Privacy Expectation in Public Workplace Electronic Communications

WHITE PAPER

INTRODUCTION

Employers have several legitimate reasons for wanting to control and monitor workplace communications including: (1) maintaining a professional work environment; (2) increasing employee productivity; and (3) controlling and limiting the dissemination of trade secrets or other proprietary and confidential information.[1] Often, these employer interests run contrary to employee privacy expectations.[2] The integration of new communication technologies into the workplace has increased the difficulty for employers to protect their interests, especially as technology in the workplace evolves.[3]

The U.S. Supreme Court decision in *City of Ontario v. Quon* (2010)[4] provides guidance about the use and enforcement of electronic communication policies in the workplace. Additionally, the recent Louisiana Supreme Court decision *Shane v. Parish of Jefferson* (2015),[5] addresses non-employee third party expectation of privacy in electronic communication with public employees. This paper first provides a general overview of privacy right case law prior to *Quon,* including privacy in the public workplace. Next, the U.S. Supreme Court's *Quon* decision and the Louisiana Supreme Court's *Shane* decision are discussed. Finally, the implications of both the *Quon* and *Shane* cases on employers' monitoring of employee use of the employers' computer or communication facilities are addressed.

[1] Mary Ellen Callahan, et al, *Reading Your Employees' Text Messages May Get You Into Hot Water,* Privacy Tracker Vol.1, No. 6 September 2008, at 2-8.
[2] *Id.* at 3.
[3] *Id.*
[4] *City of Ontario v. Quon*, 560 U.S. 746, 130 S.Ct. 2619, 177 L.Ed.2d (2010).
[5] *Shane v. Parish of Jefferson, et al,* 14-2225 (La. 12/8/15); 209So.3d 726.

I. GENERAL PRIVACY RIGHTS CASE LAW PRIOR TO *QUON*

The Fourth Amendment protects the "rights of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[6] This Fourth Amendment "right to privacy" affords protection against unreasonable government intrusion into protected privacy interests. In the context of public employers, this makes the Fourth Amendment applicable to non-criminal investigations in the workplace.[7]

In order for a search and seizure to be considered unreasonable, and thus violate the Fourth Amendment, a person must have a reasonable expectation of privacy in the place or item searched. Although always a fact specific question, a long line of jurisprudence provides guidance as to when an expectation of privacy is reasonable and thus a search unreasonable.

In *Katz v. United States* (1967)[8] the U.S. Supreme Court considered the question of whether a person had a reasonable expectation of privacy in a telephone call made in a public phone booth. In that case, the government placed a wiretap to electronically listen to and record the defendant's telephone conversations in a phone booth frequently used by the defendant. First, the Court noted that the Fourth Amendment protects people, not places. Next, the Court stated that what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. However, what a person seeks to preserve as private, even in a public area, may be constitutionally protected. The Court explained that the application of the Fourth Amendment turns on a two-party inquiry: (1) whether the person has exhibited actual (subjective) expectation of privacy; and (2) whether the person's expectation is one that society is prepared to recognize as reasonable. As to the first question, the Court concluded that when a person enters a phone booth, shuts the door and places a call, he has exhibited an actual expectation that his conversation will not be broadcast to a third party. As to the second question, the Court concluded that the use of public phone booths to place private telephone calls had become a societal norm such that a person's expectation of privacy in placing such a call was

[6] US Const. amend. IV.
[7] The Fourth Amendment applies to the States through U.S. Const. amend. XIV.
[8] *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967)

reasonable. Accordingly, the Court held that governmental wiretapping of the public telephone booth was an unreasonable search under the Fourth Amendment that violated the privacy of the defendant.

The Court distinguished its *Katz* holding in *Smith v. Maryland* (1979),[9] where the state police, with the cooperation of the telephone company, used a pen register to record the telephone numbers dialed by the defendant on his home telephone. The Court's decision turned on the fact that unlike a wiretap, which records the actual contents of a conversation, a pen register records only the telephone number entered. The Court reasoned that 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. Accordingly, the Court held that the governmental use of the pen register was not an unreasonable search under the Fourth Amendment.

Two U.S. Ninth Circuit cases extended the reasoning of *Katz* and *Smith* to postal mail and email. In *United States v. Hernandez* (2002),[10] the U.S. Ninth Circuit held that a person has a reasonable expectation of privacy in the contents of a letter or package, which is concealed from third parties, but not in the address of the sender or recipient, which is on the exterior of the letter or package, and visible to third parties. In *United States v. Forrester* (2008),[11] the U.S. Ninth Circuit held that while a person may have a reasonable expectation of privacy in the content of emails, there is no expectation of privacy in the "to/from" addresses of email, which is provided to and used by the internet service provider to transmit the message.

[9] *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979).
[10] *United States v. Hernandez,* 313 F.3d 1206 (9th Cir. 2002).
[11] *United States v. Forrester,* 512 F.3d 500 (9th Cir. 2008).

II. PRIVACY IN THE PUBLIC WORKPLACE

The right to privacy of government workers in the workplace was addressed by the U.S. Supreme Court in *O'Connor v. Ortega* (1987).[12] In that case, the public employer searched an employee's office as part of a non-criminal investigation, which search included the employee's desk drawer and file cabinets. Although *O'Connor* is a plurality opinion, the justices unanimously affirmed the Fourth Amendment's application to non-criminal investigations in the workplace of public employers. Further, the justices unanimously recognized the public employee's protected privacy interest in his desk and filing cabinet because he had exclusive use of them and stored personal items there.

The plurality recognized the onerous burden that requiring public employers to obtain search warrants for non-investigative, work-related and investigative work-related misconduct searches would place on employers and created an exception to the warrant requirement for such searches in the public workplace. The *O'Connor* court established a two-part test necessary to support a finding of a Fourth Amendment violation during a non-criminal workplace search: (1) the employee must have had a reasonable expectation of privacy in the area or item searched, which is a factual determination made on a case-by-case basis; and (2) the search itself must have been unreasonable under the circumstances. The plurality concluded that an intrusion by a public employer on such a protected privacy interest of a government employee for non-investigative, work-related purposes and for investigation of work-related misconduct does not violate the Fourth Amendment if the search was reasonable in its inception and scope.

Additionally, the plurality noted that certain "operational realities of the workplace" may render an employee's expectation of privacy unreasonable. As an example, the Court noted that if the employees where informed that the employer would conduct searches of offices and were advised not to keep personal items in their desks and file cabinets, then that "operational reality" would diminish the employees' reasonable expectation of privacy in their offices.

[12] *O'Connor v. Ortega,* 480 U.S. 709, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987).

In *United States v. Ziegler* (2007)[13] the U.S. Ninth Circuit applied the *O'Connor* two-part test to determine whether a public employee had a reasonable expectation of privacy in the contents of a work computer locked in his office. In that case, the employer had a written policy stating that computer usage would be monitored. As part of a criminal investigation into the employee's possible access to child pornography from his workplace computer, the employer cooperated with, consented to and assisted in a government search of the employee's office computer. The Ninth Circuit held that while the employee did have a reasonable expectation of privacy in his office, his employer could consent, on the employee's behalf, to a search of the employer-owned computer within that office. The factors the court found dispositive were: (1) the employer routinely and actively monitored the computer usage of its employees; and (2) the employer informed employees through its written policies and through training that the computers would be monitored and should not be used for personal reasons.

In a case involving a private employer, *Muick v. Glenayre Elecs.* (2002),[14] the employer seized and held the defendant's work laptop computer while law enforcement authorities obtained a search warrant. The U.S. Seventh Circuit found the fact that at the time the employer issued the laptop to the employee, it informed him that it reserved the right to inspect the laptop at any time dispositive. The Seventh Circuit held that any reasonable expectation of privacy the employee may have had in the laptop was destroyed when the employer announced its right to inspect the company-issued laptop at any time. Additionally, the Seventh Circuit held that the employer, as owner of the laptop, had the right to attach specific conditions to its use, which made its policy of monitoring inherently reasonable.

In *Bohach v. City of Reno* (1996)[15], the U.S. district court considered a case involving two-way pagers issued to police officers. The district court reasoned that the police officers' privacy rights were not violated during an internal investigation that examined messages they sent using the department's computerized paging system because when the pagers were issued the department informed all employees, via memorandum, that messages sent on the pagers would be: 1) logged onto the department's network; 2) were subject to review; and 3) that certain types

[13] *United States v. Ziegler,* 474 F.3d 1184 (9th Cir. 2007).
[14] *Muick v. Glenayre Elecs.,* 280 F3d 741 (7th Cir. 2002).
[15] *Bohach v. City of Reno,* 932 F.Supp. 1232 (D. Nev. 1996).

of messages where prohibited. The U.S. district court held that the "operational reality" of the department's policy led to the police officers having a diminished expectation of privacy in the messages sent on the pagers.

These cases demonstrate three important factors regarding privacy expectations in the context of electronic communications. First, employees' privacy expectations are not automatically overcome by an employer's ownership of the property or device being searched; the question always turns on the reasonableness of the employees' privacy expectation. Second, employee privacy expectations may be diminished through employer policies and procedures; that is, the "operational realities" of the workplace. Third, privacy determinations must always be made on a factual case-by-case basis.[16]

III. THE *QUON* DECISION

In *Quon,* 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, California (together, the "City"), and the City's wireless service provider, Arch Wireless, asserting, among other claims, Fourth Amendment violations resulting from the audit of Quon's text messages by the department. The text messages in question were sent by Quon on a two-way alphanumeric pager issued to him and paid for by the police department.

The City distributed the pagers to members of the police department's SWAT team, which included Quon. The issuance of city-owned pagers was to enable better coordination and more rapid and effective responses to emergencies by providing nearly instantaneous situational awareness to the SWAT team. The two-way pagers were not intended for personal use. The City had no written policy regarding text messaging at the time the two-way pagers were issued, but 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 the right to monitor and log all network activity including email and Internet use

[16] Callahan, *supra* n. 1 at 5.

and prohibited the use of "inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language," in emails. 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. At an April 18, 2002 staff meeting, at which Quon was present, the OPD officer responsible for the City's contract with Arch Wireless, Lt. Duke, told officers that messages sent from the pagers were considered email and would fall under the City's auditing policy. This warning was put in writing in a memorandum sent on April 29, 2002.

By the second billing cycle after being issued the pager, Quon exceeded his monthly allotment of 25,000 characters. Lt. Duke verbally reminded Quon that the text messages sent using the City-owned pager were "considered email and could be audited at any time," but also told him that his messages would not be audited if he paid the overage charges himself. Thereafter, Quon exceeded the monthly character limit several times and paid the City for the overages each time without being audited.

After several months of Quon and others exceeding the monthly character limit, Lt. Duke became tired of playing, as he characterized it, the role of "bill collector" and spoke with the police chief about the overages. In response, the police chief ordered transcripts of Quon's text messages, as well as those of other employees who used the pagers, to determine whether the text messages were work-related. Lt. Duke contacted Arch Wireless to obtain copies of the text messages to conduct the audit of August and September of that year. No notice was given to Quon or the other employees of the audit.

The transcript for Quon's pager totaled forty-six pages. Many of the text messages that were sent or received on Quon's pager while he was on duty, both to his wife, plaintiff Jerilyn Quon, and to his mistress, plaintiff April Florio, a member of the Police Department's dispatch center, were sexually explicit in nature. Other messages, while not sexually explicit, but were nonetheless private, were sent or received from Quon's co-worker, plaintiff Sergeant Trujillo. The police chief determined that Quon's pager was being misused and that "too much duty time was used for personal pages." The matter was then referred to internal affairs in October 2002 for an investigation "to determine if someone was wasting . . . City time not doing work when they should be," which could be potential grounds for a finding of misconduct.

Quon, along with the other plaintiffs, filed suit in February 2003 asserting 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, invasion of privacy and defamation.

1. The *Quon* U.S. District Court Decision

The district court first decided the issue of whether Arch Wireless violated the Stored Communications Act (SCA) by supplying the City with the transcripts of Quon's text messages, eventually concluding that Arch Wireless was an immune entity within the definition of the SCA and, therefore, was not liable to the plaintiffs.

The court then considered whether the audit conducted without their consent or knowledge violated the plaintiffs' Fourth Amendment privacy rights. The district court used the *O'Connor* test for its Fourth Amendment analysis. That is, the district court considered first whether Quon had a reasonable expectation of privacy in the text messages sent and received from his pager; and, if so, second, whether the City's search was reasonable from inception and in scope. As part of this analysis, the district court looked at the "operational realities" of the workplace that may impact expectations of privacy, such as whether Quon had been notified in writing and in person that the City regarded use of the pagers to fall within its e-mail policy, or whether the use of the pagers would be monitored or audited. If so, according to the district court, Quon would not have a reasonable expectation of privacy in his text messages.

First, citing *O'Connor* and *Ziegler*, the district court rejected a *per se* rule that public employees cannot have a reasonable expectation of privacy when using property owned by their employer. The district court found that such a rule would be at odds with precedent that expectations of privacy are not always related to property rights because the Fourth Amendment "protects people, not places." Second, the district court considered whether Quon had a reasonable expectation of privacy in the text messages sent and received on the City issued pagers. Of particular importance to the district court was the City's informal policy regarding the treatment of overage charges. The district court held that in light of the informal policy giving employees the option to pay overage charges rather than having their messages audited, Quon did 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 district court then considered whether the City's search was reasonable under the circumstances (that is, reasonable at its inception and in its scope) and 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, and therefore reasonable at inception, all defendants were absolved of liability in the district court. The plaintiffs appealed the decision to the U.S. Ninth Circuit.

2. The *Quon* U.S. Ninth Circuit Decision

The Ninth Circuit affirmed in part, reversed in part and remanded the case back to the district court for further proceedings. The only portion of the district court's decision the circuit court upheld was its finding that plaintiffs had a reasonable expectation of privacy in their text messages. The Ninth Circuit reversed and remanded the lower court as to its finding that Arch Wireless was immune from liability under the SCA and as to the jury trial's findings pertaining to the reasonableness of the City's audit of the text messages.

Like the district court, the circuit court applied the *O'Connor* two-part test to hold that the *Quon* plaintiffs had a reasonable privacy expectation in the content of the text messages they sent to and received from Quon. The circuit court agreed with the district court that the City's informal policy that the text messages would not be audited if he paid the overages rendered Quon's expectation of privacy in those messages reasonable. The circuit court noted that if not for this "operational reality," the formal policy contained in the City's "Computer Usage, Internet, and E-mail Policy" would have defeated any reasonable expectation of privacy Quon may have had in the text messages.

The circuit court then considered whether the audit conducted by the City was reasonable at its inception and in its scope. The circuit court did not overturn the jury's determination that the search was reasonable at its inception because 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. However, under a *de novo review* as to the search's scope, the circuit court concluded that the

scope was unreasonable, primarily because there were less intrusive means of conducting the audit. Examples of less intrusive means cited by the circuit court were: (1) the City could have 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; or (2) the City could have given Quon the opportunity to redact from the transcript any messages that were personal in nature. The circuit court concluded that because there were less intrusive means of reviewing the text message transcript, the scope of the City's search was unreasonable.

The circuit court remanded the case back to the district court for a determination of Arch Wireless' and the City's liability towards the plaintiffs. The defendants applied for a writ of certiorari to the U.S. Supreme Court.

3. The *Quon* U.S. Supreme Court Decision

The Supreme Court granted writs as to the Fourth Amendment issues only and, in a unanimous decision, reversed the Ninth Circuit and ruled that the City's examination of Quon's text messages was reasonable under the Supreme Court's *O'Connor* standard. The Court reasoned:

> Petitioners' warrantless review of Quon's pager transcript was reasonable under the *O'Connor* plurality's approach because it was motivated by a legitimate work-related purpose, and because it was not excessive in scope. The city had a reasonable interest in controlling excessive personal use of communications devices, and also in setting an appropriate level of city-funded communications so that officers were not forced to pay for work-related communications.

The Court observed that the City's review was limited to a two-month sample of messages and that the City redacted Quon's messages sent and received while he was off duty, to limit the intrusion into his personal life. Further, the Court rejected the considerations engaged in by the lower courts of "less intrusive" means of conducting the search. The Court held that no part of the *O'Connor* test held reasonableness of scope as equating to "least intrusive means."

Further, the Court noted that any reasonable privacy expectations the *Quon* plaintiffs had were limited by the City's "Computer Usage, Internet, and E-mail Policy," which stated that users "should have no expectations of privacy or confidentiality" when using City computers. Additionally, the subsequent memo circulated by the police department after the pagers were issued made it clear that this policy extended to all communications devices furnished by the City.

As argued before the lower courts, Quon again argued that this policy was modified by his superior's subsequent verbal assurance that there would be no audit as long as officers paid for excess text usage. The Court declined to make a finding on that argument, assuming for purposes of the decision that Quon had some reasonable expectation of privacy. Instead, the Court ruled that the City's search of message content was reasonable because: (1) it was undertaken for a work-related purpose; and (2) used measures that were not excessively intrusive under the circumstances. The Court concluded that because the employer's search was reasonable, the other parties who sent messages to Quon could not prevail on their argument that the review of message content violated their own Fourth Amendment rights.

The *Quon* opinion is of particular significance because the Supreme Court justices often disagree on what is a "reasonable expectation of privacy" and whether the government entity in question has appropriately limited the scope of its intrusion into private life. The *O'Connor* opinion, as noted *supra,* was rendered by a plurality of the justices. *Quon,* on the other hand, is a unanimous decision on its results, with limited concurring opinions by Justices Stevens and Scalia.

Justice Scalia's concurring opinion argued that the "reasonable expectations" of employees using employer-issued devices should be addressed generally and not limited to public employees. In response, Justice Kennedy's opinion for the Court suggests that reasonable expectations of privacy are typically limited in private sector employment just as they are for government employees:

> For these same reasons—that the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification—the Court also

> concludes that the search would be 'regarded as reasonable and normal in the private-employer context.

Additionally, Justice Kennedy cautioned that judges should not rush to broad conclusions about reasonable privacy expectations with regard to the use of rapidly changing technologies:

> 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 the Fourth Amendment implications of emerging technology before its role in society has become clear.

IV. THE SHANE DECISION

William Henry Shane, a private citizen, exchanged emails related to political matters in 2010 with Lucien Gunter, who was then the Executive Director of the Jefferson Parish Economic Development Commission ("JEDCO").[17] Both men were also members of two private nonprofit organizations, the Jefferson Business Council ("JBC") and the Committee for a Better Jefferson ("CBJ"), comprised of local businesspersons who sought to improve the economic well-being and quality of life in Jefferson Parish. In addition, Gunter and Shane were members of the Jefferson Community Foundation ("JCF"), a public charity administering donations for the educational, cultural, and charitable benefit of Jefferson Parish citizens. The emails at issue were exchanged during 2010 between Gunter (via his JEDCO email address), Shane, and other members of these organizations.

[17] JEDCO was created by La. R.S. 34:2021(A) as a "special parish district," originally designated as the "Jefferson Parish Economic Development and Port District," having the power "to acquire, construct, improve, maintain, and operate projects" and "to provide such additional parish services within the district as may be required by the Jefferson Parish Council." JEDCO was further declared to be "a body politic and political subdivision of the state of Louisiana" by La. R.S. 34:2021(A).

In June of 2012, the results of an audit on JEDCO operations were released by outside auditing company Postlethwaite & Netterville, which noted that there had been some "*de minimis* use" of JEDCO's email systems by "certain JEDCO employees" to engage in "political campaign activities" during 2010.

In August 2012, the results of an internal audit were released by Jefferson Parish auditor Tommy Fikes, which also addressed Mr. Gunter's use of his JEDCO email for private purposes, along with other alleged improprieties related to Gunter's employment as JEDCO's Executive Director. Fikes' report noted the fact that the Postlethwaite & Netterville audit report referenced *de minimis* use of JEDCO's email system for political activities; however, the Fikes report focused on Gunter's "significant political activity related to the 2010 Jefferson Parish School Board Election" and concluded that the use of Gunter's "public time" for his political activity should be reviewed by the JEDCO Board of Commissioners for any violation of the Louisiana Code of Ethics, particularly La. R.S. 42:1116(B).

Subsequently, on October 26, 2012, The Times–Picayune reporter Drew Broach transmitted a public records request, via email, to JEDCO seeking to inspect the following:

> (1) All "political" emails that were so deemed during or as a result of JEDCO's annual audit for 2011. This should include emails composed and sent in 2010.
> (2) All correspondence between JEDCO and the Jefferson Parish attorney's office, or other attorneys, relating to the JEDCO executive director's residency requirement.

On November 8, 2012, Broach submitted a "revised and restated" public records request to JEDCO, requesting release of the following:

> [A]ll emails that were referenced by Postlethwaite & Netterville professional accounting corporation on Page 51 of the JEDCO's Financial Statements and Schedules for the year ending Dec. 31, 2011, said report bearing a release date of June 6, 2012. I specifically refer to this language from said report: "During the course of our audit procedures for the year ended December 31, 2011, we were made aware of certain JEDCO employees that

were engaged in political campaign activities during the year ended December 31, 2010. We observed *de minim[is*] use of JEDCO's email system to engage in these activities."

JEDCO's then-public records custodian, Cynthia Grows, denied the public records request, stating that the emails at issue were not subject to disclosure because they were "purely personal in nature" and had "no relation to the public business of JEDCO," and, even if considered public records, they were exempted from disclosure under La. Const. Art. I, Sec. 5's right to privacy.

Broach again modified his public records request, on November 21, 2012, to ask that the emails be released after redaction to mask the identities of senders or recipients who were not JEDCO employees. Grows again denied the request "for the same reasons given" in her earlier denial.

On December 20, 2012, The Times–Picayune and Broach submitted a public records request to Jefferson Parish, seeking release of the emails previously sought in the November 8, 2012 public records request submitted to JEDCO. Jefferson Parish, having obtained the emails for purposes of the internal audit by Fikes, concluded that the emails were public records and announced its intent to make the records available for public inspection on February 1, 2013.

On February 1, 2013, Shane filed suit for declaratory and injunctive relief against Jefferson Parish and JEDCO, seeking to prevent the disclosure of the email correspondence with Gunter, asserting a right of privacy under La. Const. Art. I, Sec. 5.[18] A temporary restraining order was immediately issued by the district court, enjoining the defendants from "permitting inspection and/or copying of any and all emails between [Shane] and any other members of [JBC, CBJ, and/or JCF], including but not limited to Lucien Gunter, by The Times–Picayune and/or The Advocate."

Jefferson Parish responded, admitting that it did announce its intent to make the emails available to the requesting parties and further alleging that "JEDCO employees were aware that

[18] "Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable searches, seizures, or invasions of privacy." La. Const. of 1974, Art. I, §5.

they were using government time, talent and resources to further their political activities, and thus had no expectation of privacy."

JEDCO responded, stating that Shane was "entitled to an injunction against the Parish of Jefferson." JEDCO further alleged that its current public records custodian, Dottie Stephenson, concurred in the prior denial of the media's public records request by its prior public records custodian, Cynthia Grows. JEDCO also asserted that the media's sole remedy, upon denial of its request, was, pursuant to La. R.S. 44:35, to institute suit against its custodian for the issuance of a writ of mandamus or for injunctive or declaratory relief. JEDCO alleged that the media failed to avail themselves of the sole remedy available under La. R.S. 44:35 and, instead, "attempted to circumvent the custodian (JEDCO) and made a public records request on Jefferson Parish, who is not the custodian of the electronic correspondence in question." JEDCO alleged that its designated records custodian (previously, Grows; currently, Stephenson) was the only person authorized to release the emails at issue under the Public Records Law.

An intervention was filed by The Times–Picayune, L.L.C. and Broach (hereinafter, "media-intervenors") to assert the public's right of access and to oppose Shane's request for an injunction. In his answer and affirmative defenses to the intervention, Shane further alleged that release of the emails would violate La. Const. Art. I, Sec. 7[19] and La. Const. Art. I, Sec. 9[20].

1. The *Shane* District Court Decision

The district court rendered judgment granting Shane's request for injunctive relief, in part. First, the district court considered whether the emails containing "purely private" matters were public records. The district court reasoned that because the emails had been used by JEDCO's external auditor and by Jefferson Parish's internal auditor in reviewing the business affairs of JEDCO, the emails were public records.

[19] "No law shall curtail or restrain the freedom of speech or of the press. Every person may speak, write, and publish his sentiments on any subject, but is responsible for abuse of that freedom." La. Const. of 1974, Art. I, §7.
[20] "No law shall impair the right of any person to assemble peaceably or to petition government for a redress of grievances." La. Const. of 1974, Art. I, §9.

Next, the district court considered whether Shane, as a non-employee third party was entitled to assert Louisiana state constitutional rights of privacy and association, as a private citizen, relative to the emails. Shane asserted that the emails contained ideas, strategies and opinions concerning political advocacy among members of the private associations, which the associations' members intended to be private and that the disclosure of the association members' internal deliberations and planning would eliminate all associational privacy and have a chilling effect.

The district court concluded that Shane possessed such right and, after balancing of the various interests, determined that the emails should be redacted prior to release as public records. Further, the district court ruled that the redaction should include the identities of all persons reasonably believed to have been private citizens, and not public employees, at the time the emails were written. The redactions, as to the private citizens, were to include names, addresses, email addresses, phone numbers, and places of employment, within the sender, recipient, address, and body sections of the emails, as well as within any attachments to the emails. The names of the employees of JEDCO, elected officials, and political candidates, who had qualified for the office, were not ordered redacted. Both Shane and the media-intervenors appealed the district court's ruling.

2. The *Shane* 5th Circuit Decision

The 5th Circuit reversed the district court decision and granted Shane injunctive relief.[21] First, the 5th Circuit considered the question of whether the emails were public records. The 5th Circuit reasoned that emails generated and received by an employee at a public employer's email address, and maintained on computer equipment owned and controlled by the employer that were not used or prepared for the employer's use or performance of its business, did not fall within the definition of public records under the state's public records law. The 5th Circuit further found there was no evidence that the individuals who generated or were recipients of the emails were acting on behalf of the public employer and there were no pending investigations concerning the public employee's possible misconduct, which might have justified seizure of emails. The 5th Circuit

[21] *Shane v. Parish of Jefferson,* 13–0590 (La.App. 5 Cir. 9/24/14), 150 So.3d 406.

concluded that the emails were purely private communications between private citizens concerning private political activity, and the content of the emails has nothing to do with the business of JEDCO.

The 5th Circuit then considered whether Shane, as a non-employee third party, was entitled to assert Louisiana state constitutional rights of privacy and association, as a private citizen, relative to the emails. The 5th Circuit concluded that Shane, as a private citizen, had a reasonable subjective expectation of privacy in his email correspondence with the JEDCO employee, notwithstanding the fact that the emails were sent to a large number of individuals involved in political activity where the non-employee third party testified that he believed recipients of the emails involved in political activity would keep the communication private, and that if one attempted to obtain emails from the other members "[t]hey won't give it to you, they're private." The 5th Circuit further reasoned that because the right to privacy extended equally to content of private email messages as it did to names of other correspondents, even with redaction of identities of all persons reasonably believed to have been private citizens, a private citizen's constitutionally protected rights of privacy and of freedom of association outweighed need for disclosure under Public Records Law.

The media-intervenors sought review of the appellate court decision to the Louisiana Supreme Court, which granted a writ of certiorari.[22]

3. The *Shane* Louisiana Supreme Court Decision

The Louisiana Supreme Court reversed the 5th Circuit Court of Appeal and reinstated the district court's ruling. First, the Court reaffirmed the broad scope of the public records law:

> The legislature, by enacting the "Public Records Law" sought to guarantee, in the most expansive and unrestricted way possible, the right of the public to inspect and reproduce those records which the laws deem to be public. There was no intent on the part of the legislature to qualify, in any way, the right of access. . . .

[22] *Shane v. Parish of Jefferson,* 14–2225 (La.2/6/15), 157 So.3d 1137.

> [A]ccess to public records can be denied only when the Public Records Law or the Constitution specifically and unequivocally provide otherwise.[23]

The Court held that the emails fell within the broad definition of public records because they "were used in JEDCO's regular business, transactions, work, duties or functions" in that the emails were used in the audits of the agency's operations.

The Court then considered whether Shane, as a non-employee third party, could assert any exceptions to the public records laws, specifically the Louisiana state constitutional rights of privacy and association. The Court found that the content of the emails "consisted of the discussion of private political matters which had nothing to do with JEDCO's operations" and held that Shane, as a non-employee third party, could assert rights of privacy and association in the emails. Therefore, the Court concluded, these "rights must be balanced against the right of the public to inspect the records."

The Court held that upon balancing the public's right to inspect the emails against the private citizen's constitutional rights of freedom of association and privacy, the latter may be adequately protected by redacting identifying information, which should include the names, addresses, email addresses, phone numbers and places of employment of all private citizens, before releasing the emails. Information about JEDCO employees, elected officials and candidates for public office were not required to be redacted.

Finally, the Court considered the question of whether only JEDCO, or also the Parish government, was a custodian of the emails, as only custodians are subject to public records requests. The Court stated that the Public Records Law defines "custodian" as the "**head of any public body having custody *or* control of a public record"** (emphasis in original). The Court reasoned that the use of the word "or" in the definition of custodian led to the conclusion that "custody" under the statute may include "a mere physical possession." The Court found that this conclusion was supported by the fact that the definition of "public records" is not limited to originals, but includes "all copies, duplicates, photographs, including microfilm, or other

[23] *Shane* at 5 (internal citations omitted).

reproductions." La. R.S. 44:1(A)(2)(a). The Court further reasoned that its interpretation of public records custodian – to include not only the original custodian, but also subsequent public officials who have obtained custody of the record – to be consistent with the legislative goal of the Public Records Law to resolve all doubt in favor of the public's expansive and unrestricted right to access.

The *Shane* decision is significant because many state courts have previously ruled that emails written by public employees on public email systems are, nevertheless, not public records if their contents are private.[24] The *Shane* decision rejects that interpretation of Public Records Law to hold that email correspondence with non-employee third party private individuals about private matters, even constitutionally protected matters, may be public records if they are also used in a public function. Under *Shane,* at least one such public function – an auditor's review of private, constitutionally protected correspondence between a public employee and a private citizen -- may turn that correspondence into a public record under the Louisiana Public Records Law. Further, redaction of the non-employee third party identifying information from such public records adequately preserves the third party's constitutionally protected rights of privacy and association.

V. CONCLUSION

Although *Quon* deals with public employees and the Fourth Amendment and *Shane* deals with non-employee third parties and Louisiana state constitutional rights, both decisions can be read to suggest public employers take a prudential approach in monitoring employee use of computers or communications facilities in the workplace. Such approach should take into consideration the following factors:

- Employers should establish the level of privacy expectations with a coherent policy that covers all the technologies used in the workplace. Such policy should include:

[24] See, *Schill v. Wisconsin Rapids School Dist.,* 786 N.W.2d 177 (WI 2010); *Easton Area School Dist. V. Baxter,* 35 A.3d 1259 (Penn. 2012); *Assoc. Press v. Canterbury,* 688 S.E.2d 317 (W. Va. 2009); *Howell Ed. Ass'n MEA/NEA v. Howell Bd. of Ed.,* 789 N.W.2d 495 (App. MI 2012); *State v. City of Clearwater,* 863 So.2d 149 (FL 2003).

- Clear notice of the employer'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 affirmative consent by employees to any company policies with regard to monitoring or auditing activities;
- Ensure policy covers all methods of communication generally to avoid having to constantly update as technology evolves;
- Training of supervisors and employees to ensure compliance with the policy;[25]

- Clearly articulate a work-related purpose (such as a targeted investigation of suspected wrongdoing or a non-investigative financial or administrative objective) prior to performing content review of text messages or computer searches; [26]

- Content review should be structured so as to limit privacy intrusions. The *Quon* decision emphasizes that this does not mean the "least intrusive search practicable" but simply a search reasonably limited to the employer's legitimate, work-related objectives; and

- A reasonably structured review of employee communications may also serve as a defense against privacy claims by non-employee third parties who communicate with the employee in light of the *Shane* decision.

[25] Callahan, *supra* n. 1 at 8.
[26] *Id.*