have a general "Computer Usage, Internet and E-mail Policy" in place at the time Officer Quon was issued the pager. *Id.* at 896. However, it is undisputed that the policy did not cover pagers or text messages. Allegedly, management orally informed Quon and other officers that text messages would be considered e-mail pursuant the city policy. *Id.* There is also a dispute between the parties as to whether an "informal" policy existed with regard to officer pager usage. Regardless of whether an "informal" policy existed or rose to the level to negate the "formal" policy, it is undisputed that the lieutenant tasked with overseeing the pagers told the officers that as long as they paid for any overages each month, he would not audit the text messages. *Id.* at 897.

Thus, the major issue in *Quon* surrounding the officer's expectations of privacy was created, at least in part, by the City of Ontario's lack of a comprehensive policy addressing city-issued pagers. More importantly, to the extent that the City of Ontario argues that a policy did exist, it is clear that the record is conflicted as to whether and to what extent the affected employees were educated regarding the policy.

The Supreme Court opinion makes it clear that when these cyber world issues arise, the Supreme Court will apply existing case law and analogies to the technical mediums. Additionally, even when the employee has an expectation of privacy, if the search is justified at its inception and carried out reasonably, then a violation of the Fourth Amendment is unlikely. The Supreme Court further provides insight as to factors that weigh in favor of the employer when conducting a search of computer messages. For example, in *City of Ontario*, the Court noted that the City only audited two months worth of texts and during its internal affairs investigation redacted the content of off-duty texts. *City of Ontario,* 2010 U.S. LEXIS 4972, at *13-14. The Court also noted that the fact that the employee was an officer and knew his actions could come under scrutiny meant that the audit of his on-duty text communications was not too intrusive. Most importantly, the Supreme Court specifically rejected that a search must be the "least intrusive" means. *Id.*

IV. WHAT SHOULD OUR POLICY SAY ANYWAY?

The Ninth Circuit's ruling in *Quon* should serve as a warning to employers about having unclear policies regarding technology, and about administrators "bending the rules." Additionally, existing case law and statutes serve as the starting point for creating defensible personnel policies should a public employer find itself defending a discipline of an employee for speech related to e-mail, text communications, or a social networking site. Most organizations have "computer usage" policies that have been in place for many years; however, because of the ever expanding cyber world, any policy over five years old should be reviewed. Particularly, policies that focus on an employee's use of city equipment for electronic access do not address the employee's use of their own personal equipment while in the course and scope of employment with the city. Further, how much does the city want to police personal use on personal time that may adversely impact the organization? For example, off-duty conduct is often actionable if it tends to discredit the organization or the position the employee holds. Do general standards of conduct policies suffice when the off-duty conduct is a comment on Facebook? Arguably they would and should but a practical approach would dictate that the policy reflect that an employee's off-duty cyber world conduct may be subject to scrutiny. Certainly, a written policy would at least provide some notice to the employee and counter to the employee's potential expectation of privacy argument. Public employers should examine existing policies with an eye towards the expanded uses and accesses that employees have to many electronic mediums during their work day. Two keys

to a defensible policy are (1) the policy contents and (2) consistent enforcement. Acceptable use policies typically outline an organization's position on how employees are expected to use the governmental entity's resources, restrictions on use for personal interests and consequences for violating the policy.

With regard in particular to social/professional network sites, many social media policies note that employees are responsible for the content that they provide on social media sites. A good example is the U.S. Air Force which encourages employees to consider themselves on duty 24/7 when it comes to social media use. http://www.af.mil/shared/media/document/AFD-090406-036.pdf. Sample language from the State of Utah addresses social/professional website usage by employees as follows:

> "[The] lines between public and private, personal and professional are blurred. By identifying yourself as a State employee, you are creating perceptions about your expertise and about the State by legislative stakeholders, customers, business partners and the general public. …Be sure that all content associated with you is consistent with your work and the State's values and professional standards." http://www.utahta.wikispaces.net/file/view/State%20of%20Utah%20Social%20Media%20Guidelines%209.22.09.pdf

The State of Utah's policy specifically addresses the issue of "conduct" on a social networking site and puts the employee on notice as to the expectations. Most policies also warn employees against the use of any materials that are discriminatory, intimidating, hostile, offensive, or pornographic. Just as these types of conduct would be actionable by an employer in any setting, it bears repeating that such conduct is actionable in an electronic media setting as well.

Some policies proactively require employees to use disclaimers on social media sites in order to detach the opinions and actions of individual employees from their employer. For example, the City of Hampton Virginia's policy states:

> "Make it clear that you are speaking for yourself and not on behalf of the City of Hampton. If you publish content on any website outside of the City of Hampton and it has something to do with the work you do or subjects associated with the City, use a disclaimer such as this: 'The postings on this site are my own and don't necessarily represent the City's positions or opinions.' " Hrdinová, Helbig & Stollar Peters at p. 11.

Each organization must carefully craft its policy to represent its philosophy while keeping legal challenges in mind. Policies must be reasonable and realistic in that wholesale prohibitions on all personal use of city IT systems or personal systems while at work present challenges to the operational realities of today's world. All policies should also be reviewed in light of the governing law on public records and sunshine laws. Any policy should be drafted with legal, management and IT professionals who can evaluate monitoring and enforceability from each unique perspective. Last but not least, once a policy is drafted, educate the supervisors and educate the workforce.