PEPPERDINE UNIVERSITY

The Journal of Business, Entrepreneurship & the Law

Volume 4 | Issue 2 Article 7

4-20-2011

Managing the Impact of New Media on the Employment Relationship

Susan A. O'Sullivan-Gavin

John H. Shannon

MANAGING THE IMPACT OF NEW MEDIA ON THE EMPLOYMENT RELATIONSHIP

SUSAN A. O'SULLIVAN-GAVIN*

JOHN H. SHANNON+

INTRODUCTION

Attention to privacy issues in the workplace has increased over the past two decades as use of electronic mail and text messages has made these means of communication commonplace. Beyond text messages and emails, employees can access the internet at their place of employment at many different entry points. This access can be through company issued desktops or laptops, mobile phones, mobile internet devices (MIDs), Smartphone technology (photography; video and voice recording capabilities; file transfer and storage), off-site internet connections, Wi-Fi access or hot spots. Employees can access and/or post information on various sites including blogs, wikis, RSS feeds, instant messaging (IM's), e-newsletters, Twitter (micro-blogging), YouTube, Facebook, cloud computing, podcasting, tagging, and Web 2.0 tools. These are all forms of "new media" or the new communication tools that are sweeping the employment world.

What information is derived via New Media, what is discoverable and what is the impact on the employment relationship? How does developing case law affect this relationship? Employers and businesses that do not understand the importance and ramifications of these new communication tools may find that they

* Assistant Professor, Legal Studies, Rider University, Lawrenceville, New Jersey.
+ Associate Professor, Legal Studies, Seton Hall University, South Orange, New Jersey.

have inadvertently opened the door to litigation and liability, or loss of profit and/or loss of competitive advantage.[1] Companies also increase their risk of exposure to spam, phishing or malware attacks; risk loss of proprietary information, sensitive data and proprietary information.[2] This paper examines how the employment relationship is impacted by "new media" given current social research and developing federal and state case law, including *City of Ontario, California v. Quon*,[3] *O'Connor v. Ortega*,[4] and *Stengart v. Loving Care Agency*.[5]

WHAT IS REVEALED?

Have you "Googled" yourself recently? Results can show personal information, likes or dislikes, hobbies, interests, photos, professional associations, employment history, education history, publications, presentations and organizational memberships.[6] There are also web sites that aggregate information on individuals in order to identify on-line presence.[7] On the corporate level, searchers can discover corporate intranet sites as well as companies' consumer-directed Web sites.[8] Many employers utilize new media or hire a search company in order to obtain background information on present and potential employees.[9]

---

[1] *Two Thirds of Businesses Fear that Social Networking Endangers Corporate Security, Sophos Research Reveals, Press Office*, SOPHOS, (Apr. 28, 2009), *available at* http://www.sophos.com/press office/news/articles/2009/04/social-networking.html [hereinafter SOPHOS].

[2] *Id.*

[3] City of Ontario, California v. Quon, 130 S. Ct. 2619 (2010); Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) *reh'g denied*, 554 F.3d 769 (9th Cir. 2009).

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

[5] Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010).

[6] *You Are What You Post*, BLOOMBERG BUSINESSWEEK, Mar. 27, 2006, *available at* http://www.businessweek. com/magazine/content/06_13/b3977071.htm [hereinafter *You Are What You Post*].

> You are what you post because today, there are two of you. There's the analog, warm-blooded version: the person who presses flesh at business conferences and interprets the corporate kabuki in meetings. Then there's the online you, your digital doppelganger; that's the one that is growing larger and more impossible to control every day. Because anyone, anywhere, at any time can say anything about you on the Web, reputations are scarily open-source. And because entire companies dedicate themselves to recording every inch of information on the Web, it's becoming difficult to unplug from the Google matrix, let alone make anything on the Internet go away.

Id.

[7] *See* Flowtown, http://www.flowtown.com (last visited Mar. 13, 2011). "When all you have is an email address, Flowtown can give you a name, age, gender, occupation, location, and all the social networks that person is on.;" *see also* Scott Scanlon, *6 Tools for the New Media Marketer*, YOUBRANDINC (May 18, 2010), *available at* http://www.youbrandinc.com/new-media-tools/6-tools-for-the-new-media-marketer/.

[8] *You Are What You Post*, *supra* note 6.

[9] *Id.* Googling people is also becoming a way for bosses and headhunters to do continuous and stealthy background checks on employees, no disclosure required. Google is an end run around discrimination laws, inasmuch as employers can find out all manner of information – some of it for a nominal fee – that is legally off limits in interviews such as your age, your marital status, the value of your house (along with an aerial photograph of it), the average net worth of your neighbors, fraternity pranks, stuff you wrote in college, liens, bankruptcies, political affiliations, and the names and ages of your children. *Id.* "Employees who are recent graduates often retain their college e-mail addresses, which enables them to see pages. Sometimes, too, companies ask college students working as interns to

Companies also use new media to obtain market information for new products and services, survey the public as to general attitudes and expectations, and to plan for future growth and expansion.[10]

Management of new media tools can be an asset or a liability for both the employer and the employee depending upon how these tools are used and how a company controls or limits their applicability in the workplace. New media and its effects can disrupt rights and expectations in the modern employment relationship. Disruption, as defined by Larry Downes, indicates that while "technology changes exponentially . . . social, economic and legal systems change incrementally."[11] Without question, we all face challenges in our personal and employment lives that result from the very real effects of new media and its resultant "disruption." It is evident that our analog and digital personas are increasingly merging.[12] As early as 2006, the discussion of the physical, i.e., analog, person's "digital doppelganger" was already identified.[13] The integration of analog and digital, in both personal and professional lives, affects employment relationships in numerous unknown ways and will continue to create on-going challenges for employers.[14] As new media increases in sophistication and ease of use, the average user will be able to continue to blur the distinction between their analog and their digital existence.

When creating a plan to manage these new media tools, a company will also need to factor in a new reality, that no matter the form of the media, information posted on the World Wide Web is now archived in perpetuity. David Kesmodel, in the *Wall Street Journal*, noted in 2005 that:

> The Web, seemingly one of the most ephemeral of media, is instead starting to leave permanent records. Through the Wayback Machine, and similar services offered by companies such as Google Inc., it's now easy to retrieve all kinds of online material, from defunct Web pages to old versions of sites.
>
> . . .

---

perform online background checks," said Patricia Rose, the director of career services at the University of Pennsylvania. Alan Finder, *When a Risqué Online Persona Undermines a Chance for a Job*, N.Y. TIMES, June 11, 2006, *available at* http://query.nytimes.com/gst/fullpage.html?res=9C0DE3D61231F932A25 755C0A9609C8B63&pagewanted=all.

[10] *See Facebook Unveils Privacy Changes*, CNN, Dec. 10, 2009, http://articles.cnn.com/2009-12-10/tech/facebook.privacy_1_privacy-settings-facebook-social-networking-site?_s=PM:TECH. The December 2009 controversy over changes to Facebook's privacy controls was based on allowing third parties to gather information for products and services. "If a user retains the 'Everyone' option, the information is accessible by the Web at large." *Id.* In short, this is Facebook's answer to Twitter, leveraging real-time search information and syndicating it to other places, like Google and Bing. *Id.* The feature has been available in the site's privacy settings since last summer, but most people didn't use it (and probably didn't even know it was there). The new privacy launch today puts this as the default option for many users. *See Id.* In June 2010, in response to a global outcry, Facebook again changed their privacy controls to make it easier for users to control what information was being made available, although critics do not believe that Facebook has gone far enough to protect user's privacy. Ben Worthen, *Facebook's Settings Don't Quell Critics*, WALL ST. J., May 27, 2010, at B1.

[11] LARRY DOWNES, THE LAWS OF DISRUPTION: HARNESSING THE NEW FORCES THAT GOVERN LIFE AND BUSINESS IN THE DIGITAL AGE 2, 17 (2009).

[12] *You Are What You Post*, *supra* note 6.

[13] *Id.*

[14] Sophos Press Release, *supra* note 1.

> The Wayback Machine (www.waybackmachine.com) is run by the Internet Archive, a nonprofit group started in 1996 to build a massive digital repository of cultural artifacts, including old TV shows, books and live music recordings. This free service, named for the time-travel device in the "Rocky and Bullwinkle" cartoons, searches for specific Web addresses and pulls up multiple versions, sometimes dating back years. The Wayback Machine has archived 40 billion Web pages using computer programs, known as "bots," that crawl the Internet and make electronic copies of information they come across. Google also has a system in place to store internet postings. Google's system, known as Google Cache – 'cache' is a computer term for a place where information is stored – works in a similar way, although its archive is less extensive. On Google's results page, users can click on a link to see how sites look whenever Google last indexed them, something it does often.[15]

Sometimes information can be removed from the archive, but generally that would only happen if the information contained some type of personal information.[16] Website administrators who do not want their information archived, can insert computer code to block access to the Wayback Machine and other search engines.[17]

This archived information can aid in the discovery process in various types of corporate litigation[18] such as domain name battles, trademark protection, copyright protection, partnership disputes, ownership contests, and shareholder cases.[19] Other forms of litigation also benefit from information obtained from archived files: personal litigation (family law disputes in divorces and child custody cases), tax cases, cases involving receipt of government benefits

---

[15] David Kesmodel, *Lawyers' Delight: Old Web Material Doesn't Disappear*, WALL ST. J., July 27, 2005, at A1.

[16] *Id.*

> Neither archive is exhaustive. Individual Web-site [sic] operators can ask the Wayback Machine and Google to remove pages. Both services say they'll comply if the person making the request demonstrates they have authority over the Web site [sic] in question. In the wake of the Sept. 11, 2001, terrorist attacks, for example, the Nuclear Regulatory Commission asked Google to take certain Web pages [sic] out of its cache.

Id. "Requests from third parties to remove information are generally denied. The Wayback Machine makes exceptions in certain circumstances, for example if the Web pages [sic] contain personal information provided in confidence, such as medical data." *Id.*

[17] *Id.* "In addition, Web-site [sic] operators can prevent material from remaining in the public domain by using a piece of computer code, known as a robots.txt file, which stops bots belonging to the Wayback Machine and regular search engines from copying pages." *Id.*

[18] *Id.*

> The archive tools provide lawyers with a quick and inexpensive way to unearth evidence that otherwise might not be available. Lawyers have always been able to seek copies of old Web pages [sic] in a pretrial phase known as discovery. But some parties might not save every version of their Web sites [sic] and others might routinely get rid of stored pages. Meanwhile, in domain-name disputes handled by arbitrators, there's no discovery process. Allison McDade, counsel for trademarks and copyrights at Dell, of Round Rock, Texas, says the company frequently uses the Wayback Machine and other computerized tools to protect its trademarks online, as it did in its dispute with Innervision.

Id.

[19] Jennifer L. Nelson, *Social Media*, N.J. BUS., Dec. 4, 2009, at 60-61.

(unemployment insurance, workers compensation),[20] tax cases and tort cases,[21] to name a few. As a result, companies must assess their current policies and procedures in light of how new media can impact their relationship with their employees and the extent of exposure the company will face if litigation ensues due to a poorly drafted or conveyed new media policy.[22]

IMPACT ON EMPLOYERS

The use of new media by both the employer and the company's employees, "may amplify a businesses' exposure to potential liabilities such as harassment, defamation,[23] copyright infringement, and privacy violations."[24] Companies also open the door to law suits for breach of contract, contractual interference, breach of non-competition agreement,[25] loss of opportunity, breach of corporate security, breach of the duty of loyalty, breach of fiduciary relationship,[26] shareholders suits, life style discrimination,[27] and, for companies that do business in Canada, an

---

[20] Kathryn Leger, *(Canada) Woman's Disability Payments Cutoff b/c of Facebook*, THE GAZETTE (Montreal), Nov. 27, 2009, at B3. On November 27, 2009, The Gazette (Montreal) reported that a woman's disability payments were terminated due to posts to her Facebook account:

> The viewing of personal information on Facebook and other online social networks by third parties such as employers, insurers, job recruiters, advertisers or spoilers is growing and raising legal questions about privacy protocols and to what extent images or other personal information posted on privately managed online sites can be relied upon to determine the validity of insurance or medical leave claims . . . . If [insurance companies] suspect that the beneficiaries are cheating on them or not telling the truth, they have a right to investigate and Facebook can be a trigger.

Id. Lavin added, "[w]here we are strongly opposed is that we don't believe that they can just on that basis [of Facebook photos] cut off her benefits." *Id.*

[21] *See* Karen Sloan, *Dismissal in Early Test of Twitter Libel Liability*, NAT'L L.J., Jan. 25, 2010, http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202439486524&slreturn=1&hbxlogin=1 (discussing a defamation suit based upon "tweets" posted on Twitter).

[22] Sophos Press Release, *supra* note 1.

[23] *Id.*

[24] *Workers Liable to Reveal All to Network Sites*, BUS. INS., Aug. 31, 2009, *available at* http://www.business insurance.com/article/20090830/ISSUE0504/308309990 (citing Kathy Swendsen, President of Travelers global technology unit) [hereinafter BUS. INS.].

[25] *See* Sloan, *supra* note 21 (discussing a noncompete case involving solicitation of employees via Twitter).

[26] *Id.*

[27] *See* Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24 BERKELEY J. EMP. & LAB. L. 377, 381 (2003):

> More generally, the question is: should employer interests always trump the employee's privacy interests? Or, put the other way around and more precisely, should society intervene, and if so, when and through what legal mechanisms, to preclude employers from making hiring, promotion, discharge, discipline and other job decisions based on off-the-job conduct?

Id.

> The third state that perhaps belongs in this category is New York, which enacted a wide-ranging lifestyle discrimination statute that lists four broad categories of off-duty conduct that employers generally may not use in making employment decisions. They are: legal recreational activities, consumption of legal products, political activities, and membership in a union.

Id. at 417.

expansion of the relationship between employer and employee resulting in potential civil liability.[28] Other external factors that can negatively affect productivity are malware and spyware.[29] Potentially, companies also face allegations of violations of parallel federal and state Wiretap Acts,[30] parallel federal and state Stored Communications Acts (the "SCA"),[31] and claims of wrongful termination in violation of a clear mandate of public policy.[32]

Additionally, there is risk to a company's reputation and good will could have a domino effect resulting in lost market position, profit, and market value.[33] A company also loses time and money in litigation to protect a domain name, trademark, copyright, or other proprietary information. In some cases, if the issue begins as an internal dispute between employees and then becomes known externally, there could be a loss of faith in the company.

In 2009, Deloitte LLP published an Ethics & Workplace Survey (Social Networking and Reputational Risk in the Workplace).[34] The Deloitte survey asked 2,000 working adults and 500 business executives about the privacy of online activity, its potential effect on employers, and the rights of employers to monitor their employees' social networking sites.[35] "The results of this study are eye-opening and clearly underscore the need for businesses to educate themselves and address the issues that can arise as a result of their employees' use of online social

---

[28] In Canada, a proposed amendment to the Occupational Safety and Health Administration ("OSHA") statute would require employers who find out about or suspect domestic violence is happening to an employee to intervene via human resource department and to train all employees in recognition and reporting of domestic violence. Howard Levitt, *When Push Comes to Legal Shove: Employer Asked to deal With Domestic Discord*, FIN. POST, Dec. 2, 2009, *available at* http://www2.canada.com/ story.html?id=2292839.

[29] Sophos Press Release, *supra* note 1.

> We're seeing more incidents of unwanted adverts and malicious links being spammed out, particularly to Facebook users, from their friends' compromised accounts, continued Cluley. Although social networking sites are going some way to mitigate threats to users – activating pop-up windows to confirm if a user really wants to visit that external link for example – unfortunately it's just not enough. Organizations need to incorporate defenses into their IT security policy, and a key part of this is to educate individuals to choose strong passwords and to take good care of them to prevent cybercriminals from taking over online accounts which could provide an entry point to the IT infrastructure.

Id. Sophos's research confirms that, "although one-third of organizations still consider productivity issues to be the major reason for controlling employee access to social networking sites, the threat from both malware and data leakage is becoming more apparent with one in five citing these as their top concerns." *Id.*

[30] Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §§ 2510-22 (1986).

[31] Unlawful Access to Stored Communications, 18 U.S.C. §§2701-11 (1986).

[32] *See* Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2008 U.S. Dist. LEXIS 108834 (D.N.J. July 25, 2008) [hereinafter *Pietrylo* I]; Pietrylo v. Hillstone Rest. Group, No. 06-5754, 2009 U.S. Dist. LEXIS 88702 (D.N.J. Sept. 25, 2009) [hereinafter *Pietrylo* II].

[33] Deloitte LLP, *2009 Ethics & Workplace Survey Results: Social Networking and Reputational Risk in the Workplace, Deloitte LLP 2009 Ethics & Workplace Survey*, http://www.deloitte.com/ assets/DcomUnitedStates/Local%20Assets/Documents/us_2009_ethics_workplace_survey_220509.pdf.

[34] *Managing the Web 2.0: Issues Facing Companies As A Result of Employees' Online Social Networking and Blogging*, BUS. TIMES (SING.), Oct. 19, 2009, at BTC [hereinafter *Web 2.0*].

[35] *Id.*

networking sites, blogs and other 'Web 2.0' applications."[36] The survey findings include:

"Deloitte LLP's 2009 Ethics & Workplace Survey shows that there is great reputational risk associated with social networking as 74% of employed Americans surveyed believe it is easy to damage a brand's reputation via sites such as Facebook, Twitter, and YouTube."[37]

"[S]urprisingly only 15% of executives surveyed are addressing these risks in the board room, though 58% agree it is important enough to do so. Moreover, a mere 17% have programs in place to monitor and mitigate the potential reputational risks related to the use of social networks."[38]

> As this medium is evolving, there are different opinions about use and access. Sixty percent of business executives say they have the 'right to know' how employees portray themselves and their organizations online, while 53% of the employees contend that 'social networking pages are none of an employer's business.' In fact, nearly one third of employed respondents say they never consider what the boss would think before posting materials online.[39]

"Twenty-seven percent of employees surveyed don't consider the ethical consequences of posting comments, photos, or videos online – and more than one-third don't consider their boss, their colleagues, or their clients."[40]

"Fifty-six percent of business executive respondents say that using social networking sites helps their employees achieve better work-life balance, but only 31% of the employee respondents agree."[41]

"Fifty-five percent of executives say their companies don't have an official use of social networks, and 22% said their companies would like to use social networking tools, but haven't yet figured out how."[42]

When asked if they were worried that employees were sharing too much personal information on social networking sites, 62.8% of employers responded, "yes."[43]

Asked if they thought employees' activities on social networking sites could endanger security at the company, 66% of employers said, "yes."[44]

60% of business executives say they have the "right to know" how employees portray themselves and their organizations online.[45]

53% of the employees contend "social networking pages are none of an employer's business."[46]

---

[36] *Id.*

[37] Deloitte LLP Survey, *supra* note 33.

[38] *Id.*

[39] *Id.*

[40] *Id.* at 8.

[41] *Id.* at 9.

[42] *Id.* at 13.

[43] Deloitte LLP Survey, *supra* note 33.

[44] *Id.*

[45] *Id.* at 2.

[46] *Id.*

In another recent survey, IT security and control firm, Sophos, revealed:

> [Sixty-three] percent of system administrators worry that employees share too much personal information via their social networking profiles, putting their corporate infrastructure – and the sensitive data stored on it – at risk. The findings also indicate that a quarter of businesses have been the victim of spam, phishing or malware attacks via sites like Twitter, Facebook, LinkedIn and MySpace.[47]

Often, "paranoia over privacy concerns can inhibit some employers from instituting practices and procedures that would greatly benefit their companies."[48] Companies (or enterprises) that could benefit from utilizing new media and search engines to gather information often fail to do so. According to InformationWeek Analytics Enterprise Search Survey of 552 business technology professionals, "not even one in four organizations uses any type of enterprise search system today."[49] The survey asked how respondents who've adopted enterprise search are using their systems, and whether they "provide a unified search capability across network shares, databases, applications, intranets, SharePoint, and desktops, plus consolidation of Web browsing.[50] "Of the 24% who've deployed enterprise search, less than 8% provide hooks into multiple silos. That's not quite 2% of the total."[51] Healy states:

> The problem isn't technology. It's the three Ps that plague many an IT initiative: politics, privacy, and perception . . . E-mail search is one of the most politically charged areas CIOs will encounter. Almost every organization's official policy is that e-mail is owned by the company and employees have no expectation of privacy, yet almost every survey respondent limited e-mail search to the individual level, with only 3% allowing search within departments or teams.[52]

Although the capability exists for employers to capture information and to plan for its use, the majority of modern companies have failed to grasp that the issues presented by new media have to be viewed in their entirety in order to arrive at solutions that benefit both employer and employee.

Even the federal government, in its capacity as an employer, had to adopt an email privacy policy.[53] In particular, the Government's policy states that employees logging on to their computers (at work) have "no reasonable expectation of privacy" while using the network.[54] "By notifying government employees logging on to their computers that they have 'no reasonable expectation of privacy' while using the network, the government's Einstein 2 program is

---

[47] Sophos Press Release, *supra* note 1.

[48] Michael Healy, *InformationWeek Analytic Research: Federated Search*, INFORMATIONWEEK, Nov. 9, 2009, *available at* http://www.informationweek.com/news/internet/search/showArticle.jhtml?articleID=221600491.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] Ellen Nakashima, *Cybersecurity Plan Doesn't Breach Employee Privacy, Administration Says*, WASHINGTON POST, Sept. 19, 2009, at A16, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/09/18/AR2009091804147.html.

[54] *Id.*

lawful," according to an August 14, 2009 U.S. Justice Department memo.[55] The policy also applies to private citizens who send e-mails to a government employee – even to the employee's private account if he or she opens it at work.[56] According to David J. Barron, acting assistant attorney general for the Office of Legal Counsel, "'A person communicating with another assumes the risk that the person has agreed to permit the Government to monitor the contents of that communication' . . . alluding to the "one-party consent" rule set out in the Wiretap Act of 1968."[57]

The positive impact of new media is not to be ignored. There are many advantages to employers who assess the use and exposure of new media within their workplace and beyond the traditional brick and mortar of their establishments. These include enhanced employee productivity, marketing communications, strategies, campaigns through social networking and "tweets" via Twitter, increased brand recognition, loyalty, and consumer trust, and product development leads from customer suggestions and criticisms.[58]

IMPACT ON EMPLOYEES

A national survey, sponsored by Deloitte LLP, of employees who use new media found that 27% of employees surveyed do not consider the ethical consequences of posting comments, photos, or videos online.[59] More than one third of employees do not consider their boss, their colleagues, or their clients when posting on the Internet.[60] Yet, in the same survey, when employees were asked: "The economy is forcing you to be much more conservative online, as you fear that your employer can use anything and everything as an excuse to fire you." Twenty-nine percent responded that was true.[61] The survey also found that 56% of business executive respondents believe that using social networking sites helps their employees achieve better work-life balance, whereas only 31% of the employee respondents agreed.[62]

This disconnect is related to the perception of how new media is used by the employee.[63] If users perceive new media as something they do in private, that is unrelated to the workplace, and employers are beginning to view new media as a risk that needs to be regulated, then it will be up to employers to educate their employees about policies and procedures.[64] Employees might not take the time to consider that a post to a blog or a social network could harm the reputation of the

---

[55] *Id.*

[56] *Id.*

[57] *Id.*

[58] Jennifer L. Nelson, *Social Media*, N.J. BUS., Dec. 4, 2009, at 60-61.

[59] Deloitte LLP Survey, *supra* note 33.

[60] *Id.* at 8.

[61] *Id.* at 12.

[62] *Id.* at 9.

[63] *See* Travelers Enterprise Market Research, Social Media/ Networking Usage Trends Report (2009), http://www.travelers.com/iwcm/Trv/docs/Travelers_Social_Media_Report_082709.pdf (reviewing users' perceptions of new media).

[64] *Id.*

company or result in defamation litigation or a harassment complaint.[65] Pictures and posts of leisure activities that do not comport with the mission or vision of an employer could jeopardize a future employment opportunity. Future employees and students need to become savvy as to their new media use and the impact it has upon their job search. Job recruiters say students' lack of discretion online will catch up to them in their professional lives.[66] A 2005 study conducted by executive job-search agency ExecuNet found that 75% of recruiters already use Web searching as part of the applicant screening process.[67] More than a quarter of these same recruiters say they have eliminated candidates based on information they found online.[68]

Likewise, posts to blogs or micro-blogs like Twitter can also create future problems.[69] Archived information contained on personal blogs and social networking sites could reveal personal information that later in life an employee might not want an employer to know.[70]

This may not seem to be much of a problem, but Michelle Dennedy, chief privacy officer at Sun Microsystems, said it could matter a great deal.

> Imagine a day when a contentious topic of a Supreme Court nominee hearing is the content of the candidate's resurrected MySpace page, Flickr account and personal blog from her college days, or the log of phone calls and internet searches she made in the previous year, or a posted list of purchases made for a party.[71]

Given the difference in the perception of and the education about these issues, future and current employees need to be informed about corporate reputational risk, potential contract and tort litigation, threats to proprietary information and the expansion of the employment relationship into the digital world with the attendant rights and responsibilities of both employers and

---

[65] Thomas Parent, *The Past May Come Back to Haunt You*, S. CHINA MORNING POST, Apr. 29, 2008, at Supplements p.8.

> If you posted something on MySpace that came back to bite you years later then you made a mistake and you suffered the consequences. Live and learn. But what if you posted something on MySpace that included a friend of yours without getting their permission first and it came back to bite them. In America, you might get – and I dare say deserve – a lawsuit.

Id.

[66] *See You Are What You Post*, *supra* note 6.

[67] Jimmy Greenfield & David Haugh, *When What Happens on MySpace Doesn't Stay on MySpace*, CHI. TRIB., Mar. 28, 2006, at C1, *available at* http://articles.chicagotribune.com/2006-0328/news/0603280160_1_facebook-athletes-xanga.

[68] *Id.* Steven Rothberg, manager of the largest national employment website for recent university graduates, CollegeRecruiter.com, told the Columbia News Service: "I hope that students get a wake-up call . . . I think of social networking sites much like a tattoo: It seems like a great idea at the time, but you have to live with it the rest of your life." *Id.*

[69] *How Well Connected Are You?*, EXPRESS (UK 1. ED.), Feb. 6, 2009, at NEWS 40, *available at* http://www.express.co.uk/posts/view/83648/How-well-connected-are-you%3F/ ("[t]here are privacy issues as Twitter collects personally identifiable information about users, considers this an asset and reserves the right to sell it if the company changes hands").

[70] *See* Greenfield & Haugh, *supra* note 67 ("The world seems to be losing any sense of privacy it once had. Young people in particular seem completely oblivious to what they reveal on websites such as MySpace and Facebook.").

[71] *Id.*

employees.[72]

DEVELOPING CASE LAW

From *O'Connor v. Ortega* (1987)[73] to the most recent decision from the U.S. Supreme Court, *City of Ontario, California v. Quon* (2010),[74] developing case law addressing various forms of new media and its impact on the employment relationship have identified (1) the issue of whether or not the employee has an expectation of privacy and (2) whether or not the employer's search was in violation of the Fourth Amendment of the United States Constitution.[75] The developing law shows that the onus is on the employer to make clear the policies and procedures that apply to usage of new media within the office and outside of the office.[76] The burden then shifts to the employee to understand and acknowledge company policies and procedures.[77] Upon acknowledgement of the company's policies and procedures, the employee has notice that use of new media within the workplace or via employer issued equipment is subject to those policies and procedures.

O'Connor v. Ortega (1987)

In the *O'Connor v. Ortega* case, the defendant, Dr. Ortega was employed by a state hospital.[78] He was placed on administrative leave when questions arose regarding possible improprieties within the program that he supervised.[79] While he was on administrative leave, an investigation of the charges on impropriety was initiated.[80] During the investigation, Dr. Ortega's office was searched and items belonging to the state and several items of personal property belonging to Dr. Ortega were seized by hospital investigators.[81] Dr. Ortega claimed that his Fourth

---

[72] Sophos Press Release, *supra* note 1.

[73] *O'Connor*, 480 U.S. at 709.

[74] *Quon*, 130 S. Ct. at 2619.

[75] See *O'Connor*, 480 U.S. at 709.

[76] See *Quon*, 130 S. Ct. at 2619.

[77] *Id*.

[78] *See O'Connor*, 480 U.S. at 709.

[79] *Id.*

> In July 1981, Hospital officials, including Dr. Dennis O'Connor, the Executive Director of the Hospital, became concerned about possible improprieties in Dr. Ortega's management of the residency program. In particular, the Hospital officials were concerned with Dr. Ortega's acquisition of an Apple II computer for use in the residency program. The officials thought that Dr. Ortega may have misled Dr. O'Connor into believing that the computer had been donated, when in fact the computer had been financed by the possibly coerced contributions of residents. Additionally, the Hospital officials were concerned with charges that Dr. Ortega had sexually harassed two female Hospital employees, and had taken inappropriate disciplinary action against a resident.

Id. at 712.

[80] *Id*.

[81] *Id.* at 713-14.

> Dr. O'Connor selected several Hospital personnel to conduct the investigation, including an accountant, a physician, and a Hospital security officer. Richard

Amendment protection against unreasonable searches and seizures had been violated as he had an expectation of privacy in his office.[82] The Supreme Court reviewed the case on two issues:

> whether the employee had a reasonable expectation of privacy in his office, desk, and file cabinets at his place of work; and . . . the appropriate Fourth Amendment standard for a search conducted by a public employer in areas in which a public employee is found to have a reasonable expectation of privacy.[83]

The district court had upheld the search;[84] the Court of Appeals for the Ninth Circuit Court affirmed in part and reversed in part finding that Dr. Ortega had a reasonable expectation of privacy in his office and, that while the hospital had a policy regarding employees that were leaving or terminated, the search was in violation of Dr. Ortega's Fourth Amendment rights.[85] Citing *United States v.*

> Friday, the Hospital Administrator, led this "investigative team." At some point during the investigation, Mr. Friday made the decision to enter Dr. Ortega's office. The specific reason for the entry into Dr. Ortega's office is unclear from the record. The petitioners claim that the search was conducted to secure state property. Initially, petitioners contended that such a search was pursuant to a Hospital policy of conducting a routine inventory of state property in the office of a terminated employee. At the time of the search, however, the Hospital had not yet terminated Dr. Ortega's employment; Dr. Ortega was still on administrative leave. Apparently, there was no policy of inventorying the offices of those on administrative leave. Before the search had been initiated, however, petitioners had become aware that Dr. Ortega had taken the computer to his home. Dr. Ortega contends that the purpose of the search was to secure evidence for use against him in administrative disciplinary proceedings.
>
> . . .
>
> The resulting search of Dr. Ortega's office was quite thorough. The investigators entered the office a number of times and seized several items from Dr. Ortega's desk and file cabinets, including a Valentine's Day card, a photograph, and a book of poetry all sent to Dr. Ortega by a former resident physician. These items were later used in a proceeding before a hearing officer of the California State Personnel Board to impeach the credibility of the former resident, who testified on Dr. Ortega's behalf. The investigators also seized billing documentation of one of Dr. Ortega's private patients under the California Medicaid program. The investigators did not otherwise separate Dr. Ortega's property from state property because, as one investigator testified, "[t]rying to sort State from non-State, it was too much to do, so I gave it up and boxed it up." Id. at 712. Thus, no formal inventory of the property in the office was ever made. Instead, all the papers in Dr. Ortega's office were merely placed in boxes, and put in storage for Dr. Ortega to retrieve.

Id.

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

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

[83] *See O'Connor*, 480 U.S. at 711-12.

[84] *See id.* at 714.

[85] *Id.*

> Dr. Ortega commenced this action against petitioners in Federal District Court under 42 U.S.C. § 1983, alleging that the search of his office violated the Fourth

Jacobsen, 466 U.S. 109 (1984), the Supreme Court held,

> Our cases establish that Dr. Ortega's Fourth Amendment rights are implicated only if the conduct of the Hospital officials at issue in this case infringed "an expectation of privacy that society is prepared to consider reasonable." We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable. Instead, "the Court has given weight to such factors as the intention of the Framers of the Fourth Amendment, the uses to which the individual has put a location, and our societal understanding that certain areas deserve the most scrupulous protection from government invasion.[86]

The Court noted that the appropriateness of a search and the reasonableness of an expectation of privacy depend upon the context, and, so defined "[t]he workplace includes those areas and items that are related to work and are generally within the employer's control." [87] The Court also noted:

> Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the

---

> Amendment. On cross-motions for summary judgment, the District Court granted petitioners' motion for summary judgment. The District Court, relying on *Chenkin v. Bellevue Hospital Center, New York City Health & Hospitals Corp.*, 479 F. Supp. 207 (SDNY 1979), concluded that the search was proper because there was a need to secure state property in the office. The Court of Appeals for the Ninth Circuit affirmed in part and reversed in part, 764 F.2d 703 (1985), concluding that Dr. Ortega had a reasonable expectation of privacy in his office. While the Hospital had a procedure for office inventories, these inventories were reserved for employees who were departing or were terminated. The Court of Appeals also concluded–albeit without explanation–that the search violated the Fourth Amendment. The Court of Appeals held that the record justified a grant of partial summary judgment for Dr. Ortega on the issue of liability for an unlawful search, and it remanded the case to the District Court for a determination of damages.

Id.

[86] *Id.* at 715.

[87] *Id.* at 715-16.

> At a hospital, for example, the hallways, cafeteria, offices, desks, and file cabinets, among other areas, are all part of the workplace. These areas remain part of the workplace context even if the employee has placed personal items in them, such as a photograph placed in a desk or a letter posted on an employee bulletin board. Not everything that passes through the confines of the business address can be considered part of the workplace context, however. An employee may bring closed luggage to the office prior to leaving on a trip, or a handbag or briefcase each workday. While whatever expectation of privacy the employee has in the existence and the outward appearance of the luggage is affected by its presence in the workplace, the employee's expectation of privacy in the *contents* of the luggage is not affected in the same way. The appropriate standard for a workplace search does not necessarily apply to a piece of closed personal luggage, a handbag or a briefcase that happens to be within the employer's business address.

Id. The Court continued:

> Within the workplace context, this Court has recognized that employees may have a reasonable expectation of privacy against intrusions by police. *See* Mancusi v. DeForte, 392 U.S. 364 (1968). As with the expectation of privacy in one's home, such an expectation in one's place of work is "based upon societal expectations that have deep roots in the history of the Amendment."

Id. (citing Oliver v. United States, 466 U.S. 170, n.8 (1986)).

> workplace, however, may make *some* employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.[88]

The Court then noted that an expectation of privacy by an employee should be reviewed on a case-by-case basis.[89]

Upon finding that Dr. Ortega had a reasonable expectation of privacy, and in addressing the search, the Court held, in the case of searches conducted by a public employer, "we must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace."[90] The Court rejected the need to obtain a warrant when an employer wishes to enter an employee's office, desk, or file cabinets for a work-related purpose that would seriously disrupt the routine conduct of business and would be unreasonable.[91] Moreover, requiring a probable

---

[88] *O'Connor*, 480 U.S. at 717.

[89] *Id.*

> The employee's expectation of privacy must be assessed in the context of the employment relation. An office is seldom a private enclave free from entry by supervisors, other employees, and business and personal invitees. Instead, in many cases offices are continually entered by fellow employees and other visitors during the workday for conferences, consultations, and other work-related visits. Simply put, it is the nature of government offices that others-such as fellow employees, supervisors, consensual visitors, and the general public-may have frequent access to an individual's office. We agree with Justice SCALIA that "[c]onstitutional protection against *unreasonable* searches by the government does not disappear merely because the government has the right to make reasonable intrusions in its capacity as employer," post, at 731, but some government offices may be so open to fellow employees or the public that no expectation of privacy is reasonable. Cf. Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection"). Given the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis.

Id. at 717-18.

[90] *Id.* "There is surprisingly little case law on the appropriate Fourth Amendment standard of reasonableness for a public employer's work-related search of its employee's offices, desks, or file cabinets. Generally, however, the lower courts have held that any 'work-related' search by an employer satisfies the Fourth Amendment reasonableness requirement." *See* United States v. Nasser, 476 F.2d 1111, 1123 (7th Cir. 1973) ("work-related" searches and seizures are reasonable under the Fourth Amendment); United States v. Collins, 349 F.2d 863, 868 (2nd Cir. 1965) (upholding search and seizure because it was conducted pursuant to "the power of the Government as defendant's employer, to supervise and investigate the performance of his duties as a Customs employee"). Others have suggested the use of a standard other than probable cause. *See* United States v. Bunkers, 521 F.2d 1217 (9th Cir. 1975) (work-related search of a locker tested under 'reasonable cause' standard); United States v. Blok, 188 F.2d 1019, 1021 (D.C. Cir. 1951) ("No doubt a search of [a desk] without her consent would have been reasonable if made by some people in some circumstances. Her official superiors might reasonably have searched the desk for official property needed for official use."). Only two cases imply that a warrant should be required to involve searches that are not work related. *See* Gillard v. Schmidt, 579 F.2d 825, 829 (3rd Cir. 1978) (for searches for evidence of criminal misconduct); *see also* United States v. Kahan, 350 F. Supp. 784 (S.D.N.Y. 1972).

[91] *O'Connor*, 480 U.S. at 722.

cause standard for searches of the type at issue would impose intolerable burdens on public employers. The intrusions on the constitutionally protected privacy interests of government employees for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances. Under this standard, both the inception and the scope of the intrusion must be reasonable.[92] The Court further stated,

> As an initial matter, it is important to recognize the plethora of contexts in which employers will have an occasion to intrude to some extent on an employee's expectation of privacy. Because the parties in this case have alleged that the search was either a non-investigatory work-related intrusion or an investigatory search for evidence of suspected work-related employee misfeasance, we undertake to determine the appropriate Fourth Amendment standard of reasonableness *only* for these two types of employer intrusions and leave for another day inquiry into other circumstances." The Supreme Court remanded the case for "the District Court must determine the justification for the search and seizure, and evaluate the reasonableness of both the inception of the search and its scope.[93]

Regarding the existing policy and procedures in this case, the Supreme Court noted that the Hospital did not have a "reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or file cabinets, although the absence of such a policy does not create an expectation of privacy where it would not otherwise exist." The Supreme Court agreed with the Court of Appeals that Dr. Ortega had a reasonable expectation of privacy in at least his desk and file cabinets.[94] The analysis of privacy expectations and the employment relationship beyond traditional physical offices, cabinets or other "spaces," into an analysis of the expectation of privacy in the more elusive realm of new media is further expanded in developing case law.[95] Courts are now confronted with expectations of both employers and employees relative to intangible "spaces" and information obtained, stored and accessed beyond the brick and mortar of the workplace.[96]

---

[92] *Id*. at 725-26. Regarding the inception and scope of the search, the Court held: "Determining the reasonableness of any search involves a twofold inquiry: first, one must consider 'whether the . . . action was justified at its inception.'" *Id.* (citing Terry v. Ohio, 392 U.S. 1, 20 (1968)); Second, "one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place.'" *Id.* at 726 (citing New Jersey v. T.L.O., 469 U.S. 325, 341 (1984)). Ordinarily, a search of an employee's office by a supervisor will be "justified at its inception" when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a non investigatory work-related purpose such as to retrieve a needed file. *O'Connor*, 480 US. at 726. Because petitioners had an 'individualized suspicion' of misconduct by Dr. Ortega, we need not decide whether "individualized suspicion" is an essential element of the standard of reasonableness that we adopt today. *See id.* at 342. The search will be permissible in its scope when "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]." *Id.*

[93] *Id.* at 723.

[94] *Id.* at 719 (citing Gillard v. Schmidt, 579 F.2d 825 (3rd Cir. 1978)).

[95] *See* discussion of *Quon infra* notes 149-79 and accompanying text.

[96] *See* discussion of *Quon infra* notes 149-79 and accompanying text.

Pure Power Boot Camp, Inc., et.al., v. Warrior Fitness Boot Camp, LLC, et.al. (2008)

In 2008, the District Court for the Southern District of New York reviewed issues related to access of employee's e-mail accounts by an employer.[97] In *Pure Power Boot Camp, Inc., et.al. v. Warrior Fitness Boot Camp, LLC*,[98] (Pure Power Boot Camp), the Plaintiff's sought to enter into evidence defendant's e-mails that supported Plaintiff's claims of breach of a restrictive covenant.[99] Defendant opened a competing fitness center upon termination of his employment.[100] Plaintiff's sought "an injunction and damages, and accused Defendants of (1) stealing Plaintiffs' business model, customers, and internal documents, (2) breaching employee fiduciary duties, and (3) infringing Plaintiffs' trademarks, trade-dress, and copyrights."[101] Plaintiff sought to enter into evidence e-mails obtained from Defendant's personal (non-work) e-mail service providers (Gmail, Hotmail and Plaintiff's new company's email account) subsequent to Defendant's termination.[102] Access was gained through passwords that were saved to Defendant's work computer and by applying that same password to other accounts; access was not granted by Defendant.[103] Defendant sought to bar the emails from evidence, compel their return and sought damages.[104]

The company had an e-mail policy,[105] which limited employee's expectation of privacy in company e-mails and granted the company full access to review all e-mail sent via the company system.[106] The court noted

> this is not, however, a case where an employee was using an employer's computer or e-mail system, and then claimed that the e-mails contained on the employer's computers are private. Here, the employee - Fell - did not store any of the communications which his former employer now seeks to use against him on the employer's computers, servers, or systems; nor were they sent from or received on the company e-mail system or computer. These e-mails were located on, and accessed from, third-party communication service provider systems. There is not even an implication that Fell's personal e-mail accounts were used for PPBC work

---

[97] Pure Power Boot Camp, Inc., et al. v. Warrior Fitness Boot Camp, LLC, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

[98] *Id.*

[99] *Id.* at 551.

[100] *Id.* at 552.

[101] *Id.* at 551.

[102] *Id.* at 552.

[103] *Boot Camp*, 587 F. Supp. 2d at 552, 559.

[104] *Id.* at 551.

> [E]-mail users have no right of personal privacy in any matter stored in, created on, received from, or went through or over the system. This includes the use of personal e-mail accounts on Company equipment. The Company, in its discretion as owner of the e-mail system, reserves the right to review, monitor, access, retrieve, and delete any matter stored in, created on, received from, or sent through the system, for any reason, without the permission of any system user, and without notice.

Id.

[105] *Id.* at 552-53.

[106] *Id.*

> or that PPBC paid or supported Fell's maintenance of those accounts.[107]

Regarding the company e-mail policy, the district court held,

> Courts have routinely found that employees have no reasonable expectation of privacy in their workplace computers, where the employer has a policy which clearly informs employees that company computers cannot be used for personal e-mail activity, and that they will be monitored." In *Pure Power Boot Camp*, the Court noted that, "there is nothing in the PPBC policy that even suggests that if an employee simply views a single, personal e-mail from a third party e-mail provider, over PPBC computers, then all of his personal e-mails on whatever personal e-mail accounts he uses, would be subject to inspection.[108]

The court distinguished *Pure Power Boot Camp* from other cases which discuss expectations of privacy in company owned computers. The court, citing *Leventhal v. Knapek*, noted that in *Leventhal*, even though there was a company policy, an employee with a private office with a door, had a reasonable expectation of privacy in the contents of his exclusively used company computer.[109] The court also noted *Curto v. Medical World Communications*,[110] which held that an

---

[107] *Id.* at 560.

[108] *Id.* at 559-60 (citing United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use."); Thygeson v. U.S. Bancorp, CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004) ("[W]hen, as here, an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy."); Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002) ("But Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim.")). "In these cases, because the employee had no reasonable expectation of privacy, the employer did not need consent to search the employee's computer files." *Id.*

[109] *Boot Camp*, 587 F. Supp. 2d at 560 (citing Levanthal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)).

> The Second Circuit held that an employee had a reasonable expectation of privacy in the contents of his computer where the employee occupied a private office with a door, had exclusive use of the computer in his office, and did not share use of his computer with other employees or the public, notwithstanding the fact that there was a policy which "prohibited 'using' state equipment 'for personal business.'" In Leventhal, there was no clear policy or practice regarding regular monitoring of work computers; technical staff conducted infrequent and selective searches for maintenance purposes only.

Id.

[110] *Id.* at 560-61 (citing Curto v. Medic. World Communic'ns, No. 03CV6327, 2006 U.S. Dist. LEXIS 29387 (E.D.N.Y 2006)).

> The employer hired a forensic consultant to restore portions of the computer files that the employee had deleted, nearly two years earlier, from a home-based work computer, including e-mails of communications with the employee's lawyer. Even though the computer belonged to the employer, and the employer had a policy that warned employees they had no reasonable expectation of privacy in "anything they create, store, send, or received on the computer, or through the Internet or any computer network," the employee successfully asserted attorney-client privilege over those e-mails, in part because she had a reasonable expectation of privacy in a home-computer which was not connected to the employer's network.

Id.

employee who worked from home with a work issued computer had a protected attorney-client privilege in e-mails sent from that computer, notwithstanding the existence of a company policy that provided to the contrary. The court also noted the 2008 Ninth Circuit Court decision in *Quon v. Archwireless*,[111] which held that a police officer had a reasonable expectation of privacy in text messages sent on a city issued pager.[112]

In *Pure Power Boot Camp*, the court concluded that the employer accessed Defendant's third party server e-mails without authorization and precluded the e-mails from evidence.[113] *Pure Power Boot Camp* emphasizes the need for companies to have a thorough policy regarding new media. Employers must not only educate employees as to their expectations of privacy on company owned and issued equipment, but also must educate themselves as to accessing new media beyond the scope of the employment arena.[114] In addition, *Pure Power Boot Camp* also recognized the need for companies to properly implement those policies and practices, and recognized the ramifications if those same policies, procedures, and state and federal law, are not followed.[115]

Stengart v. Loving Care Agency Inc., et al. (2010)

In March 2010, the New Jersey Supreme Court also addressed the issue of retrieval of an employee's e-mail messages by an employer from a company owned and issued laptop computer. In *Stengart v. Loving Care Agency*,[116] the court addressed "questions about the extent to which an employee can expect privacy and confidentiality in personal e-mails with her attorney, which she accessed on a computer belonging to her employer . . . [Plaintiff, Stengart] used her company-issued laptop to exchange e-mails with her lawyer through her personal, password-protected, web-based e-mail account."[117]

Stengart accessed her personal e-mail account through her company's server.

> Unbeknownst to Stengart, certain browser software in place automatically made a copy of each web page she viewed, which was then on the computer's hard drive in a 'cache' folder of temporary Internet files . . . . [I]n December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop.[118]

After Plaintiff left Defendant's employ, she brought suit alleging employment discrimination.[119] Defendant's anticipated litigation and hired experts

---

[111] *Arch Wireless*, 529 F.3d at 892 (9th Cir. 2008).

[112] *Id.*

[113] *Boot Camp*, 587 F. Supp. 2d at 561.

[114] Sophos Press Release, *supra* note 1.

[115] *See also* Denise J. Pipersburgh & Keyanna C. Laws, *Cyberspace in the Workplace: Employer Protection Requires a More Than Mere Ownership of the Computer Systems*, 198 N.J.L.J. 800 (2009).

[116] *Stengart*, 990 A.2d at 650.

[117] *Id.* at 655.

[118] *Id.* at 656.

[119] *Id.* at 655.

to create a forensic image of the laptop's hard drive, including temporary Internet files.[120] Those files contained the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account.[121] At the bottom of the e-mails sent by Stengart's lawyer, a legend warns readers that the information "is intended only for the personal and confidential use of the designated recipient" of the e-mail, which may be a "privileged and confidential" attorney-client communication.[122] Attorneys from the law firm (the "Firm") representing Loving Care reviewed the e-mails and used the information in discovery.[123] Stengart's lawyer demanded that the e-mails be identified and returned.[124] The Firm disclosed the e-mails but argued that Stengart had no reasonable expectation of privacy in files on a company-owned computer in light of the company's policy on electronic communications ("Policy").[125] The Policy states that Loving Care may review, access, and disclose "all matters on the company's media systems and services at any time."[126] It also states that e-mails, Internet communications and computer files are the company's business records and "are not to be considered private or personal" to employees.[127] It goes on to state that "occasional personal use is permitted."[128] The Policy specifically prohibits "certain uses of the e-mail system," such as discriminatory or harassing messages.[129]

"The trial court ruled that, in light of the company's written policy on electronic communications, Stengart waived the attorney-client privilege by sending e-mails on a company computer. The Appellate Division reversed and found that Loving Care's counsel had violated RPC 4.4(b) by reading and using

---

[120] *Id.* at 656.

[121] *Id.*

[122] *Stengart*, 990 A.2d at 656.

[123] *Id.*

[124] *Id.* at 657.

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *Stengart*, 990 A.2d at 657.

[129] *Id.* The proffered Policy states, in relevant part:

> The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice . . . . E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee. The principal purpose of electronic mail (e-mail) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources . . . . The Policy also specifically prohibits "[c]ertain uses of the e-mail system" including sending inappropriate sexual, discriminatory, or harassing messages, chain letters, [m]essages in violation of government laws, or messages relating to job searches, business activities unrelated to Loving Care, or political activities. The Policy concludes with the following warning: Abuse of the electronic communications system may result in disciplinary action up to and including separation of employment.

Id.

the privileged documents."[130] The New Jersey Supreme Court held that the Plaintiff (employee)

> could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them using a company laptop did not eliminate the attorney-client privilege that protected them. By reading e-mails that were at least arguably privileged and failing to notify Stengart promptly about them, Loving Care's counsel violated RPC 4.4(b).[131]

Citing the appellate court's decision, the supreme court agreed that

> The panel balanced Loving Care's right to enforce reasonable rules for the workplace against the public policies underlying the attorney-client privilege. The court rejected the notion that 'ownership of the computer [is] the sole determinative fact' at issue and instead explained that there must be a nexus between company policies and the employer's legitimate business interests. The panel concluded that society's important interest in shielding communications with an attorney from disclosure outweighed the company's interest in upholding the Policy.[132]

The supreme court found the Defendant's policy "unclear" in that it did not define key terms, address personal web-based e-mail accounts, or make clear to employees that e-mail was monitored, or that copies of e-mails were stored and could subsequently be electronically retrieved.[133] The policy also provided for limited personal use.[134] Regarding Plaintiff's expectation of privacy, the court noted the "reasonable-expectation-of-privacy standard used by the parties derives from the common law and the Search and Seizure Clauses of both the Fourth Amendment and Article I, paragraph 7 of the New Jersey Constitution. The latter sources do not apply in this case, which involves conduct by private parties only."[135] Instead, the court analyzed the expectation of privacy within the context of the tort of intrusion on seclusion, noting that, "a plaintiff must establish that the intrusion 'would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object.'[136] Citing *O'Connor*, the court noted that, "whether an employee has a reasonable expectation of privacy in her particular work setting 'must be addressed on a case-by-case basis.'"[137]

In analyzing company's policy and whether it controlled, the court referenced *In re Asia Global Crossing, Ltd.*, in which the Bankruptcy Court for the Southern District of New York

> developed a four-part test to "measure the employee's expectation of privacy in his computer files and e-mail": (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the

---

[130] *Id.* at 657-58.

[131] *Id.*

[132] *Id.* at 661.

[133] *Id.* at 659.

[134] *Stengart*, 990 A.2d at 659.

[135] *Id.* at 660.

[136] *Id.*.

[137] *Id.* (citing *O'Connor*, 480 U.S. at 718 (reviewing public sector employment)).

> employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[138]

The court also noted distinctions by other courts between employees using personal web-based email and company e-mail, and referenced *National Economic Research Associates v. Evans*, which also involved forensic recovery of personal emails to/from the plaintiffs and his attorneys from plaintiff's company issued laptop.[139]

Noting that other courts have held that a zero tolerance policy for personal use of email would limit an employee's expectation of privacy, the court stated that it recognized that "a zero-tolerance policy can be unworkable and unwelcome in today's dynamic and mobile workforce and do not seek to encourage that approach in any way."[140] The court held that Plaintiff Stengart had an expectation of privacy in her web-based personal e-mail, even though it was accessed via a company issued laptop.[141] The court also held that those e-mails were protected by the attorney–client privilege.[142]

Regarding company polices, the court clarifies that companies

> can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy.[143]

However, the court also held that a company policy, even if clearly drafted and communicated to the employee, would not be enforced if it attempted to claim that the company could retrieve, read or own communications that were protected

---

[138] *Id.* at 662 (citing In re Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)).

[139] *Id.* at 661 (referencing Nat'l Econ. Research Assocs. v. Evans, 21 Mass. L. Rptr. 337 (Mass. Super. Ct. 2006)).

> According to some courts, employees appear to have a lesser expectation of privacy when they communicate with an attorney using a company e-mail system as compared to a personal, web-based account like the one used here. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp 97, 100-01 (E.D. Pa. 1996) (finding no reasonable expectation of privacy in unprofessional e-mails sent to supervisor through internal corporate e-mail system); Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, 441-43 (N.Y. Sup. Ct. 2007) (finding no expectation of confidentiality when company e-mail used to send attorney-client messages). *But see* Contervino v. U.S. Dep't of Justice, 674 F. Supp. 2d. 97 (D.D.C. 2009) (finding reasonable expectation of privacy in attorney-client e-mails sent via employer's e-mail system). As a result, courts might treat e-mails transmitted via an employer's e-mail account differently than they would web-based e-mails sent on the same company computer.

Stengart, 990 A.2d at 662.

[140] *Id.* at 662-63.

[141] *Id.* at 663.

[142] *Id.* at 664.

[143] *Id.* at 665 (referencing Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d. 11 (N.J. 1992); Wooley v. Hoffman-LaRoche, Inc., 491 A.2d 1257 (N.J. 1985); Pierce v. Ortho Pharm. Corp., 417 A.2d 505 (N.J. 1980)).

by the attorney-client privilege.[144]

Stengart, like *Pure Power Boot Camp*, recognized an employee's expectation of privacy in e-mails accessed on company issued equipment.[145] *O'Connor, Pure Power Boot Camp and Stengart,* all recognized an expectation of privacy that an employee has utilizing new media in the employment arena.[146] All three cases addressed private employers, unlike *O'Connor*, in which the employer was a government entity.[147] Courts may split their decisions based upon the nature of the employer, but they acknowledge the impact of new media on the employment relationship and the developing nature of the law relative to both employer and employee rights.[148]

The City of Ontario, California, et al. v. Quon (2010)

The US Supreme Court's June 2010 decision in *City of Ontario, California, et al. v. Quon*,[149] like *O'Connor*, involved a government employer and an employee who contended that he had a reasonable expectation of privacy in seized text messages sent on a government issued pager.[150] Jeff Quon was employed as an officer by the City of Ontario, California police department.[151] Officers were issue pagers as part of their official equipment in order to send text messages in order to respond to official emergencies.[152]

Quon (and other officers) who exceeded their monthly text message character allotment were reminded by a supervisor of the City policy on character allotment and the fact that the City could audit all messages.[153] The same supervisor stated he did not intend to audit the accounts and suggested the officers (Quon included) who exceeded the allotment pay the overage fees.[154] After several months of allotment overages, a supervisor decided to audit the accounts to determine if the character allotment was too small and whether or not the officers were paying for work related messages or if the messages were personal.[155] Upon receipt of the transcripts of the text messages from the service provider (Arch Wireless), it was determined that Quon utilized his pager for personal messages in violation of the City policy and was disciplined.[156] Quon brought suit alleging violation of his Fourth Amend rights and violation of the Store Communications

---

[144] *Id*. (for a further discussion of the company's policy see *Stengart*, 973 A.2d at 650, 657).

[145] *Id*. at 663.

[146] *O'Connor*, 480 U.S. at 470, *Pure Power Boot*, 587 F. Supp. 2d at 548; *Stengart*, 990 A.2d at 650; *see also infra* note 199 (discussing *Pietrylo*).

[147] *See O'Connor*, 480 U.S. at 470.

[148] *See* discussion on *Quon*, *infra* notes 149-79 and accompanying text.

[149] *Quon*, 130 S. Ct. at 2619.

[150] *Id*.

[151] *Id*.

[152] *Id*. at 2625.

[153] *Id*.

[154] *Id*.

[155] *Quon*, 130 S. Ct. at 2625.

[156] *Id*. at 2626.

Act ("SCA")[157] by the City of Ontario and Arch Wireless.[158]

The district court granted Arch Wireless' motion for summary judgment on the Stored Communications Act claim and held a jury trial on the Fourth Amendment issue. A jury held that the purpose of the audit was to determine the efficacy of the policy and the district court entered judgment in favor of the City of Ontario.[159] Upon appeal, the United States Court of Appeals for the Ninth Circuit reversed in part, finding Quon had a reasonable expectation of privacy in the text messages, disagreed with the District Court that the search was reasonable, and held that Arch Wireless had violated the SCA.[160] The US Supreme Court granted certiorari.[161]

The Supreme Court reviewed the *O'Connor v. Ortega* case,[162] and discussed the fact that in ". . . the two decades since *O'Connor*, however, the threshold test for determining the scope of an employee's Fourth Amendment rights has not been clarified further." Here, though they disagree on whether Quon had a reasonable expectation of privacy, both petitioners and respondents start from the premise that the *O'Connor* plurality controls. That is, that ". . .a court must consider '[t]he operational realities of the workplace' in order to determine whether an employee's Fourth Amendment rights are implicated."[163] On this view, "the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[164] Next, where an employee has a legitimate privacy expectation, an employer's intrusion on that expectation "for non-investigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances."[165]

Relative to the City policy, the Court noted that the policy itself was clear and the subsequent memos and statements which addressed text messaging all made it very clear that an employee did not have an expectation of privacy in text messages.[166] However, due to the supervisor's contradictory statements, an expectation of privacy may have arisen.[167] The Supreme Court's review found that Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City, albeit a limited expectation given the nature of his employment and the purpose for the pager,[168] that search was motivated by a

---

[157] The Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2002) [hereinafter SCA].

[158] *Quon*, 130 S. Ct. at 2626.

[159] *Id.* at 2627.

[160] *Id.*

[161] Certiorari was limited to "the petition for certiorari filed by the City, OPD, and Chief Scharf challenging the Court of Appeals' holding that they violated the Fourth Amendment." *Id.* The petition for certiorari filed by Arch Wireless challenging the Ninth Circuit's ruling that Arch Wireless violated the SCA was denied. *See supra* note 3 and accompanying text.

[162] *Quon*, 130 S. Ct. at 2628.

[163] *O'Connor*, 480 U.S. at 717.

[164] *Id.* at 718.

[165] *Id.* at 725-26.

[166] *Quon*, 130 S. Ct. at 2629.

[167] *Id.* (giving rise to an analysis of "operational difficulties" referenced in *O'Connor*).

[168] *Quon*, 130 S. Ct. at 2629.

legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the O'Connor plurality, and last, "principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere."[169] The Court held that the search was reasonable and did not violate Quon's Fourth Amendment rights thereby reversing the judgment of the Court of Appeals for the Ninth Circuit and remanded the case.[170]

Regarding the impact of new media upon the employment relationship the Court noted it "must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer.[171] The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[172] Further it stated that "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."[173] As one amicus brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency.[174] Another amicus points out that the law is beginning to respond to these developments, as some states have recently passed statutes requiring employers to notify employees when monitoring their electronic communications.[175] At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.[176]

The Court addressed developing employment policies stating that "policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."[177] The Court was cautious in its holding given the constantly evolving nature of new media asserting "a broad holding concerning employees' privacy expectations vis-a-vis employer-provided technological equipment might have implications for future cases that cannot be predicted."[178] What is emerging from the developing case law is that the rights and expectations of both employers and employees must be clearly identified, communicated, and uniformly applied.[179]

---

[169] *Id.* at 2630.

[170] *Id.* at 2633.

[171] *Id.* at 2628.

[172] *Id.*

[173] *Id.*

[174] *See* Brief for Elec. Frontier Found. et al. as Amici Curiae supporting Respondents, The City of Ontario, California, et al. v. Quon, et al., 130 S. Ct. 2619 (2010) (No. 08-1332), 2010 WL 1063463.

[175] *See* Brief for N.Y. Intellectual Prop. Law Ass'n supporting Respondents, The City of Ontario, California, et al. v. Quon, et al., 130 S. Ct. 2619 (2010) (No. 08-1332), 2010 WL 1186480.

[176] *Quon*, 130 S. Ct. at 2630.

[177] *Id.*

[178] *Id.*

[179] *Id.*

THE FUTURE IMPACT OF NEW MEDIA

As new media applications and technology develops, both employers and employees will have to develop their own reasoned responses to enhance the application of these technologies and to minimize their negative impacts. Companies are "deploying software and assigning employees to monitor Internet postings and blogs. They're also assigning senior leaders to craft corporate strategies for social media."[180] Companies are also ramping up their risk management perspective by "tracking social media outlets such as Facebook and Twitter to gauge consumer sentiment and avert potential public-relations problems.[181]

Companies are also utilizing the world wide web to help in the hiring process.[182] By utilizing search engine marketing, employers can recruit employees at a substantial cost savings.[183] Companies are learning to use new media tools, such as Twitter and Facebook, to address public relations crises[184] and enforcement of non-competition clauses.[185] Social networks, such as Facebook, MySpace and LinkedIn will become more specific in the amount of material that companies can mine about users and their friends.[186] Facebook continues to face a global firestorm about the type of and quantity of information revealed by its users that it is releasing to advertisers on its site. In this aspect, the more information that is available, the better it is for a company.

Not all companies want to send tweets on Twitter, but they might want to follow other companies to find out what the competition is doing and what is being said about their own company.[187] Employers that give their employees access to

---

[180] Sarah E. Needleman, *For Companies, a Tweet in Time Can Avert PR Mess*, WALL ST. J., Aug. 3, 2009, at B6.

[181] *Id.*

[182] *You Are What You Post*, *supra* note 6.

[183] Sarah E. Needleman, *Recruiters Use Search Engines to Lure Job Hunters*, WALL ST. J., Mar. 9, 2009, at B4, *available at* http://online.wsj.com/article/SB123638064919857503.html.

> In search-engine marketing, employers bid to place ads next to search results for certain keywords, like "accountant," or "nurse." The ads can be limited to users in specific ZIP codes. Advertisers pay search engines when a user clicks on their ad. Last March, Baylor Health Care System, a large Dallas-based nonprofit, began purchasing keywords on Google, Yahoo and employment-related search engines SimplyHired.com and Indeed.com. The search-engine ads generated more applicants, at less cost, than the other recruiting methods, says Eileen Bouthillet, director of human resources communications . . . . If the strategy becomes more popular, Mr. Sterling notes, it will also become more expensive, as employers compete to bid up the price of keywords. That could make it less effective compared with other media. For now, though, the few companies using it get in front of applicants faster and without competition in many cases.

Id.

[184] *Id.*; *see also* Sarah E. Needleman, *Entrepreneurs 'Tweet' Their Way Through Crises*, WALL ST. J., Sept. 15, 2009, at B5.

[185] *See Jaikumar Vijaya, Lawsuit Posits Social Network Connects Are a Noncompete Violation*, WIRED, June 16, 2010, *available at* www.wired.com/epicenter/2010/06/lawsuit-posits-social-network-connects-are-a-non-compete-violation/2/.

[186] *Facebook Unveils Privacy Changes*, *supra* note 10.

[187] *See* Sloan, *supra* note 21, for a discussion of a dismissed Illinois suit where a real estate management company alleged defamation against a former tenant who tweeted about mold in her

new media tools expect that these same employees know not only how to use them, but also how *not* to use them.[188] Employers then must create policies and procedures that give guidance to employees. These policies must be updated at least on an annual basis in order to keep current with the fast growth of new media.[189] In addition, employers must educate employees as to all policies and procedures. Expectations must be conveyed in a way that all employees understand (multiple languages, etc.) and policies enforced in a consistent manner in order to avoid situations like *Quon* and *Stengart.*[190] Potentially, companies might want to create a new position of Chief Privacy Officer or to integrate that concept into a new position of Chief Technology Officer.[191] According to Michelle Dennedy, chief privacy officer at Sun Microsystems, "[t]he first steps that should be taken to deal with this . . . [are to] harmonize regulations, build privacy into products and services, gain competitive advantage, and consider privacy part of good corporate governance."[192] She even advocates creating the position of chief privacy officer at a senior level.[193]

Companies must develop policies that do not just broadly interpret use and practices, but that specifically identify how employees use new media.[194] This need is underscored by recent Court decisions, enlightening social polls and recent media reports.[195] A company must create the expectations of the employer and the employee in order to regulate the use and effect of new media in the workplace.[196] Emergent new media technologies demand that employers be ahead of the learning curve and anticipate new issues.[197] Likewise, courts will continue to address the applicability of new media in the employment arena and its impact upon the rights of employers and employees.[198]

---

apartment.

[188] *Web 2.0*, *supra* note 34.

[189] *Id.*

> There are, however, some common bits of advice that appear in the available literature on the subject. Any blogging or social networking policy should remind employees that negative or disparaging comments regarding the company posted to blogs or social networking pages are a breach of their duty of loyalty to their employer which may result in termination (particularly in at-will employment states). The company's anti-harassment and discrimination policies should be incorporated into the blogging and social networking policy. Employees should be encouraged either to refrain from identifying themselves as employees of the company in blog or social networking posts or to include a disclaimer that states that their opinions are personal in nature and do not reflect those of their employer.

Id.

[190] *Quon*, 130 S. Ct. at 2619; *Stengart*, 990 A.2d at 650.

[191] *See* Parent, *supra* note 65.

[192] *Id.*

[193] *Id.*

[194] *Web 2.0*, *supra* note 34.

[195] *Id*.

[196] *Id.*

[197] *Id.*

[198] See *Pietrylo* I, 2008 U.S. Dist. LEXIS 108834, an unpublished decision which addresses an employer accessing employees' MySpace user chat group accounts without authorization in order to review comments posted; the employer subsequently fired the employees. *Id.* The case involved issues

If our social systems change incrementally and are not able to respond to the rapid pace of change, is it not unreasonable to expect employers to anticipate the impact of these changes and manage their employment policies accordingly? Or, to expect courts to be able to respond thereafter? Some employees, on the other hand, are comfortable with and reliant upon their continuous use of and access to new media for personal use and undoubtedly in support of their employers interests.[199] The real problem arises at the intersection of those two uses.[200] The finding in *Quon* suggests that the use of employer provided hardware, software and Internet access for personal use by employees is not protected.[201] As Justice Kennedy noted in *Quon*,

> [c]ellphone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification . . . [o]n the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cellphones or similar devices for personal matters can purchase and pay for their own.[202]

The challenge for employers is to balance employer policies with the increasing ubiquity of new media technologies and the manner in which reasonable persons use them.

If a reasonable person simply uses the device most near at hand to communicate, and that device is employer provided, as in *Quon*, should that behavior require a new standard? We would argue that as users become more technologically sophisticated, and platforms become even more ubiquitous and easy to use, it is it is highly likely that users will merge their analog and digital personas without necessarily understanding the legal implications of doing so. In light of recent case developments, should we apply the "reasonable person" standard? How, when society, employers and the court system all have difficulty keeping current with rapidly changing technology, would we define what a "reasonable person" is when levels of technological understanding vary from person to person? Should the standard be based upon technological sophistication?

---

of the common law right to privacy, violation of the federal Stored Communications Act, and the New Jersey statute on unlawful access to stored communications. *Id.* at *4. Plaintiffs alleged that their use of MySpace was private and the user group was created on personal time, users gained access by invitation-only, which were distributed on personal time, and a password was required to access. *Id.* at *1-2. Subsequently, supervisors at Defendant's restaurant gained unauthorized access to the site, which included negative comments about the employer, and plaintiffs were fired; the reason cited for their termination was violation of company policy involving "professionalism and a positive attitude." *Id.* at *4. The jury returned a verdict in favor of Plaintiffs on the Stored Communications Acts claims, finding that Defendant had, through its managers, knowingly, intentionally, or purposefully accessed the private chat group without authorization on five occasions. *Pietrylo II*, 2009 U.S. Dist. LEXIS 88702, at *2. The jury also found Defendant had acted maliciously, leading to a right to punitive damages. *Id.* The jury awarded compensatory damages to Plaintiffs. *Id.* at *3. By stipulation of the parties, the award of punitive damages equaled four times the amount of compensatory damages awarded by the jury; the district court noted that Federal Stored Communications Act and the New Jersey statute both provide for punitive damages. *Id.* at *3, 16-21.

[199] Sophos Press Release, *supra* note 1.

[200] *Id*.

[201] *Quon*, 130 S. Ct. at 2630.

[202] *Id.*

If that becomes the basis for a standard, then employers with the financial and technical wherewithal have an advantage. Employees, particularly those who lack 21st-century new media skills, would be clearly disadvantaged.

Within the singular category of employees, what standard should we apply to employees who are more technologically sophisticated, who actively attempt to stay off the employer–provided grid? What if all their activities are conducted in the "cloud" and they are simply using employer-provided platforms to access their private communications platforms and data? Will courts recognize the employees' efforts to protect their privacy and rule accordingly? It could be argued that technologically sophisticated persons would be provided with a higher-level privacy protection than persons who are not as sophisticated. That suggests that a dual standard is being created with multiple levels of protection. This dual standard would violate concepts of equality afforded protection in the Equal Protection and Due Process Clauses of the U.S. Constitution.[203] The cases reviewed above would suggest that several alternative scenarios dependent upon the type of employer may have an impact on these questions. Any time a government employer provides the hardware, software and/or Internet access for employee use, the employee has a limited expectation of privacy.[204] Private employers who have clear, uniformly enforced company polices also create a limited expectation of privacy in employees, but might create "notice" issues if the policy is unpublished, vague or not clearly communicated.[205] However, if the employee can access private, password protected communication platforms, e.g., voice, SMS, e-mail, etc., then communication on those private, personal platforms is either protected if it is privileged, as in *Stengart*, or has an increased level of privacy expectation, but might not be protected, as in *Quon*.[206] As Justice Scalia notes in *Quon*, ''[a]pplying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case, we have no choice . . . . The-times-they-are-a-changin' is a feeble excuse for disregard of duty."[207]

RECOMMENDATIONS

Developing case law, including the recent *Quon* decision, and pending or proposed federal and state legislation, strongly suggest both public and private employers must address developing technology and new media.[208] Companies today must address issues that accompany the use of new media by creating new company polices that address not only privacy concerns, but concerns of risk, litigation and loss.[209] "By implementing policies to address social media usage, and making employees aware of those policies, businesses can reduce their

---

[203] U.S. CONST. amend. XIV, § 1.

[204] *See O'Connor*, 480 U.S. at 709; *Quon*, 130 S. Ct. at 2619.

[205] *See Stengart*, 990 A.2d at 650.

[206] *Stengart*, 990 A.2d at 650; *Quon*, 130 S. Ct. at 2619.

[207] *Quon*, 130 S. Ct. at 2635.

[208] *Id.*

[209] Deloitte LLP Survey, *supra* note 33.

exposures to legal liabilities, breaches of proprietary information and damage to a company's brand and reputation."[210] Employers must take a top down approach, beginning with a review of the information that the company and employees share online, review security settings regularly and policies that address sharing of work-related information.[211] Telephone, Smartphone and email usage must be reviewed and updated in light of developing case law such as *Quon* and *Stengart*.[212]

> E-mail search is one of the most politically charged areas CIOs will encounter. Almost every organization's official policy is that e-mail is owned by the company and employees have no expectation of privacy, yet almost every survey respondent limited e-mail search to the individual level, with only 3% allowing search within departments or teams.[213]

Yet, as Quon shows, e-mail is not the only concern that companies must face when addressing new media.[214]

Employers must decide whether or not to filter access to social networking sites, blogs, etc. at specific times[215] or completely, or how and when to monitor sites.[216]

> While such a policy will prohibit unwanted Internet surfing and the use of company computers for negative posts, the gain in productivity could be offset by the negative effects of preventing employees from effectively networking with friends and past colleagues or conducting research for business purposes and a decrease in employee morale particularly among younger, more technologically savvy employees.[217]

> The danger is that by completely denying staff access to their favourite social networking site, organizations will drive their employees to find a way round the ban – and this could potentially open up even greater holes in corporate defenses . . . . Let's not also forget that social networking sites can have beneficial business purposes for some firms too, giving them the chance to network with existing customers and potential prospects.[218]

"Prior cases demonstrate that the tipping point in work-related, free speech cases dealing with personal time and/or personal computer equipment may be

---

[210] BUSINESS INSURANCE, *supra* note 24.

[211] *Web 2.0*, *supra* note 34.

[212] *Quon*, 130 S. Ct. at 2619; *Stengart*, 990 A.2d 650.

[213] Healy, *supra* note 48.

[214] *Quon*, 130 S. Ct. at 2619.

[215] Sophos Press Release, *supra* note 1.

[216] *Web 2.0*, *supra* note 34.

> One very simplistic approach is to prohibit access to social networking sites and blogs from computers on the company network. According to a survey in February 2008, over 65 percent of companies use some form of Internet blocking software to prohibit employee access to certain sites with 50 percent of those companies blocking access to social networking sites and 18 percent to external blogging sites.

Id.

[217] *Id.*

[218] Sophos Press Release, *supra* note 1.

whether there was an explicit policy in place by the employer dealing with speech regarding work and work-related issues."[219] Current case law suggests that this balancing of rights and expectations is developing but not at the pace that new media is evolving.[220]

New media policies should remind employees that negative or disparaging comments about the company that are posted to blogs or social networking pages are a breach of their duty of loyalty to their employer which may result in termination (particularly in at-will employment states).[221] Employees should be encouraged either to refrain from identifying themselves as employees of the company in blog or social networking posts or to include a disclaimer that states that their opinions are personal in nature and do not reflect those of their employer.[222] Employers must also remember to update other company policies that are impacted by new media, such as overall technology and internet policies, harassment policies and discrimination policies.

Once a company has a policy, the employer must publicize, educate and train employees. Employees must be trained as to the content of the policy, the expectation of the employer and the ramification of any policy breaches. "Make sure all employees are aware of the impact that their actions could have on the corporate network; educate your workforce about online risks."[223] Employers, as we have learned from *Quon*, must uniformly support and enforce policies in order to validate the policies and reaffirm the top down approach.[224]

Thereafter, employers must continue the process. They must have a solution in place that can proactively scan all websites for improper employee use, malware, spam and phishing content.[225] As stated earlier, paranoia over privacy concerns can inhibit some employers from instituting practices and procedures that would greatly benefit the company,[226] however, given the inherent risk posed by not addressing new media concerns, companies must find a way to allay fears over privacy in order to protect themselves. Employers can do so by encouraging management to follow technology trends and educating management and employees on risks, policies and expectations. Companies must also improve communication within the company itself, so that employees feel part of the process of incorporating new media into the workplace to the benefit of both employer and employee.

---

[219] Mark G. McCreary, *Privacy in Work-Related Matters Discussed In Social Networking Sites*, PRIVACY COMPLIANCE & DATA SECURITY, Apr. 27, 2009, *available at* http://dataprivacy.foxrothschild.com/2009/04/articles/privacy-rights/privacy-in-workrelated-matters-discussed-in-social-networking-sites/.

[220] *Quon*, 130 S. Ct. at 2629.

[221] *Web 2.0*, *supra* note 34.

[222] *Id.*

[223] Sophos Press Release, *supra* note 1.

[224] *Quon*, 130 S. Ct. at 2619.

[225] Sophos Press Release, *supra* note 1.

[226] Healy, *supra* note 48.

CONCLUSION

It is clear that employers and employees must adapt to the challenges that new media poses to our social systems. Our social systems however, are not necessarily capable of responding in a timely manner to the extraordinary speed with which technology is changing. There is also no question that the opportunities presented by new media to enhance communication, collaboration, and productivity are having a dramatic impact on the workplace.[227] As a result, employers will continue to provide access or risk a loss of competitiveness.[228] Employment, and other issues that will surely develop, must be examined within the broader context of the pace of technological change, its impact on social systems, and their relationship to the privacy rights of individuals, most particularly where those individuals interact in the employment arena.[229] The critical question that we face is not whether, but how quickly our systems can accommodate the impact of new media. Of course, faced with the bewildering pace of technological change and the delays our systems historically experience, employers, employees, legislatures and courts must take action. The review of cases, social literature and emerging employment disputes support the Supreme Court's decision in *Quon* to continue to review cases addressing issues arising from new media on a case-by-case basis.[230] The analysis recognizes the difficulty in adopting a broad standard at this point in time, but as Justice Scalia suggests, there can be no excuses.[231]

---

[227] Sophos Press Release, *supra* note 1.

[228] *Id*.

[229] *Quon*, 130 S. Ct. at 2629.

[230] *Id*. at 2628 (citing *O'Connor*, 480 U.S. at 717).

[231] *Quon*, 130 S. Ct. at 2635.