MONITORING EMPLOYEES' ELECTRONIC MUSINGS:
New Ways For Employers And Employees To Get Into The Same Old Trouble

I. INTRODUCTION

Imagine a female employee and her boyfriend meet for a drink after work and, under the influence of work-related stress and her favorite alcoholic beverage, she relays a tale of office harassment involving her married supervisor and his assistant. She's adamant that the company knows of the harassment, but has chosen to turn a blind eye because her supervisor is a valued employee. In the sober light of the following morning there's a good chance the couple will decide to keep their opinions between themselves and the issue will go no further. It's unlikely the company ever will become aware of the woman's comments.

Now, imagine instead that the woman returns from work and texts her thoughts to her friends, who then proceeded to share them with their friends, and soon nearly 20 people knew of the supervisor and his infidelity. The company hears rumors of this text and eventually acquires a copy. While the employee's comments are still relatively private, she has cast the company in a bad light, in writing, and to a much wider audience. The company now has a strong desire to discipline the employee, and she has an equally strong desire to sue them for invading her privacy – arguing that reviewing her confidential text messages is an invasion of privacy. As explained below, the United States Supreme Court has recently addressed this very issue.

Finally, imagine the woman returns from work and posts her thoughts as a status update on MySpace or Facebook, or "tweets" it via Twitter, and the entire free world suddenly believes that her boss is a sexual predator and the company knowingly permits his conduct at work. In so doing, she has aired the company's dirty laundry to anyone with an Internet connection and potentially subjected it to fall out from her supervisor, his spouse, his boss, customers, investors, and others. The company wants to terminate her for what she's done, but it's not sure if she has the right to print whatever she wants on her MySpace page, especially if there's some truth to it. Can the company terminate her? Unfortunately for employers, this question has been answered in a variety of ways by courts throughout the country. What follows is a summary of a few of those rulings and some guidelines for employers to follow.

II. SOCIAL MEDIA AND EMPLOYEE PRIVACY

A. Does An Employee Have A Right Of Privacy In Personal Text Messages Sent From A Company Cell Phone?

The issue of electronic workplace privacy has made its way to the United States Supreme Court in *City of Ontario v. Quon*, a case involving an employer's monitoring of employee text messages sent via employer-issued equipment. The City of Ontario provided certain employees with pagers that could be used for sending text messages, and paid the associated wireless

service fees. The wireless plan included a 25,000 character per-month limit, after which overage charges were assessed. Quon, a police sergeant and SWAT team member, received one such pager.

Quon's problems began when he exceeded the City's monthly text messages limit for a few months. Each time, he personally paid the overage charges that were assessed by the wireless service provider, and no further action was taken by the City. After a while, however, Quon's lieutenant got tired of being a bill collector, and decided to order transcripts of the text messages "for auditing." This audit was supposed to serve two related purposes: first, to see whether the City's character limit needed to be extended, and second, to see whether Quon was wasting time texting when he should have been working.

From the audit, the City learned that the reason behind Quon's inability to stay within the character limitation: in addition to his work-related texts, he was also sending sexually explicit texts to not one, but two women. One was his wife, another Ontario police officer; the other was his mistress, who worked as a dispatcher for the City. As a result, the City exposed Quon's intra-workplace, extramarital affair, and Quon, his wife, and his paramour all sued the City of Ontario in federal court, asserting that their privacy rights were violated by the City's inspection of the text messages.

In general, in order for an individual to successfully demonstrate that their constitutional right to privacy has been violated, they must establish three elements. First, the person must identify a specific, legally-protected ***privacy interest***. In other words, a plaintiff must show that they had an expectation of a right to privacy under the circumstances. Second, the court must determine that that expectation was ***reasonable*** – again, considering all relevant facts, circumstances, and customs. Third, the court inquires into the ***seriousness*** of the invasion of privacy – specifically, whether it was of a "nature, scope, and actual or potential impact [as] to constitute an egregious breach of the social norms." Thus, not every invasion of privacy is actionable; instead, only those that are unreasonable under the circumstances give rise to a cause of action. This inquiry is sometimes expressed as a two-part test: whether (i) there is a reasonable expectation of privacy, and (ii) whether it was unreasonably intruded upon.

In *Quon*, the City argued that Quon could not establish a "reasonable" expectation of privacy in his texts, because its written policies asserted a right to review or monitor any messages sent on City equipment. Although there was no policy specific to the pagers, the City's general "Computer Usage, Internet and E-mail policy" stated that the City could and would monitor all activity without notice, and warned that "[u]sers should have no expectation of privacy or confidentiality when using these resources."

Quon countered, arguing that regardless of the *written* policies, the City had an informal policy whereby the texts would remain unread so long as the user personally paid the overages. The District Court agreed, found that the informal policy trumped the written language, and held that Quon had a reasonable expectation of privacy in his text messages as a matter of law. However, the jury decided that the investigation into Quon's text messages was not unreasonable in scope, and therefore absolved the City of liability for the search.

Quon and others appealed the decision to the Ninth Circuit Court of Appeals, which reversed the District Court. The Ninth Circuit agreed that Quon had a reasonable expectation of privacy in his texts, which was justified by the City's informal policy of not auditing text messages so long as the overages were paid. However, the Ninth Circuit held that the City's audit constituted an unreasonable intrusion into Quon's privacy, commenting that "[t]here were a host of simple ways to verify the efficacy of the 25,000 character limit . . . without intruding on" Quon's privacy rights. The case was appealed again, to the U.S. Supreme Court.

The Supreme Court expressly ducked the issue of whether Quon had a reasonable expectation of privacy in his texts. Instead, it assumed that he had such an expectation, and moved on to whether the City's search of the text messages was reasonable. The Supreme Court held that it was.

In ruling that the City's review of Quon's text messages constituted a "reasonable" search, the Court first reasoned that the City had a legitimate, non-investigatory reason for the search: namely, to determine whether the overages were due to work-related or personal messages. The City needed this information to determine if the cellular plan was sufficient to meet City employee needs, or rather whether employees were being forced to pay overages for work-related texts.

The Court then noted that the City's review of the text message transcripts was an efficient and expedient way to conduct the search. Moreover, the search was limited to only two months worth of texts, and the City only reviewed texts sent while Quon was on duty. The Court also reasoned that whatever expectation of privacy it assumed Quon to have would be a limited one. As a SWAT team member and police officer, Quon should have understood that the City might need to audit or review his text messages.

Finally, and perhaps most importantly for employers, the court concluded that the search would have been "reasonable and normal in the private-employer context." Thus, while the court earlier indicated a willingness to confine this case to its facts, it specifically broadened the scope of its ruling by expanding the facts and holding of *Quon* to the private sector.

For employers, there are several key lessons to be learned from *Quon*. First, the court repeatedly referenced the city's "Computer Usage, Internet and E-Mail Policy," which clearly indicated that all e-mail and network activity was subject to monitoring without notice. Although this policy did not specifically apply to text messages, at a subsequent meeting the city made it clear to Quon and others that texts were considered e-mails, and thus fall under the same policy.

The importance of an Internet usage policy that is both specific and flexible cannot be overstated. The policy should make clear that all communications undertaken on company time and company equipment are subject to being monitored. The policy must also be flexible enough to apply to all forms of ever-changing technology, from computers to cell phones, and from texts to tweets. It must also be unwaveringly enforced by all supervisors and management-level personnel.

Second, any monitoring undertaken by employers should be conducted with a minimum of invasiveness. Simply monitoring an employee's on-duty e-mails or texts may be considered reasonable, but entering a private chat room or monitoring an employee's off duty private texts is an entirely different, and riskier, endeavor. It is only of limited defense that the equipment was provided by the employer. In fact, the New Jersey Supreme Court recently concluded that an employer violated a former employee's privacy rights by reading emails that the employee sent *from a company laptop* – even though the company's written policy warned that computer resources, including emails, were not confidential and could be read by the company. As such, care should always be taken in this area.

B. Can An Employer Terminate An Employee Based On Comments Found On A Social Media Website?

For many employers, the prevalence of social media represents an easy, fairly untraceable method by which to check up on applicants or employees. However, employees' use of social media websites – even during their own, off-duty time – potentially raises many of the same legal issues embraced by the facts of *Quon*. While published case law is scarce, it takes little imagination to see that employers risk potential privacy violations by making employment decisions based in whole or in part on online postings.

For example, the Houston's restaurant chain was sued after it fired a couple employees based on statements they discovered in a private MySpace chat group. In that case, a Houston's server formed a MySpace group for the purpose of "vent[ing] about any BS we deal with [at] work without any outside eyes spying in on us." The group was created in such a way that it was private and password-protected, and could only be accessed by those who were invited. A number of past and present Houston's employees subsequently joined the group. The employees used the forum to make sexual remarks about Houston's management and customers; make jokes about Houston's "core values;" share a copy of the new wine test to be given to servers; and otherwise keep a running commentary about working at the restaurant.

Problems predictably arose when a member of Houston's management gained access to the forum and saw the unsavory and inappropriate remarks that had been posted. How this manager was able to access the site is one of the main disputes in the case – the manager said that an employee voluntarily gave him the password, while the employee claimed that the password was coerced out of her by management. What *is* certain is that the retribution for the comments was swift. Pages of the forum commentary were printed and circulated to senior management and human resources, and a number of the employees who were responsible for the postings were terminated.

The terminated employees then sued Houston's, bringing a claim for invasion of privacy as well as various other causes of action. Houston's moved for summary judgment on the privacy claim, arguing that there could be no "reasonable" expectation of privacy in messages that were intentionally posted in an online messaging forum. The court denied Houston's motion, however, and found instead that the "invitation only" aspect of the discussion board

supported the view that the plaintiff's expectation of privacy was reasonable. According to the court, "reasonableness" is a fact question better left for the jury to decide.

From a business perspective, the Houston's case simply confirms that privacy litigation is unpredictable and expensive. Even if company management gains access from employees who "voluntarily" or "willingly" provide a password, the company cannot be certain that this access will not later be cast as unauthorized or coerced. On the other hand, some California courts have held that information posted on a fully-public, non-exclusive website can waive any argument that the poster had an expectation of privacy in their posting. Thus, employers should use particular care in accessing online media that is not available for all the world to see – including Facebook pages, private MySpace accounts, and other similar sites.

III. THE POTENTIAL PITFALLS OF BASING EMPLOYMENT DECISIONS ON ON-LINE POSTINGS

The use of social media to make employment decisions can potentially give rise to claims of other unlawful conduct, such as discrimination or harassment. While many employers run Google or other Internet searches on prospective employees, such actions can give rise to an argument that the decision was based on facts that cannot legally be considered.

For example, say a particular employer is hiring, and has received a stack of résumés from qualified applicants. Suppose that this employer runs a Google search on each two equally-qualified applicants after interviewing both, in an effort to decide between the two. Via this informal "research," the employer learns from pictures on MySpace or Facebook that one of the applicants is homosexual. Although both applicants are equally qualified, the employer decides that it would rather not hire the homosexual applicant because he or she would not be a good "fit" for the company.

The employer in this example has just opened itself up for a discrimination claim. Even if the company can articulate other legitimate bases for its decision, there is always a chance that a jury will latch onto the "MySpace" investigation as having provided the employer's true motivation. When it comes to the Internet – for employers as much as for individual users – there are just some things that you can't un-see.

As paranoid as this must sound, there are cases to support the concerns. For example, a North Carolina school district was sued after it terminated one of its employees for damaging his position as a "role model" in "the school community." The district claimed that the "damage" was caused by the plaintiff's MySpace account, where he revealed himself as a follower of the Wiccan religion, and his wife as a bisexual. Although the plaintiff's claims failed, the employer's victory was presumably an expensive one, thus causing one to question the wisdom of the employer's decision to act on the MySpace posting.

In another case, a firefighter sued for gender and racial discrimination and retaliation after she was terminated following an investigation involving photos posted on her MySpace account. Tiffany Marshall posted photographs of herself and fellow firefighters in uniform, as

well as some personal modeling photos in which Marshall was scantily clad. The fire department received an anonymous phone call notifying them that the photos on Marshall's MySpace account "'may conflict' with the way Savannah Fire wanted to be portrayed." After viewing the MySpace page, the department disciplined Marshall. The disciplinary meeting was somewhat heated, and Marshall was terminated shortly afterwards, purportedly for her disrespectful and insubordinate reaction to being disciplined. Again, while the employer ultimately prevailed, the case dragged on for nearly three years – all the way to the Eleventh Circuit Court of Appeals – before that result was obtained.

Finally, in perhaps the most entertaining case regarding social media, a former Starbucks barista filed a claim for religious discrimination based on the employer's supposed misconstruing of the plaintiff's MySpace page. The plaintiff, Nguyen, had been exhibiting strange behavior at work for some time by, for example, providing advice to a female employee about "how much money she could charge for various sex acts if the co-worker ever decided to become a prostitute." Nguyen later took a leave of absence – via a letter addressed, "Dear Mr. Starbucks" – that stated she would "rather be saving da world via a porn-star instead of working as a barista." Shortly thereafter, other Starbucks employees made management aware of Nguyen's Myspace website, on which she posted the following comment (quoted with original spelling and punctuation):

> Starbucks is in deep [expletive] with GOD!! I am now completely disenchanted with humans n I have NO MO Energy left 2 deal w/ their negativety . . . I thank GOD 4 pot 2 calm down my frustrations n worries or else I will go beserk n shoot everyone . . . I will not be happy unless I win because I AM GOD N GOD DON'T LOSE.

Understandably, the Starbucks employees felt threatened, and the police were called in to ensure that no threats were carried out. Starbucks also made the not-so-difficult decision to terminate Nguyen's employment. Nguyen responded by filing a lawsuit in federal court, alleging that the "real" reason she was terminated was because of the religious beliefs she espoused on her MySpace page. Starbucks prevailed after more than a year and a half of litigation.

As each of these cases make clear, an employer's review of employee social media postings can lay the foundation for claims of harassment, discrimination, and retaliation. And because of the fact-intensive nature of the claims, even those arguments that turn out to be meritless must be thoroughly investigated at considerable time and expense. Employers may be better served by not opening the door to such litigation by steering clear of employee social media sites altogether.

IV. CONCLUSION

Although privacy in the workplace is by no means a new issue, thorny issues arise when aspects of the present-day online lifestyle interact with well-entrenched workplace rights. Sites

such as Facebook, Myspace, and Twitter have dramatically altered the amount of information employers can learn about current and prospective employees. Facebook alone boasts that more than 5 *billion* items of content – pictures, videos, and blog entries – are uploaded *each month*. The Supreme Court made special mention of this new reality in its *Quon* opinion, stating that when attempting to describe privacy notions in relation to new technology,

> [i]t is not so clear that courts at present are on so sure a ground. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

Like the employers trying to wade through this information, the courts are struggling with trying to apply Old World concepts such as privacy rights to a Twitter world. What is clear is that the areas in which an employer can run into new-technology trouble are many. As such, a clearly-defined policy – faithfully implemented and consistently applied – is a baseline necessity for any business. For those employers who choose to peruse the Internet in search of information on their employees, remember the words of Oscar Wilde, who cautioned that when the gods want to punish us, they answer our prayers. In other words, be careful what you look for, and even more careful with what you find.

Jeffrey Wertheimer is a Partner in the Employment and Labor Department of Rutan & Tucker, LLP, where he draws on more than two decades of litigation and counseling experience to protect business and employer interests. Mr. Wertheimer has successfully defended clients in a variety of employment matters, including class action and multi-plaintiff wage and hour, harassment, disability discrimination, retaliation, wrongful termination, and breach of contract claims. Mr. Wertheimer may be contacted at jwertheimer@rutan.com.

Brandon Sylvia is an Associate in the Employment and Labor Department of Rutan & Tucker, LLP. Mr. Sylvia's practice involves representing employers in a broad range of employment-related litigation, including wage-and-hour class action disputes, trade secret litigation, and retaliation, harassment, and discrimination claims. Mr. Sylvia may be contacted at bsylvia@rutan.com.