Hofstra Labor & Employment Law Journal

Volume 30 | Issue 2 Article 7

2013

Then and Now: How Technology has Changed the Workplace

Nancy B. Schess, Esq.

THEN AND NOW: HOW TECHNOLOGY HAS CHANGED THE WORKPLACE

*Nancy B. Schess, Esq.**

I. INTRODUCTION

When this law journal's first issue was published in 1983, the workplace was, technologically speaking, a very different place. There was no e-mail,[1] no texting,[2] and no instant messaging.[3] While some workplaces maintained central mainframe computers, there were no laptops, or tablets and precious few personal computers.[4] There were no personal data assistants (PDAs) or smart phones.[5] There was no Internet

* Nancy B. Schess, Esq. is a partner in the law firm of Klein Zelman Rothermel LLP, a boutique firm representing management in all aspects of labor and employment law located in Manhattan. She is grateful to her colleagues Charles Caranicas, Esq., Jesse Grasty, Esq. and Caroline Bishop, Esq., associates with the firm, for their significant work and substantive contribution to this article.

1. While the first e-mail can be traced back to 1971, e-mail communication as we know it today did not come into existence until 1996, when free internet e-mail became available. Sarah Left, *Email Timeline*, GUARDIAN (Mar. 13, 2002), http://www.guardian.co.uk/technology/2002/mar/13/internetnews.

2. Chris Gayomali, *The Text Message Turns 20: A Brief History of SMS*, THE WEEK (Dec. 3, 2012), http://www.theweek.com/article/index/237240/the-text-message-turns-20-a-brief-history-of-sms.

3. Jeff Tyson & Alison Cooper, *How Instant Messaging Works*, HOW STUFF WORKS, http://computer.howstuffworks.com/e-mail-messaging/instant-messaging.htm (last visited Apr. 15, 2013).

4. *See Indicators 2000 – Chapter 9: Significance of Information Technologies – IT and the Citizen*, NATIONAL SCIENCE FOUNDATION, http://www.nsf.gov/statistics/seind00/frames.htm (last visited Apr. 15, 2013); *see also* Tracy V. Wilson & Robert Valdes, *How Laptops Work*, HOW STUFF WORKS, http://www.howstuffworks.com/laptop6.htm (last visited Apr. 15, 2013); John Markoff, *Microsoft Brings in Top Talent to Pursue Old Goal: The Tablet*, N.Y. TIMES (Aug. 30, 1999), http://www.nytimes.com/1999/08/30/business/microsoft-brings-in-top-talent-to-pursue-old-goal-the-tablet.html.

5. Harry McCracken, *Newton, Reconsidered*, TIME (June 1, 2012), http://www.techland.time.com/2012/06/01/newton-reconsidered/; *see* Brad McCarty, *The History of the Smartphone*, NEXT WEB (Dec. 6, 2011), http://www.thenextweb.com/mobile/2011/12/06/the-history-of-the-smartphone/.

as we know it today, no social media (e.g. Facebook, LinkedIn), and no tweeting.[6] For the legal profession, computerized research had entered the workplace but only on dedicated terminals.

The business world communicated by landline telephone, by mail or in person. Even facsimile transmissions and voice mail (or answering machines) were relatively new phenomena and were not readily available in all workplaces. Telecommuting was rare and the end of the workday had clearer delineation since taking work home required advance planning and often permission.

As technological advances have come into the workplace and become commonly used, they have challenged existing legal principles requiring the re-examination of traditional rules regulating workplace behavior. In this article we will discuss four areas of law which have adapted, and continue to adapt, to embrace workplace changes occasioned by new technology; specifically: a) wage and hour compliance; b) liability issues in discrimination and harassment cases; c) employee privacy protections; and d) the lawful scope of employer policies restricting social media communications. In each of these areas, employers are now compelled to look critically at how technology impacts their workplace and the legal principles that create the roadmaps, as well as liabilities associated with those technologies.

II. THE CHANGING BORDERS OF THE WORKPLACE: WAGE AND HOUR COMPLIANCE

The Fair Labor Standards Act ("FLSA") governs how employees in American workplaces must be paid.[7] Of particular relevance here, employees who are not exempt from coverage (i.e. "non-exempt") must be paid no less than minimum wage for "hours worked" in a week up through forty and at least one-and-one-half times that rate for hours worked over forty.[8] Only workers who fall into particular categories,

6. *See* Dr. Anthony Curtis, *The Brief History of Social Media*, U. OF N.C. AT PEMBROKE, http://www.uncp.edu/home/acurtis/NewMedia/SocialMedia/SocialMediaHistory.html (last visited Apr. 15, 2013).

7. Fair Labor Standards Act of 1938, 29 U.S.C. §§ 201-219 (2006). Corollary state laws similarly regulate compensation in the workplace. *See e.g.* N.Y. LAB. LAW § 1 199. (McKinney 2009).

8. This rule applies both under federal and New York state law. 29 U.S.C. §§ 206–207; N.Y. LAB. LAW § 652; *see also* N.Y. COMP. CODES R. & REGS. tit. 12, §§ 141-1.3, 141-1.4, 142-2.1, 142-2.2, 142-3.1, 142-3.2, 146-1.2 and 146-1.4 (Supp. I 2013). Some states require overtime pay in other circumstances. For instance, California requires that work in excess of eight hours in a workday be compensated at the rate of at least one-and-one-half times the regular rate of pay and

such as executives, administrative employees and professionals as defined by law (i.e. "exempt"), need not be paid overtime for hours worked over forty.[9] Moreover, the law requires detailed recordkeeping of hours worked to ensure that non-exempt employees are paid correctly.[10]

Violation of wage and hour laws brings significant remedies, which include liquidated damages and attorneys' fees.[11] There can also be personal liability associated with failure to pay wages.[12] Moreover,

---

that work in excess of twelve hours in a workday be compensated at the rate of at least double the regular rate of pay. CAL. LAB. CODE § 510 (West 2011).

9. 29 U.S.C. § 213; *see* 29 C.F.R. § 541.0 (2012); *see also* N.Y. COMP. CODES R. & REGS. tit. 12, §§ 141-3.2, 142-2.14, 142-3.12, and 146-3.2.

10. 29 U.S.C. § 211(c); 29 C.F.R. § 516.2(a) (2012); N.Y. LAB. LAW §§ 195(4), 661 (2011). Notably, the FLSA does not distinguish between work performed at the office and work performed at home. 29 C.F.R. § 785.12 (2011). Thus, an employer's obligation to keep accurate records of hours worked is the same, regardless of where the work is performed. *See id.*

11. 29 U.S.C. § 216(b). If the employer's violation is deemed willful, the FLSA provides a three-year statute of limitations. 29 U.S.C. § 255(a) (1998). Violations are willful "if the employer knew or showed reckless disregard for the matter of whether its conduct was prohibited by [a statute]." Trans World Airlines, Inc. v. Thurston, 469 U.S. 111, 128 (1985). Where the violation is not willful the statute of limitations is two years. 29 U.S.C. §255(a). The FLSA provides employees with additional remedies, including liquidated damages up to 100% of the unpaid wages, attorneys' fees and costs. 29 U.S.C. § 216. Willful violators may also be prosecuted criminally and fined up to $10,000 or imprisoned for up to six months. *Id.* §216(a). Employers who willfully or repeatedly violate the minimum wage or overtime pay requirements are also subject to civil money penalties of up to $1,100 per violation. *Id.* §216(e)(2) (Supp. 2012).
New York Labor Law similarly provides for up to 100% liquidated damages as well as attorneys' fees. N.Y. LAB. LAW § 198(1-a) (2011). Moreover, New York Labor Law allows employees to recover unpaid wages for the six years preceding the commencement of their lawsuit. *Id.* § 198(3). New York Labor Law also provides civil penalties of $500 for each violation and criminal penalties ranging from $500 to $20,000, as well as imprisonment for up to a year. N.Y. LAB. LAW §§ 197, 198-a (2011).

12. *See* N.Y. BUS. CORP. LAW, § 630 (McKinney 2003) (imposing individual liability for unpaid wages on the ten largest shareholders of privately held New York corporations). Under the FLSA, "employer" is defined to include "any person acting directly or indirectly in the interest of an employer in relation to an employee . . . ." 29 U.S.C. § 203(d). "The Supreme Court has emphasized the 'expansiveness' of the FLSA's definition of employer." Herman v. RSR Security Services Ltd., 172 F.3d 132, 139 (2d Cir. 1999) (citing Falk v. Brennan, 414 U.S. 190, 195 (1973)). In determining whether an individual is an employer, "the overarching concern is whether the alleged employer possessed the power to control the workers in question, with an eye to the 'economic reality' presented by the facts of each case." *Id.* (citations omitted). This broad definition of "employer" does not require an ownership interest in the employer entity for individual liability to attach. It includes corporate officers with operational control of the employer, Chan v. Sung Yue Tung Corp., No. 03 Civ. 6048, 2007 WL 313483, *12 (S.D.N.Y. Feb. 1, 2007) (quoting Donovan v. Agnew, 712 F.2d 1509, 1511 (1st Cir. 1983)), as well as non-officer managers/supervisors. *See e.g.*, Mendez v. Pizza on Stone, LLC, 2012 WL 3133522 (S.D.N.Y. August 1, 2012); "The Supreme Court has emphasized the 'expansiveness' of the FLSA's definition of employer." *Herman v. RSR Security Services Ltd.*, 172 F.3d 132, 139 (2d Cir. 1999) (citing *Falk v. Brennan*, 414 U.S. 190, 195 (1973)). In determining whether an individual is an employer, "the

wage and hour cases are often easily articulated as collective and class actions under federal and state law, respectively.[13] Taking these ever increasing penalties into account, employers are wise to understand how to pay their employees in compliance with applicable law.

Yet, with the advent of modern technology the edges of compensable "hours worked" have blurred. PDAs, cell phones, laptops and programs that connect home and work computers have changed the traditional workspace since work can now easily be performed outside the physical office, which has increased opportunities for legally compensable time.

A. After Hours "Off the Clock" Communications

While technology that permits easy access to the office may arguably make the workplace more productive, it also exposes employers to potential liability for "off-the-clock" work performed by non-exempt employees. For example, when a non-exempt employee reads and responds to work e-mails or revises a document on his home computer after regular work hours have ended, the work may be compensable.[14]

Under the FLSA, non-exempt employees who take on after-hours work through such electronic connections generally must be paid for their time, so long as it is more than *de minimis*.[15] Whether an employer

---

overarching concern is whether the alleged employer possessed the power to control the workers in question, with an eye to the 'economic reality' presented by the facts of each case." *Id.* (citations omitted). This broad definition of "employer" does not require an ownership interest in the employer entity for individual liability to attach. It includes corporate officers with operational control of the employer, Chan v. Sung Yue Tung Corp., No. 03 Civ. 6048, 2007 WL 313483, *12 (S.D.N.Y. Feb. 1, 2007) (quoting Donovan v. Agnew, 712 F.2d 1509, 1511 (1st Cir. 1983)), as well as non-officer managers/supervisors. *See e.g.*, Mendez v. Pizza on Stone, LLC, 2012 WL 3133522 (S.D.N.Y. August 1, 2012).

13. *See* FED. R. CIV. P. 23; 29 U.S.C. § 216; N.Y. C.P.L.R. 901(McKinney 2005). The first quarter of 2010 saw 1,844 wage and hour class actions, setting a pace for 25% more wage and hour class actions than 2009, which saw 40% more than 2008. Gary Mathiason & SoRelle B. Brown, *Avoiding Class-Actions and Winning in Court*, HUM. RES. EXEC. ONLINE (June 16, 2010), http://www.hreonline.com/HRE/view/story.jhtml?id=453896146.

14. Karla Grossenbacher, *Electronic Handheld Devices, Can You Give Them to Non-Exempt Employees?* EMP. LAW STRATEGIST (June 2012), http://www.seyfarth.com/dir_docs/publications/GrossenbachrLJN.pdf.

15. When an FLSA claim "concerns only a few seconds or minutes of work beyond the scheduled working hours, such trifles may be disregarded." Lewis v. Keiser Sch., Inc., No. 11-62176-Civ, 2012 WL 4854724, at *2 (S.D. Fla. Oct. 12, 2012) (quoting Anderson v. Mt. Clemens Pottery Co., 328 U.S. 680, 692 (1946)). "Most courts have found daily periods of approximately 10 minutes to be *de minimis*." *Id.* (quoting Burks v. Equity Group-Eufaula Div., LLC 571 F. Supp.2d 1235, 1247 (M.D. Ala. 2008).

must pay technically turns on whether or not the employer knew or should have known that the employee was performing the work.[16]

In the context of electronic communications, it is not difficult to cross the line to dangerous employer knowledge. For example, in an effort to be efficient, a supervisor sends an email to his non-exempt subordinate after hours asking about the status of a project. The subordinate, in an effort to be responsive, answers the email providing an update on the work. While the responsive email may have taken only a few minutes to compose, the subordinate spends some time reviewing emails so that his response is accurate. While efficient as to the work performed, this scenario can create compensable time, even where the supervisor may not have actually known that the subordinate was going to check emails to provide a response to his question but perhaps should have known that he would do so. Moreover, consider whether the employee truly understands that he should be reporting this time worked on his timecard for the week.

Similarly, consider the scenario where a dedicated staff member chooses on her own to check email after dinner from her home computer and responds to several requests for information that she was not able to complete during the day. While she was not asked to do so, the manager receiving her emails—which clearly show the time when the work was performed—gratefully acknowledges and accepts her work product.

Where employees communicate with and about work after hours, employers who do not pay face the risk of litigation.[17] When the employer accepts the work product, the law will assume that it knew the

16. *See* Chao v. Gotham Registry, Inc., 514 F.3d 280, 287 (2d Cir. 2008); Davis v. Food Lion, 792 F.2d 1274, 1276 (4th Cir. 1986); Forrester v. Roth's I.G.A. Foodliner, Inc., 646 F.2d 413, 414 (9th Cir. 1981); 29 U.S.C. § 203(g); Grossenbacher, *supra* note 14.

17. *See, e.g.,* Allen v. City of Chi., No. 10 C 3183, 2011 WL 941383, at *1 (N.D. Ill. Mar. 15, 2011) *class cert. granted*, No. 10 C 3183, 2013 WL 146389 (N.D. Ill. Jan. 14, 2013), (denying a motion to dismiss when a police sergeant sued the City of Chicago alleging that he was owed overtime because he spent time checking email and responding to other electronic communications while off duty); Kuebel v. Black & Decker Inc., 643 F.3d 352, 364 (2d Cir. 2011) (reversing summary judgment in favor of employer and holding that, despite the fact that employee had improperly filled out his timesheets, he had raised a triable issue of fact with respect to his claimed overtime hours, including hours worked from home, checking and responding to voicemails and emails, printing and reviewing sales reports and organizing materials); Zulauf v. Amerisave Mortg. Corp., 1:11-CV-1784-WSD, 2012 WL 5987860, at *1 (N.D. Ga. Nov. 29, 2012) (alleging plaintiffs were not paid for overtime when they routinely worked more than 40 hours per week, including time spent using their phones and other devices to respond to emails and calls; the court granted defendant's motion to decertify the class, finding a lack of commonality amongst the plaintiffs); *see* Laura L. Ho, Briana Cummings & Ellen C. Kerns, *Hot Topics in Federal and State Wage and Hour Litigation,* CURRENT DEVELOPMENTS IN EMPLOYMENT LAW: THE OBAMA YEARS AT MID-TERM 433, 451 (2011).

work was being performed and, therefore, the employee must be compensated.[18] Notably, the device itself will often provide a record of the fact that the work was done after hours.[19]

In order to head off such risks, employers should create policies about after hours work and clearly communicate those policies to employees. Furthermore, employers should make sure to train non-exempt staff in addition to its well-meaning but potentially liability creating managers about the importance of complying with the rules. For example, some employers have implemented "no technology after hours" policies.[20] Furthermore, some employers have gone so far as to prevent their servers from sending messages to employees outside of work hours, although lifestyle issues have also driven such policies.[21] Notably, if an employer maintains a general policy of prohibiting employees from working overtime without management approval, it is important to communicate that after hours work requires the same approval.[22]

In all cases, employees must be instructed that any after-hours work must be reported and the employer's record keeping procedures should

18. 29 C.F.R. § 785.13 (2011) ("it is the duty of the management to exercise its control and see that the work is not performed if it does not want it to be performed. It cannot sit back and accept the benefits without compensating for them."); *see, e.g.*, Brennan v. Qwest Commc'ns Int'l, Inc., 727 F. Supp. 2d 751, 755 (D. Minn. 2010); Berrios v. Nicholas Zito Racing Stable, Inc 849 F. Supp. 2d 372, 388 (E.D.N.Y. 2012). *But see, e.g.,* Kellar v. Summit Seating Inc., 664 F.3d 169, 177-78 (7th Cir. 2011). According to some commentators, even the very issuance of a handheld device or laptop to a non-exempt employee could support an argument that the employer intended that the employee read and respond to e-mails after hours. *See, e.g.,* Grossenbacher, *supra* note 14.

19. *See generally Allen*, 2011 WL 941383, at *1.

20. For example, the Atlanta-based shipping company PBD Worldwide has implemented a nights-free and weekends-free e-mail policy, and the Washington D.C. consulting firm The Advisory Board Company recently instructed its employees to stay off work e-mail during non-work hours. Cecilia Kang, *Firms Tell Employees: Avoid After Hours E-mail*, WASH. POST, (Sept. 21, 2012), http://www.articles.washintponpost.com/2012-09-21/business/35497074_1e-mail-work-culture-balckberrys.

21. For its employees in Germany, Volkswagen servers "stop routing emails 30 minutes after the end of employees' shifts, and then start again 30 minutes before they return to work." *Volkswagen Turns Off Blackberry Email After Work Hours*, BBC NEWS: TECHNOLOGY (Dec. 23, 2011), http://www.bbc.co.uk/news/technology-16314901. The French technology firm Atos even reported plans to end e-mail altogether. "Managers had been wasting five to 20 hours a week just reading and responding to e-mail, the firm said. Instead, it will use instant messaging and other tools to communicate among staff." Kang, *supra* note 20.

22. Even if an employee works without approval however, the work must be paid for if the employer knew or had reason to know the work was performed. *See* Chao v. Gotham Registry, Inc., 514 F.3d 280, 287 (2d Cir. 2008); Reich v. Stewart, 121 F.3d 400, 407 (8th Cir. 1997); Forrester v. Roth's I.G.A. Foodliner, Inc., 646 F.2d 413, 414 (9th Cir. 1981); Mumbower v. Callicott, 526 F.2d 1183, 1188 (8th Cir. 1975) ("The employer who wishes no such work to be done has a duty to see it is not performed."); 29 C.F.R. § 785.13.

be adapted to be able to record such work.[23] This process is not only legally required but also provides some mechanism for employers to monitor work being performed outside of the ordinary workday.[24] Interestingly, the U.S. Department of Labor has created an "app" for handheld devices designed to help employees independently track hours worked.[25]

B. On Call Employees

Pursuant to the FLSA, under certain circumstances, employees must be paid for "on call" time.[26] The proper inquiry for determining whether employees must be paid for "on call" work under the FLSA is "whether the employee is so restricted [during on-call hours] that he is effectively engaged to wait."[27] One of two predominant factors to be considered is "the degree to which the employee is free to engage in personal activities" during his/her "on call" time.[28]

Prior to communications devices such as pagers, cell phones and

---

23. *See* Grossenbacher, *supra*, note 14. Of course, it does not matter whether the employee performs work on company issued equipment or their own. The issue is whether or not the work was performed.

24. *See* Press Release, U.S. Dep't of Labor, Keeping Track of Wages: The U.S. Labor Department Has an App for That! (May 9, 2011), *available at* http://www.dol.gov/opa/media/press/whd/WHD20110686.htm.

25. *Id.*

26. "Time spent at home on call may or may not be compensable depending on whether the restrictions placed on the employee preclude using the time for personal pursuits." 29 C.F.R. § 553.221(d) (2011). "Whether time is spent predominantly for the employer's benefit or for the employee's is a question dependent upon all the circumstances of the case." Ingram v. Cnty. of Bucks, 144 F.3d 265, 267-68 (3d Cir. 1998) (citing Armour & Co. v. Wantock, 323 U.S. 126, 133 (1944)); *see also* Owens v. Local No. 169 Ass'n of W.Pulp & Paper Workers, 971 F.2d 347, 350 (9th Cir. 1992).

27. Berry v. Cnty. of Sonoma, 30 F.3d 1174, 1183 (9th Cir. 1994); *see Owens*, 971 F.2d at 350 ("facts may show that the employee was 'engaged to wait,' which is compensable, or they may show that the employee 'waited to be engaged,' which is not compensable."); Moon v. Kwon, 248 F. Supp. 2d 201, 229 (S.D.N.Y. 2002) ("Time that an employee spends waiting for work assignments is compensable if the waiting time is spent 'primarily for the benefit of the employer and his business."); Skidmore v. Swift & Co., 323 U.S. 134, 137 (1944); Pabst v. Okla. Gas & Elec. Co., 228 F.3d 1128, 1135 (10th Cir. 2000); Birdwell v. City of Gadsden, 970 F.2d 802, 810 (11th Cir. 1992); Burnette v. Northside Hosp., 342 F. Supp. 2d 1128, 1135 (N.D. Ga. 2004); 29 C.F.R. § 553.221(d).

28. *Berry*, 30 F.3d at 1180; Brigham v. Eugene Water & Elec. Bd., 357 F.3d 931, 936 (9th Cir. 2004). On-call time is compensable if it "is so restricted that it interferes with personal pursuits." *Ingram*, 144 F.3d at 268; *see also* 29 C.F.R. § 553.221(c) ("Time spent away from the employer's premises under conditions that are so circumscribed that they restrict the employee from effectively using the time for personal pursuits also constitutes compensable hours of work"). The other predominant factor to be considered is any relevant agreement(s) between employer and employee. *Berry*, 30 F.3d at 1180; *Brigham*, 357 F.3d at 936.

PDAs, being "on call" often meant staying home to wait for a call to come to work. Modern communications technologies, however, enable employees to more freely engage in personal activities away from their office or home yet still be easily contacted by the employer should the "on call" need arise. This eases the restrictions on employees and may result in an ultimate determination that an employee is not so restricted that his/her "on call" time is compensable.[29] Without this liberating technology, on-call employees would be (and used to be) "effectively tethered to their homes."[30] "Of course, an employee need not 'have substantially the same flexibility or freedom as he would if not on call, else all or almost all on-call time would be working time, a proposition that the settled case law and the administrative guidelines clearly reject.'"[31]

C. Telecommuting

As technology has advanced, telecommuting has become an increasingly easy and efficient option for many employers and employees. Software such as *LogMeIn* and *GoToMyPC* allow employees seamless access to their work computers (and the office network/database) from the comfort of their homes, without the hassle of a commute.[32] These advances, however, have created new problems for employers. As explained above, an employer's obligation to keep accurate records of hours worked is not dependent upon where the work

29. *Berry*, 30 F.3d at 1184 (concluding that the "use of pagers eases restrictions while on-call and permits [plaintiffs] to more easily pursue personal activities"); *Owens*, 971 F.2d at 351; *Ingram*, 144 F.3d at 268; Cannon v. Vineland Hous. Auth., 627 F. Supp. 2d 171, 177 (D.N.J. 2008) ("an employee's capacity to carry a pager and leave home weighs in favor of finding his on-call waiting time non-compensable"); Henry v. Med-Staff, Inc., No. SA CV 05-603 DOC ANX, 2007 WL 1998653, *11 (C.D. Cal. July 5, 2007) ("Cell phones likewise ease restrictions, by freeing employees to travel wherever they wish during on-call assignments as long as their destinations have cell phone reception . . . [which] weighs against compensating on-call time . . . .").

30. *See Brigham*, 357 F.3d at 937.

31. *Id.* at 936; *Owens*, 971 F.2d at 350-51. The U.S. Dep't of Labor's (DOL) Field Operations Handbook addresses "on-call" employees required to remain at home. In that context, the DOL "will accept any reasonable agreement of the parties for determining the number of hours worked." WAGE AND HOUR DIV., U.S. DEP'T. OF LABOR, FIELD OPERATIONS HANDBOOK, § 31b14 (2000), *available at* http://www.dol.gov.whd/FOH/FOH_Ch31.pdf. In addition to payment for time actually worked, such agreement should provide for "some allowance for the restriction on the employee's freedom to engage in personal activities . . . ." *Id.*

32. *See About Us*, LOGMEIN, https://secure.logmein.com/about/aboutus.aspx (last visited Apr. 15, 2013); *How it Works*, GOTOMYPC, http://www.gotomypc.com/remote_access/remote_access (last visited Apr. 15, 2013).

is performed.[33] While computer software allows employers to keep track of when employees login and logout, employers must still be able to account for any time the employee worked while logged-out. Thus, it is imperative that employers have a clear policy with respect to hours worked by non-exempt telecommuters (*e.g.*, telecommuters must fill out and sign daily time sheets).

In addition, for a telecommuting employee, employers should consider whether he or she will be working on company issued, or personal, equipment in performing job responsibilities. If using personal equipment, issues such as ownership of work product, employer confidentiality and privacy arise when business records are created on, maintained on and/or accessed through the employee's home computer.[34] Even where company equipment is used, since the workspace is now in the employee's home, a lack of appropriate safeguards may allow non-employees to have access to an employer's proprietary information.[35]

The federal government's *Guide to Telework in the Federal Government*, which was created for federal employees, is instructive on these issues, albeit not specifically applicable to private employers. The *Guide* requires that employees "take responsibility for the security of the data and other information they handle while teleworking," and enter into a written agreement and participate in an interactive telework training program.[36]

III. THE NEW FRONTIER IN DISCRIMINATION AND HARASSMENT CASES: ELECTRONIC COMMUNICATIONS

Federal, state and local laws prohibit discrimination and harassment in the workplace.[37] These prohibitions are not new, given statutes that go back to the mid 1960s. What is new, however, is the type of conduct

33. *See supra* note 10 and accompanying text.

34. Jeff Tenenbaum, *Telecommuting Employees,* EXEMPT, (June 14, 2012), http://www.exemptmagazine.com/article/detail/telecommuting-employees-4324.

35. *Id.*

36. OFFICE OF PERS. MGMT., GUIDE TO TELEWORK IN THE FEDERAL GOVERNMENT 27-28 (2011), http://www.telework.gov/guidance_and_legislation/telework_guide/telework_guide.pdf.

37. Federal law protects employees from discrimination based upon protected characteristics such as age, citizenship, sex, pregnancy, military/veteran status, race/color, religion, disability, predisposing genetic characteristics, and national origin. Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e-2 (2006); Americans with Disabilities Act, 42 U.S.C. § 12112(a) (2006); Age Discrimination in Employment Act of 1967, 29 U.S.C. § 623 (2006); *see also* N.Y. HUMAN RIGHTS LAW § 291(1) (McKinney 2010).

that is increasingly creating employer liability.[38]

Specifically, the same modern communications technology that improves connectivity and productivity has also created potential liabilities for employers. First, as technology has become more sophisticated, there has been a concomitant increase in the potential for inappropriate communications by employees whether through text messages, email, social media or other forms of technology.[39] Second, the vast amount of information available to employers without restriction via the internet has created opportunity for claims of discrimination that did not exist before these technological advancements.[40]

A. Relaxed and Dangerous Communications

Some commentators espouse that the ease of electronic communication diminishes beneficial inhibitions and that employees may become less diligent about treating electronic exchanges as business communications.[41] As a result, people tend to say things they would not ordinarily say. "Cyberspace gives people more than an illusion of

38. This liability can extend past discrimination and harassment cases. In one case in Louisiana, an employer was held vicariously liable for a car accident caused by its employee (a traveling sales manager). Ellender v. Neff Rental, Inc., 965 So.2d 898 (La. Ct. App. 2007). The employee was on a business call on his cell phone while driving and the employer had no policy or practice prohibiting cell phone usage while driving. *Id.* at 900-02; *see also* Buchanan v. Vowell, 926 N.E.2d 515, 517-18, 521-22 (Ind. Ct. App. 2010) (liability found against driver of car following other car that struck pedestrian where the drivers were speaking to one another by cell phone—and were inebriated—when the accident occurred); Ward v. Cisco Sys., Inc., No. CIV. 08-4022, 2008 WL 5101996 (W.D. Ark. Dec. 1, 2008) (alleged defamation based on statements made in a blog).

39. *See, e.g.*, Blakey v. Cont'l Airlines, 751 A.2d 538, 542-44 (N.J. 2000) (sexual harassment based on web forum postings); Garrity v. John Hancock Mut. Life Ins. Co., No. Civ. A. 00-12143, 2002 WL 974676, (D. Mass. May 7, 2002) (hostile environment based on sexually explicit e-mails); *Ward*, 2008 WL 5101996 (alleged defamation based on statements made in a blog); Complaint at 2-3, Guardian Civic League, Inc. v. Phila. Police Dep't, No. 2:09-cv-03148 –CMR (E.D. Pa. July 15, 2009) (No. 09-3148), *available at* http://www.dmlp.org/sites/citmedialaw.org/files/2009-07-15-Guradian%20Complaint.pdf (alleged hostile environment based on racially offensive web postings).

40. Social Media and the Workplace: Managing the Risks, JACKSON LEWIS, 3 (2010), http://www.jacksonlewis.com/media/pnc/3/media.1033.pdf (last visited Apr. 16, 2013).

41. "Due to the lack of social and physical cues online, people are less aware, and therefore less considerate about the other person's reaction." Larry Keller, *Cyberbullies Lurking in the Workplace*, HUM. RESOURCE EXECUTIVE ONLINE (Nov. 21, 2012), http://www.hronline.com/HRE/view/story/jhtml?id= 534354631 (quoting Carolyn Axtell, senior lecturer at the University of Sheffield's Institute of Work Psychology). "I see entire cases built on email correspondence, in large part because people don't take it as seriously as written correspondence." Dan Goodin, *Email Still Dangerous in Business*, CNET NEWS (Jan. 20, 1998), http://news.cnet.com/2100-1023-207240.html (quoting attorney Russ Elmer).

protection. . . . It allows for false fronts, a false bravado . . . ."[42]

In the course of litigation, electronic mail (or other forms of electronic communications) often contains admissions that in past years would have been nearly impossible to discover or corroborate.[43] Before the popularity of electronic communications, similar communications would have been almost entirely oral, delivered in person or by telephone, and would generally not have been preserved or retrievable. The "durable record" provided by electronic communications stands in sharp contrast.[44]

As a practical matter, potential electronic evidence is often attainable whether through a search of hard drives, backup media or otherwise and even conventionally deleted material is generally recoverable with sufficient technical prowess.[45] Even after conventional deletion, "data contained in the [deleted] file remains on the hard drive until it is overwritten. Theoretically, this data could remain on the hard drive forever."[46] To complicate employment litigation further, investigations that include e-mail and other electronic communications "rapidly become open-ended because there's such a huge quantity of information available and it's so easily searchable."[47]

---

42. Frank Bruni, *Our Hard Drives, Ourselves*, N.Y. TIMES OPINION PAGES (Nov. 17, 2012), http://www.nytimes.com/2012/11/18/opinion/sunday/Bruni-Our-Hard-Drives-Ourselves.html; *see generally* State v. Patino, No. P1-10-1155A (Sup.Ct. R.I. Sept. 4, 2012), *available at* http//www.courts.ri.gov/Courts/SuperiorCourt/DecisionsOrders/decisions/10-1155.pdf (granting motion to suppress text message evidence obtained without a search warrant).

43. *See* Goodin, *supra* note 41 ("In the litigation environment, it is often electronic mail that contains the most damning admissions.") (quoting David H. Kramer, internet law attorney).

44. *See* Bruni, *supra* note 42 ("In lieu of eavesdroppers whom he could have disputed, he had digital footprints that he couldn't deny, and they traced a path . . . to political ruin.") (discussing former Congressman Anthony Weiner).

45. *See* Tara Taghizadeh, *What Really Happens When You Press 'Delete'*, AOL DISCOVER, http://daol.aol.com/articles/what-is-delete (last visited Feb. 8, 2013).

46. John Mallery, *Secure File Deletion: Fact or Fiction?*, SANS INST. INFOSEC READING ROOM, 4 (last updated June 12, 2006), http://www.sans.org/reading_room/whitepapers/incident/secure-file-deletion-fact-fiction_631. Although there are methods to delete information securely from a computer's hard drive, they are rather complex and not commonly used in the ordinary course of business. *See id.* at 7-9; Wenner Media LLC v. N. & Shell N. Am. Ltd., No. 05 Civ. 1286, 2005 WL 323727, at *2 (S.D.N.Y. Feb. 8, 2005) (detailing the failed efforts of defendant in trying to permanently delete e-mails from company system).

47. Scott Shane, *Online Privacy Issue Is Also in Play in Petraeus Scandal*, N.Y. TIMES (Nov. 13, 2012), http://www.nytimes.com/2012/11/14/us/david-petraeus-case-raises-concerns-about-americans-privacy.html?_r=0 (quoting Marc Rotenberg, Executive Director of the Electronic Privacy Information Center in Washington, D.C.) Electronic discovery has become so vast that studies estimate that litigants spend between $1.2 billion and $2.8 billion annually on electronic discovery. Brian Dalton, *Letters From LegalTech: The Thrills of E-Discovery*, ABOVE THE LAW, (Jan. 31, 2013, 4:20 PM), http://www.abovethelaw.com/2013/01/letter-from-legaltech-the-thrills-of-

Court cases in the employment context hinging on the content of e-mail or other types of electronic messages are numerous. For example, in *Virola v. XO Commc'ns, Inc.*,[48] the court denied the employer's motion for summary judgment.[49] In finding that the plaintiffs had raised a triable issue of fact as to whether they were subjected to a hostile work environment based on sex, the court relied upon emails to one of the plaintiffs asking what she was wearing, telling her to stop "bsing" like a woman, and suggesting that they go to strip club.[50]

B. To Look or Not to Look?

Without question, employers can learn a great deal of information by reviewing a job applicant's social media presence. Social media affords employers the opportunity to acquire information that would have been virtually impossible to ascertain in the past. Not surprisingly, using social media as a recruiting tool to research candidates has become

---

e-discovery. In fact, electronic discovery has taken a prominent role in all federal litigation since Judge Shira A. Scheindlin's landmark decisions in *Zubulake v. UBS Warburg LLC* and *Zubulake v. UBS Warburg LLC*. These decisions set the framework for parties' electronic discovery obligations as well as how costs should be allocated. *See* Zubulake v. UBS Warburg LLC, 217 F.R.D. 309 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC 220 F.R.D. 212 (S.D.N.Y. 2003). Subsequent to Judge Scheindlin's decisions, on December 1, 2006, FED. R. CIV. P. 16, 26, 33, 34, 37 and 45 were amended. The amendments, amongst other things, codified *Zubulake*, explicitly added "electronically stored information" (ESI) as its own category under Rule 26(a), placed a greater burden on parties to meet and confer regarding e-discovery and required counsel to ensure that litigation holds and data destruction policies are defensible. *See* FED. R. CIV. P. 16, 26, 33, 34, 37 and 45. See generally *Best Practices in E-Discovery in New York State and Federal Courts, Report of the E-Discovery Committee of the Commercial and Federal Litigation Section of the New York State Bar Association,* N.Y. ST. B. ASS'N (July 2011), http://www.nysba.org/AM/Template.cfm?Section=Commercial_and_ Federal_ Litigation_Home&Template=CM/ContentDisplay.cfm&ContentID=58331, for additional guidance on electronic discovery.

48. No. 02-CV-5056, 2008 WL 1766601 (E.D.N.Y. Apr. 15, 2008).

49. *Id.* at *1, *17.

50. *Id.* at *9. Other examples of cases in which electronically stored information played a pivotal role are abundant. *See e.g.* DeCurtis v. Upward Bound Int'l, Inc., No. 09 Civ. 5378, 2012 WL 4561127 at *8 (S.D.N.Y. Sept. 27, 2012) (rejecting supervisor's denial of sexual harassment based on e-mail evidence to the contrary); Smith v. Reg'l Plan Assoc., No. 10 Civ. 5857, 2011 WL 4801522 at *2 (S.D.N.Y. Oct. 7, 2011) (racial harassment claim supported by e-mail evidence); D'Angelo v. World Wrestling Entm't, Inc., 3:08-CV-1548, 2010 WL 4226479 at *4 (D. Conn. Oct. 18, 2010) (defendant did "not cite a case, and the court has not located one, where a court disregarded sexual harassment because of the media (sic) used to convey it."); *Wenner Media LLC.*, 2005 WL 323727 at *4 -*5 (granting temporary restraining order to enforce a non-competition provision where efforts to delete incriminating e-mails had failed); Amira-Jabbar v. Travel Servs., Inc., 726 F. Supp. 2d 77, 81 (D.P.R. 2010) (in assessing plaintiff's claim of a racially hostile work environment the court considered a Facebook comment that a co-worker directed at plaintiff).

a modern phenomenon.[51]

However, when an employer learns information that it is not legally permitted to have, problems arise. Since employers are not permitted to discriminate on the basis of an applicant's protected characteristics (i.e., age, race, gender, etc.), the law prohibits various pre-employment inquiries that might lead to an employer acquiring impermissible information.[52] An employer may not make inquiries such as "do you wish to be addressed as Miss or Mrs.?" or "what religious holidays do you observe?"[53]

While it is not unlawful for an employer to search for public information about a candidate through social media, that exercise potentially uncovers, even unintentionally, information that the employer is not legally permitted to utilize when making decisions.[54] For example, assume a particular applicant has posted to a Facebook page news of her pregnancy which was (properly) not discussed during her job interview. If a hiring manager "googles" the applicant in an effort to learn more and stumbles upon this knowledge, his decision-making becomes potentially tainted. While his search in the first instance is not unlawful, if the applicant is not hired it will be that much more difficult to convince a trier of fact that the information about the applicant's pregnancy was not a factor in the decision.[55]

Along similar lines, some employers had started to require that applicants disclose usernames and passwords for the social networking

51. As of March 2013, Facebook had one billion monthly active users. *Facebook Newsroom Key Facts,* FACEBOOK, http:/newsroom.fb.com/Key-Facts (last visited May 10, 2013). A 2012 study conducted by Jobvite concluded, "nearly 3 out of 4 hiring managers and recruiters check candidates' social profiles – 48% always do so, even if they are not provided." *Jobvite Social Recruiting Survey Finds Over 90% of Employers Will Use Social Recruiting in 2012,* JOBVITE (July 9, 2012), http://www.recruiting.jobvite.com/company/press-releases/2012/jobvite-social-recruiting-survey-2012/.

52. EQUAL EMP. OPPORTUNITY COMM'N., PROHIBITED EMPLOYMENT POLICES/PRACTICES, http://www.eeoc.gov/laws/practices/index.cfm (last visited Jan. 31, 2013); *see also* N.Y. STATE DIV. OF HUMAN RIGHTS, RECOMMENDATIONS ON EMPLOYMENT INQUIRIES, 11-12 (Dec. 2004), http://www.nylaborandemploymentlawreport.com/uploads/file/Recommendations%20on%20Employment%20Inquiries.pdf.

53. N.Y. STATE DIV. OF HUMAN RIGHTS, *supra* note 52, at 11-12.

54. *See* C. Reilly Larson, *EEOC Lawyer Advised Careful Navigation of Issues in the Workplace,* BLOOMBERG BNA (Sept. 4, 2012), http://www.bna.com/eeoc-lawyer-advises-n17179869380/.

55. Employers that choose to use social media to research applicants would be wise to implement screening protocols such that those who conduct the searches are not the same managers making employment decisions. Employers should also carefully consider and delineate the legitimate non-discriminatory business information that is sought by the search to be conducted by approved screeners.

sites in which they participate so that employers could conduct research about their potential new hire.[56] However, in response to a general outcry that these types of requirements invaded aspects of privacy, these practices have been attacked. In March 2012, Erin Egan, Chief Privacy Officer, Policy, for Facebook issued a statement admonishing employers for asking prospective (or actual) employees to reveal their passwords suggesting that such a practice "undermines the privacy expectations and the security of both the user and the user's friends."[57] Several states have enacted legislation which in varying forms prohibits employers from requesting passwords as a condition to obtaining or retaining employment.[58]

IV. A REASONABLE EXPECTATION OF PRIVACY: MONITORING EMPLOYEE TECHNOLOGY

With thirty years of advances in communications technology have come complications with respect to traditional notions of employee privacy. From telephone calls to social media sites, employers have the technical capability to monitor a multitude of employee communications. However, whether such monitoring is lawful implicates fact intensive notions of employee privacy.

Perfectly clear lines have yet to be been drawn in this continually evolving area of law. As recognized by the U.S. Supreme Court in *City*

56. *See* Marisa Taylor, *Montana Town Stops Asking Applicants for Facebook Login,* WALL ST. J. BLOG (June 23, 2009, 8:13 AM), http://www.blogs.wsj.com/digits/2009/06/23/montana-town-stops-asking-for-facebook-logins/. Similar concerns were addressed by the United States District Court for the District of New Jersey in a case involving current employees and their online activities. *See* Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *1-2 (D.N.J. July 25, 2008). *See infra* Part IV.C. for further discussion on employer surveillance of employee social media.

57. Erin Egan, *Protecting Your Passwords and Your Privacy*, FACEBOOK (Mar. 23, 2012), http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057. Shortly, thereafter the Password Protection Act of 2012 was introduced in Congress which would have prohibited employers from compelling access to on-line information. *See* Password Protection Act of 2012, H.R. 5684, 112th Cong. (2012); Password Protection Act of 2012, S. 3074, 112th Cong. § 2 (2012). The legislation was not passed. *See* H.R. 5684 (112th): Password Protection Act of 2012, GOVTRACK, http://www.govtrack.us/congress/bills/112/hr5684 (last visited May 10, 2013).

58. According to the National Conference of State Legislatures, during 2012, six states enacted legislation prohibiting such conduct by employers (specifically, California, Delaware, Illinois, Maryland, Michigan and New Jersey) while multiple other states have similar legislation pending. *Employer Access to Social Media Usernames and Passwords: 2012 Legislation,* NAT'L CONF. ST. LEGIS. (Jan. 17, 2013), http://www.ncsl.org/issues-research/telecom/employer-access-to-social-media-passwords.aspx.

of Ontario, Cal. v. Quon:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. . . . At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. . . . Cell phone 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. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own.[59]

Where disputes arise, the issue generally boils down to whether the employee had a "reasonable expectation of privacy."[60] Yet, what constitutes an employee's "reasonable expectation of privacy" is not clear cut and "must be addressed on a case-by-case basis."[61] Clearly articulated and communicated employer policies often become the focal point of the analysis as such policies have been found to "shape the reasonable expectations of their employees."[62] Therefore, as

59. City of Ontario, Cal. v. Quon, 130 S.Ct. 2619, 2629-30 (2010). *Quon* involved a public employee and whether his Fourth Amendment rights had been violated by the City's monitoring of text messages. *See id.* at 2624. While *Quon* may be viewed as limited to its facts, the Court provided a roadmap to relevant considerations in determining whether an employee had a reasonable expectation of privacy and further stated that its reasoning would apply in the private-employer context. *See id.* at 2633. Interestingly, the Court observed that some states have "passed statutes requiring employers to notify employees when monitoring their electronic communications." *Id.* at 2630 (citing DEL. CODE ANN. tit. 19, § 705 (2005) and CONN. GEN. STAT. ANN. § 31-48d (West 2003)).

60. There are some statutory privacy protections, although they pre-date the explosion of modern communications technology. For example, the Electronic Communications Privacy Act of 1986 ("ECPA")—which includes the "Wiretap Act" and the Stored Communications Act ("SCA")—protects the privacy of electronic communications. The Wiretap Act protects against the interception of electronic communications. *See* 18 U.S.C. § 2511(1) (2006). The SCA, on the other hand, protects against the unauthorized access to electronic communications while in storage. *See* 18 U.S.C. § 2701 (2006). However, the ECPA does provide circumstances in which employers can legitimately retrieve electronic communications without violating the law. *See* 18 U.S.C. § 2511(2)(d). A party's explicit or implied consent is a defense. *See id.*; Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993). Additional defenses include the "ordinary course of business" exception which requires that an interception be "(1) for a legitimate business purpose, (2) routine and (3) with notice." Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001); U.S. v. Friedman, 300 F.3d 111, 122 (2d Cir. 2002); 18 U.S.C. § 2510(5)(a); *cf. Briggs infra* note 65.

61. *City of Ontario,* 130 S.Ct. at 2628.

62. *Id.* at 2630; *see also* State v. Young, 974 So.2d 601, 611 (Fla. Dist. Ct. App. 2008) (lack of applicable policy was factor in finding a reasonable expectation of privacy); Dukes v. ADS Alliance Data Sys., Inc., No. 2:03-CV-00784, 2006 WL 3366308, at *14 (S.D. Ohio Nov. 20, 2006)

demonstrated below, best practice dictates active and full communication with employees with respect to expectations of privacy and employee monitoring.

A. Telephone Monitoring

The genesis of employee monitoring is found in old-fashioned eavesdropping. Albeit using what seems today to be antiquated technology, consider the employer that chose (or chooses) to monitor employee telephone calls. Call centers and other phone based customer service businesses established entire protocols for monitoring phone calls as a tool for managing employee performance. One critical issue in evaluating whether an employee's privacy has been breached is whether the employee consented to having his communications monitored, either expressly or by implication.[63] The specific terms of an employer's policy (together with its methods of communication) are central to this evaluation. For example, while agreeing to a policy stating that calls are monitored with an aim toward improving employees' telephone skills and job performance may be consent for the monitoring of business calls, it is *not* implied consent to the monitoring of *personal* calls.[64] A number of judicial decisions in different jurisdictions bear this out.[65]

(reasonable expectation of privacy found where scope of monitoring policy was limited); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (clear employer policy that it could inspect company-issued laptop computers "destroyed any reasonable expectation of privacy"); Shefts v. Petrakis, 758 F. Supp. 2d 620, 631 (C.D. Ill. 2010); Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 560 (S.D.N.Y. 2008).

63. In addition to the privacy concerns implicated by monitoring phone calls, there are criminal statutes that prohibit the unauthorized interception of telephone calls. These laws vary by state, with some states permitting such eavesdropping or wiretapping with the consent of one party to the communication and others requiring the consent of both parties. *See, e.g.*, CONN. GEN. STAT. ANN. § 52-570d (West 2005) (two party consent); 18 PA. CONS. STAT. ANN. § 5704(4) (West Supp. 2012) (two party consent); N.J. STAT. ANN. § 2A:156A-4(d) (West 2011) (one party consent); N.Y. PENAL LAW §§ 250.00-.05 (McKinney 2008) (one party consent).

64. *Dukes*, 2006 WL 3366308, at *14. One court has held that a general policy that equipment provided by the employer may not be used for personal use does not provide notice sufficient to find consent to the monitoring of personal calls. *Adams*, 250 F.3d at 984 (employer-issued pagers).

65. *See* Deal v. Spears, 980 F.2d 1153, 1155 (8th Cir. 1992),where the owners of a liquor store, suspicious that their employee plaintiff had been involved in the theft of $16,000, installed recording equipment that automatically recorded all telephone conversations to and from the store. Informing plaintiff that they might monitor the phone "in order to cut down on personal calls," the owners listened to the entirety of twenty-two hours of taped conversations involving plaintiff. *Id.* at 1156. While learning nothing about the theft, they learned that plaintiff had violated a store policy and subsequently fired her. *Id.* There was no consent defense because the owners did not clearly inform plaintiff that they would be monitoring her calls, only that they *might* do so. *Id.* at 1157.

B. Monitoring E-Mail and Internet Usage

Employees using company equipment may have a difficult time establishing a reasonable expectation of privacy in their use of such equipment, particularly where the company has a policy on point. Said another way, the reasonableness of an employee's expectation of privacy can be severely curtailed by an employer's clear policy allowing for monitoring.[66] As one Court articulated, whether the plaintiff had a reasonable expectation of privacy with respect to communications sent or received on the company system "depends upon whether [the employer] had a policy in place regarding the monitoring of such communications, as well as whether Plaintiff was aware that [defendant] or others at [employer] may be monitoring his activities."[67]

Some courts have even held that when an employee communicates with his/her lawyer using the company computer, the attorney-client privilege is lost.[68] However, if such privileged communications were

---

Moreover, while the owners may have had a legitimate interest in monitoring calls in connection with their suspicions about theft or abuse of personal call privileges, "the scope of the interception in this case takes us well beyond the boundaries of the ordinary course of business." *Id.* at 1158; *see also* Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983) ("a personal call may be intercepted in the ordinary course of business to determine its nature but never its contents."); Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d. 914, 923 (W.D. Wis. 2002) (once the eavesdropping employees determined that plaintiff's call was personal (and not with a minor), "they had an obligation to cease listening and hang up."); Briggs v. Am. Air Filter Co., 630 F.2d 414, 420 n.9 (5th Cir. 1980) (monitoring of business call based on suspicion of disclosure of confidential information is within the ordinary course of business).

66. *See Pure Power Boot Camp,* 587 F. Supp. 2d at 559-60 ("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."). While the trend in the case law supports the importance of clearly articulated employer policies, an employer's policy is not always determinative. One early e-mail decision held that there was no expectation of privacy in use of the employer's e-mail system even where the employer "repeatedly assured its employees . . . that all e-mail communications would remain confidential and privileged" and that "e-mail communications could not be intercepted and used by [the employer] against its employees as grounds for termination or reprimand." Smyth v. Pillsbury Co., 914 F. Supp. 97, 98 (E.D. Pa. 1996); *see also* People v. Klapper, 28 Misc. 3d 225, 226 (N.Y. Crim. Ct. 2010) (finding no expectation of privacy in a criminal context stating "It is today's reality that a reasonable expectation of Internet privacy is lost, upon your affirmative keystroke. Compound that reality with an employee's use of his or her employer's computer for the transmittal of non-business-related messages, and the technological reality meets the legal roadway, which equals the exit of any reasonable expectation of, or right to, privacy in such communications."); Fazio v. Temp. Excellence Inc., No. A-5441-08T3, 2012 WL 300634, at *13 (N.J. Sup.Ct. Feb. 2, 2012) (no expectation of privacy even without email policy).

67. *Shefts*, 758 F. Supp. 2d at 633.

68. *See* Scott v. Beth Israel Med. Ctr., 17 Misc. 3d 934, 938 (N.Y Sup. Ct. 2007) (noting scope of defendant's e-mail policy); In re Asia Global Crossing, Ltd., 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005); *cf. Fazio*, 2012 WL 300634, at *13 (privilege lost even without email policy).

sent or received with reasonable steps taken to keep them from the employer (e.g., through a private e-mail account that was merely accessed through company-provided equipment), the privilege may survive.[69]

In certain circumstances, an employer may have an affirmative duty to investigate employee e-mails. For example, in one case, in response to a complaint by a co-worker, an employer fired certain employees after finding sexually explicit e-mails in their work e-mail folders that had been exchanged on the company system.[70] The court recognized no reasonable expectation of privacy because the allegedly sexually explicit e-mails were voluntarily sent to co-workers on the company's e-mail system.[71] The court went further however, and stated that even with a reasonable expectation of privacy, the employer's "legitimate business interest in protecting its employees from harassment in the workplace would likely trump plaintiffs' privacy interests. . . . [O]nce defendant received a complaint about the plaintiffs' sexually explicit e-mails, it was required by law to commence an investigation."[72]

C. Monitoring Employee Use of Social Media

Uncertainty in the law is particularly evident in the context of employee use of social media. As explained by one court, "[p]rivacy in social networking is an emerging, but underdeveloped, area of case law."[73] Some employers have attempted to monitor the online social media activities of their employees. While courts have held that there is

69. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010); *Pure Power Boot Camp*, 587 F. Supp. 2d at 561 (employee had reasonable expectation of privacy in personal email stored on commercial server that was password protected notwithstanding employee access while at work).

70. Garrity v. John Hancock Mut. Life Ins. Co., No. Civ. A. 00-12143-RWZ, 2002 WL 974676, at *1 (D. Mass. May 7, 2002).

71. *Id.* at *2. The defendant company had a policy in place stating that "there may be business or legal situations that necessitate company review of E-mail messages and other documents." *Id.* at *1.

72. *Id.* at *2; *see also* Blakey v. Cont'l Airlines, 751 A.2d 538, 552 (N.J. 2000) ("employers do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know that such harassment is part of a pattern of harassment that is taking place in the workplace and in settings that are related to the workplace."). The same principles have been applied with respect to monitoring employee Internet use. *See* Doe v. XYC Corp., 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005) ("an employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties.").

73. Ehling v. Monmouth–Ocean Hosp. Serv. Corp., 872 F. Supp. 2d 369, 373 (D.N.J. 2012).

no reasonable expectation of privacy as to materials posted to publicly available sites,[74] problems arise when employers attempt to look behind password protected walls. Courts have recognized an employee's reasonable expectation of privacy where access to the employee's communication is not public and is otherwise password protected.[75]

In one such case, a restaurant employee initiated a group discussion on *MySpace* designed to "vent about any BS we deal with out [sic] work without any outside eyes spying in on us."[76] A restaurant manager learned of the discussion group and asked an employee-member to provide him with the password so he could gain access—which the employee provided.[77] Management consequently fired two plaintiffs who had contributed "offensive" comments.[78] The Court denied the employer's summary judgment motion finding that if the employee gave management his password "under duress, then the Defendants were not 'authorized'" to access the site.[79]

V. THE NATIONAL LABOR RELATIONS ACT MEETS SOCIAL MEDIA

Since the advent of social media (*e.g.*, Facebook, LinkedIn, Twitter, Instagram), many employees utilize such media to stay connected with friends, family and even business contacts.[80] Unlike e-mail or instant

74. *Id.* at 373; *see, e.g.*, U.S. v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) ("it strikes the Court as obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any measures to protect the information.").

75. *See Ehling*, 872 F. Supp. 2d at 374. The *Ehling* Court ultimately determined that "given the open-ended nature of the case law[,]" the plaintiff "may have had a reasonable expectation" that a posting limited to her Facebook friends "would remain private[.]" *Id.*

76. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 WL 6085437, at *1 (D.N.J. July 25, 2008). The discussion thread included sexual remarks about management and customers, jokes about customer service and quality specifications and (supposedly joking) references to violence and illegal drug use. *Id.* at *2.

77. *See id.* at *1.

78. *Id.* at *2.

79. *Id.* at *4; *see also* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002). In *Konop*, an airline pilot started his own secure website "where he posted bulletins critical of his employer, its officers, and the incumbent union" and encouraged employees "to consider alternative union representation." *Id.* at 872. Access to the site required a user name and password. *Id.* Upon obtaining access to the site through an employee, an airline Vice President threatened to sue plaintiff for defamation based on the website postings. *Id.* at 873. The employer's access was unauthorized because the employee who shared his login information with the Vice President was not a "user" of the service and therefore could not authorize such access. *See id.* at 880 (holding that while the employee had been granted access, he had not actually "used" the site).

80. *See* Cheryl Conner, *Employees Really Do Waste Time at Work, Part II*, FORBES (Nov. 15,

messaging, which generally are direct personal communications, social media posts are often entirely public, but at a minimum shared simultaneously with large groups of people.[81] Employees, particularly younger employees, communicate electronically with increasing frequency; at the same time, employers have a strong interest in maintaining their business reputations and protecting confidential information.[82] As a result, many employers have been compelled to address problems that could not have been envisioned before social media and to develop parameters for their employees' social media use and even whole policies dedicated to such usage.[83]

However, just as verbal communication is protected under the National Labor Relations Act ("NLRA" or the "Act"), so is electronic communication, regardless of the audience. Any form of communication is legally protected if it is concerted (meaning that two employees act together or one employee solicits others) and the subject matter is protected (meaning that it concerns wages, hours, working conditions or terms and conditions of employment).[84] When employees gripe about how much they are paid and agree that their employer is a tightwad, they have a legally protected right to hold that conversation, whether it happens in person, on the phone, or on the internet, and even if the rest of the world is privy to the communication. Any attempt to stop that communication or to punish an employee for it would violate the NLRA.[85] Moreover, this analysis applies both to union and non-union employers alike.[86]

2012, 10:00 PM), http://www.forbes.com/sites/cherylsnappconner/2012/11/15/employees-really-do-waste-time-at-work-part-ii/.

81. *See* Melissa Venable, *The Public Nature of Social Media Participation*, ONLINECOLLEGE.ORG (Feb. 25, 2013), http://www.onlinecollege.org/2013/02/25/the-public-nature-social-media-participation/.

82. *See* Joe Sharkey, *E-Mail Saves Time, but Being There Says More*, N.Y. TIMES (Jan. 25, 2010), http://www.nytimes.com/2010/01/26/business/26road.html?; *Employee Online Social Networking: Advantages and Risks for Employers*, THORP, REED & ARMSTRONG (Sept. 10, 2010), http://www.thorpreed.com/secondary.aspx?id=44&p=0&LibraryID=208 [hereinafter *Employee Online Social Networking*].

83. *See Employee Online Social Networking*, *supra* note 82.

84. Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and *to engage in other concerted activities* for the purpose of collective bargaining or *other mutual aid or protection* . . . ." 29 U.S.C. § 157 (2006) (emphasis added). Section 8(a)(1) goes on to provide that "[i]t shall be an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in section 157 of this title." 29 U.S.C. § 158(a)(1) (2006).

85. Design Tech. Grp., LLC, No. 20-CA-35511, 2012 WL 1496201 (N.L.R.B. Apr. 27, 2012).

86. *See* NLRB v. Washington Aluminum Co., 370 U.S. 9, 9 (1962); *see also* NLRB v.

Social media policies in which employers dictate what employees can communicate electronically are subject to the same scrutiny by the National Labor Relations Board ("NLRB").[87] If they inhibit or prevent protected communications, they will run afoul of the Act.[88] Demonstrating the significance of these issues to the agency, the Acting General Counsel ("AGC") for the NLRB, issued three detailed memoranda directly on point between August 2011 and May 2012.[89]

In September 2012, the NLRB issued its first two decisions addressing employer social media policies.[90] Until then, the only decisions that had issued on the subject were by Administrative Law Judges,[91] who make recommended findings and conclusions to the NLRB, which can adopt or reject the recommendations. Both of these cases challenged facially neutral employer policies that the Board held inhibited "concerted activity" because an employee could "reasonably construe" those policies to restrict their right to talk about wages, hours and working conditions.[92]

Columbia Univ., 541 F.2d 922, 931 (2d Cir. 1976) ("there can be little doubt that the protection afforded to concerted activities under the NLRA applies equally to workers in unionized or in non-unionized firms.").

87. *See* Mark Robbins & Jennifer Mora, *The NLRB and Social Media: General Counsel's New Report Offers Employers Some Guidance,* LITTLER (Sept. 9, 2011), http://www.littler.com/publication-press/publication/nlrb-and-social-media-general-counsels-new-report-offers-employers-som.

88. *See id.*

89. *See generally* Memorandum from the Office of the Gen. Counsel Representative Div. of Operations-Mgmt., OM 11-74, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (Aug. 18, 2011); Memorandum from the Office of the Gen. Counsel Representative Div. of Operations-Mgmt., OM 12-31, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (Jan. 24, 2012); Memorandum from the Office of the Gen. Counsel Representative Div. of Operations-Mgmt., OM 12-59, REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (May 30, 2012) [hereinafter OM-1259]. While these memoranda are not Board precedent, Fun Striders, Inc., 250 N.L.R.B. No. 87, 520, 520 n.1 (July 10, 1980), the AGC decides when and under what circumstances they will issue complaints against employers and these memoranda show the parameters of what the AGC believes lawful activity to be. *See* Robbins & Mora, *supra* note 87.

90. *See generally* Costco Wholesale Corp., 358 N.L.R.B. No. 106 (Sept. 7, 2012); Karl Knauz Motors, Inc., 358 N.L.R.B. No. 164 (Sept. 28, 2012).

91. *See, e.g.*, Design Tech. Grp., LLC, *supra* note 85, at 1; Hispanics United of Buffalo, Inc., 359 N.L.R.B. No. 37, at 1 (Dec. 14, 2012).

92. *See generally* cases cited *supra* note 90. It is worth noting that President Obama's 2012 appointments and one 2011 appointment to the NLRB were recently were found to be invalid. *See* Canning v. N.L.R.B., Nos. 12-115, 12-1153, 2013 WL 276024, at *507, *513-14 (D.C. Cir. Jan. 25, 2013); N.L.R.B. v. New Vista Nursing and Rehabilitation, Nos. 12-1027, 12-1936, 2013 WL 2099742, at *30 (3d Cir. May 16, 2013). The District of Columbia's decision is being challenged to the Supreme Court but if it is upheld, all NLRB decisions issued in 2012 would be invalidated. Jeremiah L. Hart, *Noel Canning v. NLRB: The Decision, Its Potential Impact, and the Future of the National Labor Relations Board,* BAKER HOSTETLER (Feb. 4, 2013),

In *Karl Knauz Motors, Inc.*, the employer's "Courtesy" policy prohibited, *inter alia*, being "disrespectful or us[ing] profanity or any other language which injures the image or reputation" of the employer.[93] The NLRB found that this policy violated the NLRA because employees could reasonably construe its broad prohibitions as encompassing section 7 activity.[94] Similarly, in *Costco Wholesale Corp.*, the NLRB found unlawful a policy prohibiting, *inter alia*, statements "that damage the Company, defame any individual or damage any person's reputation . . . ."[95]

As explained by the Board in *Knauz,* certain types of employer policies violate Section 8 of the NLRA where the rule "reasonably tends to chill employees in the exercise of their Section 7 rights."[96] "If the rule explicitly restricts Section 7 rights, it is unlawful."[97] If it does not, it is still unlawful if "(1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; or (3) the rule has been applied to restrict the exercise of Section 7 rights."[98] The Acting General Counsel, who again, decides what cases go to a hearing, would go further and would allege as unlawful any policy that does not "clarify to employees that the rule does not restrict Section 7 rights."[99]

This means, for example, that restrictions on the disclosure of

---

http://www.bakerlaw.com/alerts/noel-canning-v-nlrb-the-decision-its-potential-impact-and-the-future-of-the-national-labor-relations-board-2-4-2013/. The Third Circuit's decision is also likely to be challenged. If it is upheld, certain NLRB decisions going back as far as August of 2011 could also be invalidated. Ronald Meisburg, *Third Circuit Holds Former MLRB Member Becker's Recess Appointment Invalid, Vacates NLRB Decision Made In August, 2011*, PROSKAUER (May 17, 2013), http://www.jdsupra.com/legalnews/third-circuit-holds-former-nlrb-member-b-70330/.

93. *Karl Knauz Motors, Inc.* 358 N.L.R.B. at 1.

94. *Id.* In addition to striking down the employer's courtesy policy, the NLRB in the *Knauz* case upheld an employee's termination based on his mocking Facebook posting (about an auto accident at the car dealership) which was "neither protected nor concerted." *Id.* at 10-11. Although the employee had also made other postings that arguably included protected activity, the NLRB determined that the termination was premised upon the unprotected postings. *See id.* at 11.

95. *Costco*, 358 N.L.R.B. at 1. A more recent NLRB decision found that an employer's termination of five employees pursuant to a "zero tolerance" policy against harassment and bullying violated the employees' section 7 rights where the employees had posted comments on Facebook addressing a coworker's criticism of their job performance. *See Hispanics United of Buffalo, Inc.*, 359 N.L.R.B. at 3.

96. *Karl Knauz Motors, Inc.*, 358 N.L.R.B. at 1 (citing Lafayette Park Hotel, 326 N.L.R.B. 824, 825 (1998)).

97. *Id.* (citing Lutheran Heritage Village.-Livonia, 343 N.L.R.B. 646, 646 (2004).

98. *Id.* (citing *Lutheran Heritage,* 343 N.L.R.B. at 647).

99. OM-1259, *supra* note 89, at 3. The AGC cautions that it is not sufficient to include a savings clause that tells employees that nothing in the policy is intended to restrict their section 7 rights. *See id.* at 9.

confidential information may be unlawful unless set forth along with "sufficient examples of prohibited disclosures . . . for employees to understand that it does not reach protected communications about working conditions."[100] This rule is premised on the fact that the NLRB "has long recognized that the term 'confidential information,' without narrowing its scope so as to exclude Section 7 activity, would reasonably be interpreted to include information concerning terms and conditions of employment."[101] It also means that general restrictions on "offensive, demeaning, abusive or inappropriate remarks" could be unlawful because they proscribe "a broad spectrum of communications that would include protected criticisms of the Employer's labor policies or treatment of employees."[102]

A rule's context is critical to determining its "reasonableness." For example, a rule prohibiting "disparaging or defamatory comments" about the employer was found to be unlawful.[103] According to the NLRB, employees would reasonably construe it to apply to protected criticism of an employer's labor policies or treatment of employees.[104] However, a rule prohibiting statements that are "slanderous or detrimental to" the employer that "appeared on a list of prohibited conduct including 'sexual or racial harassment' and 'sabotage,' would not be reasonably understood to restrict Section 7 activity."[105]

As the NLRB continues its aggressive examination of social media policies, employers are wise to scrutinize and revise their own policies.

VI. CONCLUSION

Advances in technology have provided today's workplace with increasingly powerful tools to address business needs in ways that could not have been anticipated thirty years ago. That very same technology, however, has also complicated issues of legal compliance in the workplace that similarly could not have been anticipated. As we expect technology to continue to advance with rapid speed, these areas of law will be called upon to adapt to the changing workplace.

100. *Id.* at 20.

101. *Id.* at 13 (citing Univ. Med. Ctr., 335 N.L.R.B. 1320, 1322 (2001)).

102. *Id.* at 8; *see also Costco*, 358 N.L.R.B. at 2 (finding unlawful a policy prohibiting the posting of statements "that 'damage the Company, defame any individual or damage any person's reputation' . . . .").

103. OM-1259, *supra* note 89 at 17.

104. *Id.* at 17; *see also Karl Knauz Motors, Inc.*, 358 N.L.R.B. at 1.

105. OM-1259, *supra* note 89 at 13 (citing Tradesmen Int'l, 338 N.L.R.B. 460, 462 (2002)).