Michigan Journal of Gender & Law

Volume 19 | Issue 1

2012

Limiting the Affirmative Defense in the Digital Workplace

Daniel B. Garrie

LIMITING THE AFFIRMATIVE DEFENSE IN THE DIGITAL WORKPLACE

*Daniel B. Garrie**

From 2009 to 2011, there were more than 30,000 sexual harassment claims filed in the United States.[1] The ubiquitous availability

* Daniel B. Garrie, Esq., is a partner at Law & Forensics LLC, a boutique e-discovery and forensics firm with locations in the United States and abroad. Mr. Garrie is also the head of Alternative Resolution Centers' E-Discovery Dispute Resolution Panel, where he frequently serves as a Forensic Neutral, E-Discovery Special Master, or Discovery Referee. Mr. Garrie is a co-author of *Dispute Resolution and e-Discovery*, published by Thomson Reuters. He can be reached at daniel@lawandforensics.com.

The author would like to note that an earlier version of this Article was published with the invaluable contributions of both Matthew Armstrong and Professor Donald Harris. *See* Donald P. Harris, Daniel B. Garrie & Matthew J. Armstrong, *Sexual Harassment: Limiting the Affirmative Defense in the Digital Workplace*, 39 U. MICH. J.L. REFORM 73, 83–87 (2005). The author would also like to thank Michelle Paulter for her invaluable contributions to the current version of the Article.

1. *See* U.S. Equal Employment Opportunity Commission, *Sexual Harassment Charges EEOC & FEPAs Combined: FY 1997–FY 2011*, http://www.eeoc.gov/eeoc/statistics/enforcement/sexual_harassment.cfm.

of digital technology devices has facilitated many instances of sexual harassment.[2] Such sexual harassment occurs through unprovoked and offensive e-mails, messages posted on electronic bulletin boards, and other means available on the Internet. To date, courts remain silent on this issue. Should this type of sexual harassment be treated differently from physical sexual harassment? The surprising answer is yes.

This Article suggests a new judicial framework for addressing sexual harassment perpetrated through digital communications. This framework accounts for the real-world technology in place in the digital workplace and the legal framework that courts have constructed in connection with affirmative defense to sexual harassment. The fundamental difference between digital and physical sexual harassment is the employer's ability to monitor and block offensive digital communications and thus prevent digital sexual harassment. This possibility of prevention is the underlying reason for treating the two forms of harassment differently and for modifying the existing affirmative defense.

This Article proposes that when an employer fails to use available technology to prevent known digital sexual harassment issues, the affirmative defense should be modified or unavailable. Adopting this approach would compel employers to use monitoring and blocking technology as a way to eliminate digital sexual harassment in the workplace.

INTRODUCTION

Sexual harassment law has evolved greatly over the last few decades. Employer liability has expanded to include liability for coworker harassment, supervisor harassment, and, most recently, third party harassment.[3] Correspondingly, courts have provided employers with

2. *See* Thomas J. Harvey, *Beware Workplace E-Mail, Survey Says*, ASAE & THE CENTER FOR ASSOCIATION LEADERSHIP, http://www.asaecenter.org/PublicationsResources/whitepaperdetail.cfm?ItemNumber=12168 (last visited Feb. 2, 2012) (stating that 8.3% of companies in a recent survey claimed that they had battled a sexual harassment or sex discrimination lawsuit based on employee e-mail or Internet use).

3. *See* Galdamez v. Potter, 415 F.3d 1015, 1022–25 (9th Cir. 2005) (finding that an employer may be responsible for actionable third party harassment of its employees); Turnbull v. Topeka State Hosp., 255 F.3d 1238, 1244 (10th Cir. 2001) (holding that an employer may be responsible for sexual harassment toward employees by acts of nonemployees); Crist v. Focus Homes, Inc., 122 F.3d 1107, 1111 (8th Cir. 1997) (holding that an employer may be responsible for sexual harassment toward employees by acts of nonemployees); Rosenbloom v. Senior Res., Inc., 974 F. Supp. 738, 743–44 (D. Minn. 1997) ("employer can be held liable for the racial hostile work environment created by a third party"); Powell v. Las Vegas Hilton Corp., 841 F. Supp.

specific defenses against this liability.[4] For example, an employer avoids liability by taking corrective measures reasonably calculated to permanently end the sexual harassment.[5] In many instances, the employer cannot prevent the initial sexual harassment but may ensure that it does not continue or recur.[6] This judicial treatment, however, provided little comfort to sexual harassment victims because it did not require an employer to prevent the first instance of sexual harassment.

The Supreme Court, recognizing this insufficiency of redress, held that employers should take preventive measures to ensure a workplace free from sexual harassment consistent with Title VII's[7] policy of encouraging the creation of anti–sexual harassment policies and effective grievance mechanisms.[8] Although an employer cannot observe or control all the actions of its employees in the physical workplace, the employer can more practically prevent sexual harassment in the digital workplace because cost-effective technology exists to actively monitor the content of digital communication in e-mail, internet postings, instant messaging, and other digital means.

Increasingly, sexually harassing conduct occurs through digital communication channels,[9] even though employers have access to information

---

1024, 1028 (D. Nev. 1992) (holding that an employer may be liable for sexual harassment in the workplace of employees by non-employees). *See generally* Noah D. Zatz, *Managing the Macaw: Third-Party Harassers, Accommodation, and the Disaggregation of Discriminatory Intent*, 109 COLUM. L. REV. 1357, 1372–73 (2009); Karen Kaplowitz & Donald P. Harris, *Third Party Sexual Harassment: Duties and Liabilities of Employers*, A.B.A. THE BRIEF, 32, 33–35 (Spring 1997).

4. *See* Faragher v. City of Boca Raton, 524 U.S. 775, 807 (1998); Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765 (1998).

5. *See, e.g.*, Dunn v. Wash. Cnty. Hosp., 429 F.3d 689, 691 (7th Cir. 2005) (finding that a hospital could be required to protect a nurse employee from harassment by a doctor even though the doctor was not an employee of the hospital); *Galdamez*, 415 F.3d at 1022 ("An employer may be held liable for the actionable third-party harassment of its employees where it ratifies or condones the conduct by failing to investigate and remedy it after learning of it."). *See also* Kaplowitz & Harris, *supra* note 3, at 36.

6. Kaplowitz & Harris, *supra* note 3, at 38.

7. Civil Rights Act of 1964, 42 U.S.C. §§ 2000e to 2000e-17 (2000).

8. *Ellerth*, 524 U.S. at 765; *Faragher*, 524 U.S. at 806. *See also Dunn*, 429 F.3d at 691; Miller v. Kenworth of Dothan, Inc., 277 F.3d 1269, 1278 (11th Cir. 2002).

9. *See* Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *4–9 (D. Mass. May 7, 2002) (holding that an employee terminated for sending harassing e-mails had no reasonable expectation of privacy in his work e-mail); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *9–13 (Tex. App. May 28, 1999) (holding that there is no reasonable expectation of privacy in an employer-owned e-mail system). *See also* Daniel B. Garrie & Matthew J. Armstrong, Comment, *The Sarbanes-Oxley Act's Effect on Electronic Discovery*, FED. LAW., May 2005, at 51; Mitchell Waldman, Annotation, *Expectation*

technology capable of preventing this conduct.[10] Employers monitor and block employees' digital communications to protect trade secrets,[11] track productivity,[12] and enforce corporate policies and procedures.[13] In light of these uses—and, more importantly, the legal sanction of these uses[14]—employers should be required to monitor their internal networks for offensive e-mails or communications that constitute sexual harassment. Whether an employer took reasonable precautions with respect to the size and scope of its existing domestic technological infrastructure should determine its liability. These precautions should also bear directly on the employer's ability to plead an affirmative defense to employee allegations of digital workplace sexual harassment.

This Article recommends a new framework for courts to analyze modern digital sexual harassment claims. Part I of the Article reviews the existing legal remedies for sexual harassment, the employer's affirmative defense, and the underlying rationale of the affirmative defense. Part II critiques the application of the affirmative defense to the digital workplace. Part III presents a new test, the Digital Workplace Defense Test, which courts should invoke when reviewing an affirmative defense to digital sexual harassment.

The proposed approach applies the affirmative defense in the digital workplace under more limited circumstances than in the physical workplace. Courts should examine the defendant employer's technological infrastructure and determine whether the employer and current technology offerings were capable of monitoring and blocking the digital communications comprising the sexual harassment claim. The employer should be permitted to plead the affirmative defense if the employer lacked these capabilities. If, however, the court finds that the existing technology did possess these capabilities, the court should then explore whether the defendant took reasonable steps to monitor and block the offensive digital communications, or whether the defendant's

---

of Privacy in Internet Communication, 92 A.L.R.5TH 15, § 3(c) (2001). *But see* Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010) (finding that, under some circumstances, employees do have a reasonable expectation of privacy in email accessed on a work computer).

10. *See* David N. Greenfield & Richard A. Davis, *Lost in Cyberspace: The Web @ Work*, 5 CYBERPSYCHOL. & BEHAV. 347 (2002).
11. *See* Frank C. Morris, Jr., *Workplace Privacy Issues: Avoiding Liability, in Employment Discrimination and Civil Rights Actions in Federal and State Courts* 697, 715 (ALI-ABA Course of Study, June 3–5, 1999), *available at* WL SD52 ALI-ABA 697.
12. *Id.* at 713.
13. *Id.* at 725–26.
14. *See* Roland E. Kidwell & Robert Sprague, *Electronic Surveillance in the Global Workplace: Laws, Ethics, Research and Practice*, 24 NEW TECH., WORK & EMP. 194, 198–99 (2009).

failure to use readily available technology to prevent the sexual harassment was reasonable. To resolve this inquiry, courts should determine whether and to what extent the employer used such technology to monitor and block communications for other purposes. If the court concludes that the employer did not take reasonable steps to prevent the sexual harassment, the court should not allow the defendant to plead the affirmative defense.[15] The adoption of this approach would appropriately place an obligation on employers who already possess and use blocking and monitoring technology capable of culling out offensive content to take reasonable preventive measures to prevent digital workplace sexual harassment.

I. Hostile Work Environment and Gender Discrimination

Gender discrimination claims derive from Title VII of the Civil Rights Act of 1964.[16] Congress enacted Title VII to protect employees from discrimination based on gender, race, or religion in the workplace.[17] Title VII establishes two different theories of liability for gender discrimination and sexual harassment: (1) hostile work environment; and (2) quid pro quo, or discriminatory acts having tangible employment consequences.[18]

A. Review of Legal Remedies

A hostile work environment is created when the discriminatory conduct of a supervisor, coworker, or third party alters the conditions of an individual's employment and creates an abusive working dynamic.[19] Courts first recognized the hostile work environment cause of action in race discrimination cases in the early 1980s.[20] In *Meritor Savings Bank v.*

15. *See* Rogers v. EEOC, 454 F.2d 234, 238 (5th Cir. 1971); Snyder v. Guardian Auto. Prod., Inc., 288 F. Supp. 2d 868, 872–74 (N.D. Ohio 2003) (holding in part that a harassed female employee failed to establish that she was subjected to a hostile work environment on the basis of her gender because anonymous computer messages telling her to "stop acting like you're actually working" did not reflect gender-based motive or bias). *See also* Vasquez v. Cnty. of L.A., 307 F.3d 884, 892 (9th Cir. 2002); Garcez v. Freightliner Corp., 188 Or. App. 397 (2003).
16. Civil Rights Act of 1964, 42 U.S.C. §§ 2000e to 2000e-17 (2000).
17. *Id.*
18. *Id.*
19. *See generally* Kaplowitz & Harris, *supra* note 3, at 32.
20. *See* Meritor Sav. Bank v. Vinson, 477 U.S. 57, 65–66 (1986); Rogers v. EEOC, 454 F.2d 234, 236–41 (5th Cir. 1971).

Vinson,[21] the Supreme Court extended the hostile work environment cause of action to gender discrimination, noting that sexual harassment constitutes a hostile work environment prohibited by Title VII.[22] The Court recognized that the standard for imputing liability to an employer for creating a hostile work environment differs depending on whether the alleged harasser is a coworker, supervisor, or third party.[23] When the harasser is a coworker or third party, the employer is liable only if the plaintiff can prove both that the employer knew of or should have known of the sexual harassment, and that the employer failed to take prompt and effective remedial action reasonably calculated to end the sexual harassment.[24] In essence, the employer's liability in this context is determined in accordance with a negligence standard. However, the Supreme Court declined "to issue a definitive rule on employer liability" [25] when a supervisor's harassing conduct creates a hostile work environment.[26] Instead, the Court stated that it "agree[d] with the [Equal Employment Opportunity Commission] that Congress wanted courts to look to agency principles for guidance in this area."[27]

The lack of a definitive standard for determining employer liability for sexual harassment by supervisors initiated twelve years of disagreement among the circuit courts.[28] This disagreement stemmed from the circuit courts' differing applications of agency principles. The courts held employers vicariously liable for supervisor misconduct according to three different criteria: (1) if the supervisor was "aided by" the scope of

---

21. *Meritor*, 477 U.S. at 57.
22. *See Meritor*, 477 U.S. at 73. *See also* Broderick v. Ruder, 685 F. Supp. 1269 (D.D.C. 1988) (finding supervisors' behavior created a hostile environment).
23. Faragher v. City of Boca Raton, 524 U.S. 775, 793–801 (1998); *Meritor*, 477 U.S. at 72. *See also* Kaplowitz & Harris, *supra* note 3, at 32, 34.
24. Llewellyn v. Celanese Corp., 693 F. Supp. 369, 380–81 (W.D.N.C. 1988) (citing Katz v. Dole, 709 F.2d 251, 256 (4th Cir. 1983)) (holding that the employer's response to a complaint of sexual harassment fell short of prompt remedial action reasonably calculated to end the harassment when the employer spoke to one alleged harasser and placed a warning letter in the file of another alleged harasser, but failed to inspect or discipline numerous other harassing employees); Kaplowitz & Harris, *supra* note 3, at 36.
25. *Meritor*, 477 U.S. at 72.
26. *Meritor*, 477 U.S. at 65 (articulating that a hostile work environment was actionable in sex discrimination cases because "the EEOC issued Guidelines specifying that 'sexual harassment,' as there defined, is a form of sex discrimination prohibited by Title VII.")
27. *Meritor*, 477 U.S. at 72. Regarding quid pro quo harassment, which by definition is committed by a supervisor or someone with power to effectuate tangible employment actions, employers are strictly liable for supervisor harassment. *Faragher*, 524 U.S. at 808.
28. *Faragher*, 524 U.S. at 786–87.

his or her employment; (2) if the supervisor was "aided by" the agency relationship; or (3) if the employer had actual or constructive knowledge of the sexual harassment and failed to remedy it.[29] Some courts have also held employers liable for supervisor misconduct on negligence grounds for failing to prevent sexual harassment.[30]

In order to resolve the disagreement among the circuit courts, the Supreme Court established a new method for determining employer liability in *Faragher v. City of Boca Raton*[31] and its companion case, *Burlington Industries, Inc. v. Ellerth*.[32] In these cases, the Court presented two different standards for employer liability for sexual harassment by supervisors. First, the Court held that an employer may be found liable even if supervisor sexual harassment is not accompanied by an adverse official act or "tangible employment action," such as discharge, demotion, or undesirable reassignment.[33] In these situations, however, the employer may raise an affirmative defense to such liability.[34] The affirmative defense consists of two necessary elements: "(a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities

29. *Faragher*, 524 U.S. at 793.

30. *See, e.g.*, EEOC v. Hacienda Hotel, 881 F.2d 1504, 1516 (9th Cir. 1989) (holding employer liable where hotel manager did not respond to complaints about supervisors' harassment); Hall v. Gus Constr. Co., 842 F.2d 1010, 1016 (8th Cir. 1988) (holding employer liable for harassment by coworkers because supervisor knew of the harassment but did nothing); Katz v. Dole, 709 F.2d 251, 256 (4th Cir. 1983) (upholding employer liability because the "employer's supervisory personnel manifested unmistakable acquiescence in or approval of the harassment"). *See also* Torres v. Pisano, 116 F.3d 625, 634–35, 634 n.11 (2d Cir. 1997) (citing Kotcher v. Rosa & Sullivan Appliance Ctr., Inc., 957 F.2d 61, 64 (2d Cir. 1992); Hunter v. Allis-Chalmers Corp., 797 F.2d 1417, 1422 (7th Cir. 1986)) (noting that a supervisor may hold a sufficiently high position "in the management hierarchy of the company for his actions to be imputed automatically to the employer"); Nichols v. Frank, 42 F.3d 503, 514 (9th Cir. 1994) ("Under traditional agency principles, the exercise of such actual or apparent authority gives rise to liability on the part of the employer under a theory of respondeat superior." (citation omitted)); *Kotcher*, 957 F.2d at 62 ("The supervisor is deemed to act on behalf of the employer when making decisions that affect the economic status of the employee. From the perspective of the employee, the supervisor and the employer merge into a single entity."); Shager v. Upjohn Co., 913 F.2d 398, 405 (7th Cir. 1990) ("[A] supervisory employee who fires a subordinate is doing the kind of thing that he is authorized to do, and the wrongful intent with which he does it does not carry his behavior so far beyond the orbit of his responsibilities as to excuse the employer.").

31. *Faragher*, 524 U.S. 775.

32. *Burlington Indus., Inc. v. Ellerth*, 524 U.S. 742 (1998).

33. *Faragher*, 524 U.S. at 807.

34. *Faragher*, 524 U.S. at 807.

provided by the employer or to avoid harm otherwise."[35] Second, the Court held that an employer must be found strictly liable if the supervisor's sexual harassment is accompanied by an adverse official act or "tangible employment action."[36] Under these circumstances, the employer may not raise the affirmative defense.[37] When a perceptible and hostile employment action accompanies sexual harassment, strict liability and the unavailability of the affirmative defense are appropriate for a variety of reasons: the supervisor's decision and act "merges" with the employer; the supervisor acts within the scope of his or her authority when he or she hires, fires, or demotes the employee; and the supervisor is aided by the agency relationship in discriminating against the employee.

B. The Rationale Behind the Supreme Court's Creation of the Affirmative Defense

The Supreme Court reasoned that the availability of an affirmative defense would provide an incentive for employers to take both preventive and remedial measures to limit occurrences of sexual harassment in the workplace.[38] Examples of such measures include instituting a grievance procedure, educating employees and supervisors about sexual harassment, and ensuring that employees are notified of their rights regarding sexual harassment.

By holding that employers can be vicariously liable for supervisors' conduct, the Court recognized that employers are in the best position to prevent sexual harassment, a clear goal of Title VII.[39] The Court also recognized that employers are not the only actors who can curtail sexual harassment.[40] Thus, while the first prong of the affirmative defense imposes an obligation on employers to prevent sexual harassment from occurring, the second prong imposes an obligation on employees to take actions to minimize resulting harm.

---

35. *Faragher*, 524 U.S. at 807; *Ellerth*, 524 U.S. at 765.
36. *Faragher*, 524 U.S. at 808; *Ellerth*, 524 U.S. at 765.
37. *Faragher*, 524 U.S. at 808.
38. *Faragher*, 524 U.S. at 777. *See* Petrosino v. Bell Atl., 385 F.3d 210, 226 (2d Cir. 2004); Pfeiffer v. Lewis Cnty., 308 F. Supp. 2d 88, 106 (N.D.N.Y. 2004); Sutton v. Zemex Corp., 261 F. Supp. 2d 392, 395 (W.D.N.Y. 2003); Sconce v. Tandy Corp., 9 F. Supp. 2d 773, 777 (W.D. Ky. 1998).
39. *Faragher*, 524 U.S. at 798, 806 ("[Title VII's] 'primary objective' . . . is not to provide redress but to avoid harm.") (citing Albemarle Paper Co. v. Moody, 422 U.S. 405, 417 (1975)). *See also* Baldwin v. Blue Cross/Blue Shield 480 F.3d 1287, 1305 (11th Cir. 2007); Swenson v. Potter 271 F.3d 1184, 1197 (9th Cir. 2001); Hathaway v. Runyon, 132 F.3d 1214, 1224 (8th Cir. 1997).
40. *Faragher*, 524 U.S. at 806–07.

While the Supreme Court did not explicitly direct employers to adopt internal anti–sexual harassment policies and procedures, the Supreme Court provided an incentive to do so by granting employers possible immunity if they implement policies and procedures.[41] In explaining why employer liability for supervisor misconduct might be appropriate, the Court justified the different treatment between supervisors, on the one hand, and coworkers and third parties, on the other, because a supervisor "[n]ecessarily draw[s] upon his superior position" in harassing the victim and because the employer has a greater opportunity to guard against supervisor misconduct.[42] The Court refused to impute "automatic liability" for supervisor sexual harassment because liability might be inappropriate under certain conditions, such as when the employer exercised due care to avoid sexual harassment and to eliminate it when it occurred.[43]

C. The Affirmative Defense Today

In 2004, in *Pennsylvania State Police v. Suders*, the Supreme Court reaffirmed the affirmative defense in the context of a constructive discharge claim.[44] In *Suders*, a female police dispatcher for the Pennsylvania State Police filed a claim against her employer alleging both sexual harassment and gender discrimination.[45] She claimed constructive discharge by alleging that relentless sexual harassment by her supervisors left her

41. *See, e.g.*, Hairston-Lash v. R.J.E. Telecom, Inc., 161 F. Supp. 2d 390, 394 (E.D. Pa. 2001) (granting summary judgment for the defendant employer, stating that plaintiff did not contest that she had received notice of employer's extensive policies and procedures on handling sexual harassment); Slay v. Glickman, 137 F. Supp. 2d 743, 752 (S.D. Miss. 2001) (granting employer's motion for summary judgment, concluding, because the employer had a sexual harassment policy of which the plaintiff was aware and promptly investigated plaintiff's allegations of harassment, plaintiff did not establish a genuine issue of material fact with regard to whether the defendant employer exercised reasonable care to prevent and promptly correct sexual harassment in the workplace). *See also* Donald P. Harris, Daniel B. Garrie, Matthew J. Armstrong, *Sexual Harassment: Limiting the Affirmative Defense in the Digital Workplace*, 39 U. MICH. J.L. REFORM 73 (2005).

42. *Faragher*, 524 U.S. at 803. *See also* Joens v. John Morrell & Co., 354 F.3d 938, 940 (8th Cir. 2004); Gordon v. Shafer Contracting Co., 469 F.3d 1191, 1194–95 (8th Cir. 2006); Al-Zubaidy v. TEK Indus., Inc., 406 F.3d 1030, 1038 (8th Cir. 2005).

43. *Faragher*, 524 U.S. at 805.

44. Pennsylvania State Police v. Suders, 542 U.S. 129, 131 (2004). *See also* Ford Motor Co. v. EEOC, 458 U.S. 219, 231 (1982) (discussing a Title VII plaintiff's responsibility to mitigate damages).

45. *Suders*, 542 U.S. at 133.

no option but to resign her position.[46] Reversing the trial court's decision, the Third Circuit held that her constructive discharge constituted an adverse employment action.[47] Therefore, under *Faragher* and *Ellerth*, her employer was strictly liable and not permitted to plead the affirmative defense.[48]

The Supreme Court reversed, holding that although some constructive discharges amounted to official employer action, others do not result from a supervisor's official act.[49] Accordingly, the Court concluded that an employer is prohibited from relying on the "affirmative defense [only] when a supervisor's official act precipitates the constructive discharge . . . ."[50] Although *Suders* reinforces the role of the affirmative defense in the physical workplace, *Suders* does not address whether the affirmative defense should be permitted in the digital workplace.[51]

II. Critique of the Affirmative Defense in the Digital Workplace

Digital workplace sexual harassment occurs when employees use e-mail or the Internet to sexually harass other employees or to create a hostile work environment.[52] Few cases have addressed employer liability for these acts. In *Owens v. Morgan Stanley & Co.*, the district court held that while unchecked offensive e-mail communications circulating within the workplace could constitute sexual harassment, a single incident of inappropriate e-mail was insufficient to establish a claim.[53] In *Strauss v. Microsoft Corp.*, the district court held that jokes and sexual parodies, in

46. *Suders*, 542 U.S. at 133.
47. *Suders*, 542 U.S. at 138.
48. *Suders*, 542 U.S. at 139.
49. *Suders*, 542 U.S. at 131.
50. *Suders*, 542 U.S. at 140–41.
51. *Suders*, 542 U.S. at 148. *See also* Mac's Shell Serv., Inc. v. Shell Oil Prod. Co., 130 S. Ct. 1251, 1258 (2010); Fincher v. Depository Trust & Clearing Corp., 604 F.3d 712, 725 (2d Cir. 2010).
52. *See* Gorzynski v. JetBlue Airways Corp., 596 F.3d 93, 102 (2nd Cir. 2010); Strickland v. United Parcel Serv., Inc., 555 F.3d 1224, 1233 (10th Cir. 2010); Helton v. Southland Racing Corp., 600 F.3d 954, 959 (8th Cir. 2010); Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 551–52 (N.J. 2000); Jay M. Zitter, Annotation, *Liability of Internet Service Provider for Internet or E-mail Defamation*, 84 A.L.R. 5th 169, § 4(b) (2000).
53. Owens v. Morgan Stanley & Co., No. 96 CIV. 9747, 1997 WL 403454, at *2 (S.D.N.Y. July 17, 1997). *See also* Martin v. MTA Bridges & Tunnels, 610 F. Supp. 2d 238, 243 (S.D.N.Y. 2009); Lueck v. Progressive Ins., Inc., No. 09-CV-6174, 2009 WL 342979, at *1 (W.D.N.Y. Oct. 19, 2009).

combination with other remarks e-mailed by a supervisor to employees, were admissible and relevant evidence of sexual harassment.[54]

The New Jersey Supreme Court, in *Blakey v. Continental, Inc.*, held that a female employee had a valid sexual harassment claim when allegedly defamatory and sexually harassing material was posted on an electronic bulletin board.[55] Although the employer, Continental, did not maintain the bulletin board and employees could only access it through the Internet, the court found that Continental had notice of the sexual harassment and that the electronic bulletin board was integrated into the workplace to such a degree that Continental had a duty to correct off-site sexual harassment by coworkers.[56] *Blakey* stressed that an employer's responsibility to prevent sexual harassment and hostile work environments extends to both the physical and digital workplace.[57] Under *Blakey*, once an employer has knowledge of employee-to-employee digital sexual harassment, the employer must take affirmative steps to halt the sexual harassment.[58]

The *Blakey* court, however, did not place an affirmative obligation on employers to prevent sexual harassment by monitoring digital communications.[59] The court stated that although "employers do not have a duty to monitor private communications of their employees," they "do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know" of the

54. Strauss v. Microsoft Corp., 91 CIV. 5928, 1995 WL 326492, at *4–5 (S.D.N.Y. June 1, 1995).

55. *Blakey*, 751 A.2d at 543. In *Blakey*, a female pilot claimed that she suffered from a hostile work environment by being the subject of a series of harassing and defamatory messages posted on an internet bulletin board accessible to all Continental pilots and crew members. *Id.* at 544. *See also* Young v. New Haven Advocate, 315 F.3d 256, 259 (4th Cir. 2002); Bible & Gospel Trust v. Wyman, 354 F. Supp. 2d 1025, 1030 (D. Minn. 2005); Burleson v. Toback, 391 F. Supp. 2d 401, 417 (M.D.N.C. 2005); Medinah Mining, Inc. v. Amunategui, 237 F. Supp. 2d 1132, 1136 (D. Nev. 2002); Barrett v. Catacombs Press, 44 F. Supp. 2d 717, 729 (E.D. Pa. 1999); Novak v. Benn, 896 So. 2d 513, 521 (Ala. Civ. App. 2004); Griffis v. Luban, 646 N.W.2d 527, 530 (Minn. 2002); Goldhaber v. Kohlenberg, 928 A.2d 948, 950 (N.J. Super. Ct. App. Div. 2007); Doe v. XYZ Corp., 887 A.2d 1156, 1162 (N.J. Super. Ct. App. Div. 2005) (repeating that companies have no duty to investigate the private communications of their employees); Lafranco v. Avaya, Inc., Docket No. A-1666-06T2, 2009 WL 2850747, at *29 (N.J. Super. Ct. App. Div. Sep. 8, 2009).

56. *Blakey*, 751 A.2d at 543, 551–52, 558.

57. *Blakey*, 751 A.2d at 551.

58. *Blakey*, 751 A.2d at 551–52.

59. AMA/ePolicy Inst. Research, *2007 Electronic Monitoring & Surveillance Survey* 2 (2008), http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (stating that 71 percent of employers monitoring employee e-mail notify such employees prior to any monitoring; 11 percent of employers do not notify employees; another 18 percent did not know whether e-mail monitoring took place).

sexual harassment.[60] The court limited the scope of its holding due to "grave privacy concerns."[61] Recent decisions and legislative enactments have reduced these concerns and suggest extending the reach of the decision.

A. Monitoring Technology in the Workplace

Courts have recognized employers' rights to monitor employees' e-mail messages and to use digital technologies to protect trade secrets.[62] Moreover, courts have consistently found that employees do not have an objectively reasonable expectation of privacy when their employer's e-mail policies notify employees that the employer may monitor their e-mail or internet use.[63] Employers have a right to invade employees' digital work-

60. *Blakey*, 751 A.2d at 552; *see also* Herman v. Coastal Corp., 791 A.2d 238, 251–52 (N.J. Super. Ct. App. Div. 2002) (finding no employer liability absent showing that harassing employee operated within scope of employment and that employer acted negligently or intentionally and/or failed to take effective remedial measures).

61. *Blakey*, 751 A.2d at 551. *See also* Tacket v. Gen. Motors Corp., 836 F.2d 1042, 1046 (7th Cir. 1987; Doe v. XYC Corp., 887 A.2d 1156 (N.J. App. Div 2005)).

62. *Blakey*, 751 A.2d at 551. *See also* Eric P. Robinson, *Big Brother or Modern Management: E-mail Monitoring in the Private Workplace*, 17 LAB. LAW. 311, 325–26 (2001). *Contra* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010) (finding that employees do have a reasonable expectation of privacy in email accessed on a work computer).

63. *See, e.g.*, United States v. Greiner, 235 Fed. Appx. 541, 542 (9th Cir. 2007) (holding that an employee had no legitimate expectation of privacy because he consented to employer monitoring when he was confronted by a warning banner each time he logged onto his computer); *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (stating that "privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user"). *See also* Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2000); Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 409 (2d Cir. 2004); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004); Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 884 (Cal. Ct. App. 2011); Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, 444 (N.Y. Sup. Ct. 2007); *Loving Care*, 990 A.2d at 687–88 (holding that "Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care's laptop. Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer. In other words, she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit. In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based email accounts accessed through company equipment. It does not address personal accounts at all. Nor

spaces because employers have legitimate interests in communications transmitted on their digital networks for a multitude of reasons:[64] to ensure work productivity,[65] to prevent trade secret disclosure,[66] to ensure compliance with federal regulations,[67] to prevent transmission of defamatory statements,[68] and to prevent transmission of unauthorized or illegal material over employers' digital communication networks,[69] among other reasons.[70]

---

does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in acknowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property. Moreover, the e-mails are not illegal or inappropriate material stored on Loving Care's equipment, which might harm the company in some way."); William A. Herbert, Symposium, *The Electronic Workplace: To Live Outside the Law you Must be Honest*, 12 EMPL. RTS. & EMPLOY. POL'Y J. 49, 60–61 (2008) (stating that "automatic screen warnings, upon logging in, can help to ensure that an employee's subjective expectation of privacy will be found unreasonable by a court."). *See generally*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010); Quon v. Arch Wireless Operating Co., 529 F. 3d 892 (9th Cir. 2008); Justin Conforti, *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the* Ortega *Test in* Quon v. Arch Wireless, 5 SETON HALL CIR. REV. 461, 472–91 (2009); Paul F. Gerhart, *Employee Privacy Rights in the United States*, 17 COMP. LAB. L.J. 175, 176–205 (Fall 1995); James P. Nehf, *Incomparability and the Passive Virtues of Ad Hoc Privacy Policy*, 76 U. COLO. L. REV. 1, 4–18 (2005); Rachel Sweeney Green, *COMMENTS: Privacy in the Government Workplace: Employees' Fourth Amendment and Statutory Rights to Privacy*, 35 CUMB. L. REV. 639 (2004–2005).

64. *See* United States v. Zeigler, 456 F.3d 1138, 1143 (9th Cir. 2006); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (holding that the abuse of access using workplace computers is so common that "reserving a right of inspection is 'so far from being unreasonable that the failure to do so might well be thought irresponsible"); United States v. Silva, 247 F.3d 1051, 1055 (9th Cir. 2001) (noting that "[t]he reasonableness of an expectation of privacy is evaluated . . . [by reference] 'to understandings that are recognized and permitted by society'" [quoting Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978)]). *See also* Daniel B. Garrie & Rebecca Wong, *Demystifying Clickstream Data: A European and U.S. Perspective*, 20 EMORY INT'L L. REV. 563, 570 (2006).

65. Morris, *supra* note 11, at 702.

66. *Id.*

67. ORACLE FINANCIAL SERVICES, ORACLE FINANCIAL SERVICES TRADING COMPLIANCE 1 (2011), http://www.oracle.com/us/industries/financial-services/046172.pdf. Benjamin Wright, *E-Message Retention Under US Securities Law*, MESSAGINGARCHITECTS.COM, http://www.messagingarchitects.com/documents/pdf/Resources/eDiscovery%20Centre%20Free%20Resources/SEC_Compliance_brief.pdf.

68. *See* Kirstie Ball, *Workplace Surveillance: An Overview*, 51 LAB. HIST. 87, 92 (2010).

69. *See* Amy Rogers, *You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5 J. TECH. L. & POL'Y 1, 9–30 (2000).

70. *See* Marc A. Sherman, *Webmail at Work: The Case for Protection Against Employer Monitoring*, 23 TOURO L. REV. 647, 651 (2007–2008) (stating that a "short list of other risks [of not monitoring employee e-mail] includes compromise of sensitive or

The vast majority of large employers use digital tracking technology to monitor employees.[71] According to a recent *Washington Internet Daily* release, 80 percent of major United States companies occasionally record and review employees' electronic communications or browser use.[72] 67 percent of employers have disciplined at least one employee for improper or excessive use of e-mail or internet access, and 31 percent have fired employees for such conduct.[73] It is estimated that more than three-quarters of major U.S. corporations record and review employee communications and activities on the job, including telephone calls, e-mail, internet communications, and computer files.[74] E-mail monitoring by employers is both a necessity and a legally recognized right.[75] Courts granted employers this right so employers can prevent personal use or abuse of company resources, investigate corporate espionage and theft, resolve technical problems, and better cooperate with law enforcement officials in investigations.[76]

Many companies also use software that monitors or blocks their employees' use of the corporate technology infrastructure.[77] SilentRun-

---

proprietary information, damage to public image, and vicarious liability for various torts").

71. *Employers Fighting Net Abuse Must Mind Privacy*, WASH. INTERNET DAILY, Apr. 24, 2002, at 1.

72. *Id.* Numerous providers offer a myriad array of employee monitoring software; the following is an incomplete list: StaffCop, by AtomPark Software Inc.; OfficeShield, by Computer Business Solutions, Inc.; Spector 360, by SpectorSoft Corp.; and GuardBay, by Interlative LLC. These solutions generally include keylogging, capture of instant messages, email, and social networking usage, file transfer recording, screenshot capture, and program usage, for example.

73. *Id.*

74. AMA, *Electronic Policies and Practices: Summary of Key Findings*, US NEWS (2001), http://www.amanet.org/research/pdfs/ems_short2001.pdf.

75. *See generally* Jennifer J. Griffin, *The Monitoring of Electronic Mail in the Private Sector Workplace: An Electronic Assault on Employee Privacy Rights*, 4 SOFTWARE L.J. 493, 502 (1991).

76. *See* United States v. Steiger, 318 F.3d 1039, 1046 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 563 (S.D.N.Y. 2008); Greenfield & Davis, *supra* note 10, at 348.

77. *See generally* Ed Orum, *10 Ways Your Employer is Spying on You*,(Dec. 27, 2009) http://jobs.aol.com/articles/2009/12/27/10-ways-your-employer-is-spying-on-you/; Stephanie Armour, *Employers Look Closely at What Workers do on Job*, USA TODAY, (Nov. 7, 2006), http://www.usatoday.com/money/industries/technology/2006- 11-07-spy-cover-usat_x.htm; Richard Hull et al., *Enabling Context-Aware and Privacy-Conscious User Data Sharing*, IEEE INT'L CONF. ON MOBILE DATA MGMT., Jan. 19–22, 2004, at 187; R. H. Irving et al., *Computerized Performance Monitoring Systems: Use and Abuse*, 29 COMM. ACM 794, 798 (1986); Pete Lindstrom, *Diverse Security Technologies Deliver the Same Message: "Keep Out!"*, INFO. SECURITY, Oct. 2002, *available at* http:// www.infosecuritymag.com/2002/oct/

ner is illustrative of such software.[78] Although most lawyers and employees have never heard of SilentRunner,[79] companies and governmental agencies use the program to monitor their agents and employees.[80] According to Susan Lee, a representative for the internet security assurance service provider TruSecure, SilentRunner provides constant employee monitoring for nearly four hundred companies.[81] Organizations such as Deloitte & Touche that use SilentRunner and similar software,[82] have adopted top-secret policies[83] regarding their use of the product.[84] Such an approach enables companies to avoid public scrutiny from groups

---

sidebar.shtml; M. Tamuz, *The Impact of Computer Surveillance on Air Safety Reporting*, 22 COLUM. J. WORLD BUS. 69, 75 (1987).

78. SilentRunner, now called *SilentRunner Sentinel* and sold by the AccessData Corporation, is capable of recognizing approximately 2000 different protocols. Jay Lyman, *SilentRunner Spyware Out-Snoops FBI's Carnivore*, NEWSFACTOR, Mar. 2, 2001, *available at* http://www.newsfactor.com/story.xhtml? story_id=7873. It can collect any traffic on the network at a rate of 195,000 plus packets per second. Jeffrey Benner, *Nailing the Company Spies*, WIRED NEWS, Mar. 1, 2001, *available at* http://www.wired.com/news/business/0,1367,41968,00.html (quoting Dave Capuano, Vice President of Product Management for TruSecure); *see also* J. Rule & P. Brantly, *Surveillance in the Workplace: A New Meaning to 'Personal' Computing*, PROC. INT'L CONF. ON SHAPING ORG., SHAPING TECH., 1991, at 183.

79. *See* Jeffrey Benner, *Privacy at Work? Be Serious*, WIRED NEWS, Mar. 1, 2001, *available at* http://www.wired.com/news/business/0,1367,42029,00.html; *see also* Benner, *supra* note 78 ("In 1999, Raytheon took action against some of its own employees it suspected of compromising company information. Some of them learned the hard way that talking about one's employer 'privately,' and even anonymously, can be risky. In February of that year, Raytheon sued 21 'John Does' for $25,000 in damages due to criticisms of the company made on Internet message boards. Raytheon said it suspected current and former employees of being responsible for the anonymous postings, accusing them of revealing confidential information. The company successfully subpoenaed Yahoo to find out who made the comments, then abruptly dropped the suit. At least four of the 21, including one VP, resigned after being identified.").

80. Benner, *supra* note 79; *see also* Kristie Lu Stout, *China Police Unleash Net Filterware*, CNN, Mar. 1, 2001, *available at* http://archives.cnn.com/2001/WORLD/asiapcf/east/02/28/hk.policefilter/index.html.

81. Benner, *supra* note 79.

82. *Id.* ("'SilentRunner is completely undetectable to end users, and it captures everything,' said Kris Haworth, manager of the Deloitte & Touche computer forensics lab in San Francisco."). *See generally* Detmar W. Straub, Jr. & William D. Nance, *Discovering and Disciplining Computer Abuse in Organizations: A Field Study*, 14 MIS Q. 45, 47 (1990).

83. *See* Andrew Gumbel, *Techno Detectives Net Cyber-Stalkers*, INDEP., Jan. 31, 1999, at 17.

84. Benner, *supra* note 79 ("Until December 2000, when security services provider TruSecure revealed it had purchased the 'lite' version of the program, not one organization, public or private, had admitted to buying SilentRunner. On Feb. 1, the computer forensic division of consulting firm Deloitte & Touche became the second to say it uses the program.").

concerned about the erosion of privacy in the workplace.[85] Although the effort to maintain secrecy about the configuration of monitoring software may seem to indicate that such monitoring is dishonest or immoral, whether it is unethical depends on the reasonable expectations of employees. When employers' policies indicate clearly that monitoring takes place, employees have little or no expectation of privacy.[86] When employees are not notified of these policies, the question of reasonable expectations is debatable.[87]

In addition to monitoring and blocking capabilities, employers often possess a high degree of control over employee computer desktops by ensuring that a uniform technical environment exists to maximize productivity.[88] For example, ActivatorDesk's Enterprise Desktops Controller monitors employee computing activities and compares them to a list of approved activities.[89] If an employee performs previously unapproved activities, "ActivatorDesk can instantly implement a 'lock-down policy'" while sending network administrators an e-mail alert of the violation.[90] Today, monitoring tools are common and available. For example, parents can utilize the stealth and anti-detection capabilities of "Spector Pro 2011" to monitor their children's activity on: the latest chat programs, such as Google Talk, Skype Chat/IM, and the latest versions of AIM, MSN, and Yahoo; webmail from Google Gmail, Microsoft Hotmail, Yahoo Mail, and AOL Mail; and Facebook and

85. *See generally* Mary J. Culnan, *Protecting Privacy Online: Is Self-Regulation Working?*, 19 J. PUB. POL'Y & MARKETING 20, 20–26 (2000). While the authors strongly believe that privacy concerns should trump employer concerns, the point of this section is to demonstrate that courts have permitted employers to use such monitoring and tracking devices despite employee privacy concerns. Whether this is appropriate is not the subject of this Article.

86. *See* Kidwell & Sprague, *supra* note 14, at 198–99.

87. *Id.*

88. *Id.* at 196.

89. Michelle Delio, *New Tools a Spying Boss Will Love*, WIRED NEWS, Nov. 13, 2002, *available at* http://www.wired.com/news /privacy/0,1848,56324,00.html.

90. *Id. See also* Wallace Immen, *Workplace Privacy Gets Day in Court*, GLOBE & MAIL, Apr. 28, 2004, at C1. On a different note, however, regarding the dangers of remote webcam access see Robbins v. Lower Merion Sch. Dist., No. 10-CV-0665, 2010 WL 1976869 (E.D. Pa. May 14, 2010). In *Robbins*, school administrators installed webcam-monitoring software on laptops issued to students. They then used the software to spy on students at home, including keylogging, webcam access, and site access logging.

MySpace.[91] Enhanced versions of these monitoring applications are readily available for corporate networks.[92]

The majority of large corporate employers in the United States currently use monitoring and blocking software that allows them to observe and block inappropriate digital communications over corporate information technology networks before the intended recipient receives them.[93] Employers exercise this power without also being required to protect their employees. As a result, employees are relinquishing privacy rights without receiving the benefit of the employer's protection in return. Due to the diminished expectation of privacy in the workplace, employees are entitled to bring suit only when an intrusion infringes upon intensely private matters or when their employers have failed to inform them of the monitoring.[94]

The Second Circuit illustrated the diminished expectation of privacy in the workplace in *Leventhal v. Knapek*, holding that an employee does not have a reasonable expectation of privacy with respect to his or her digital activities in the workplace.[95] In support of the same principle,

91. Costs are less than $100 per computer. See SpectorSoft, *Products*, http://www.spectorsoft.com/products/SpectorPro_Windows/index.asp?refer=12081 (last visited Sept. 25, 2011).

92. Delio, *supra* note 89.

93. *See* Robinson, *supra* note 62, at 325

94. "No comprehensive statutory scheme supplements the common law to provide protection for employees' privacy or even simply from employer monitoring. Instead, a variety of federal and state laws offer only targeted and limited protections . . . ." Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J. L. & PUB. POL'Y 609, 620–21, (2009). "Moreover, because the Fourth Amendment only applies when the government acts, private sector employees have [basically] no statutory federal protection. While the Electronic Communications Privacy Act of 1986 protects against various kinds of electronic surveillance and interception of communications by public and private actors . . . this regime presents several potentially insurmountable hurdles for any employee who alleges his employer intercepted private communications on workplace technology." Conforti, *supra* note 63, at 465. For case law, see Med. Lab. Mgmt. v. ABC, Inc., 30 F. Supp. 2d 1182, 1188 (D. Ariz. 1998); Doe v. Kohn Nast & Graf, P.C., 862 F. Supp. 1310, 1326 (E.D. Pa. 1994) (finding employer may have intruded on an employee's privacy by reading personal medical documents on employee's desk). *See also* Craig v. M & O Agencies, Inc., 496 F. 3d 1047 (9th Cir. 2007); Mindy C. Calisti, *You Are Being Watched: The Need for Notice in Employer Electronic Monitoring*, 96 KY. L.J. 649 (2007–08); Conforti, *supra* note 63, at 464 (reiterating that if "employers monitor communications on workplace technology and employees inadvertently divulge personal information, employees will often struggle to find any legal protection, as the American legal regime does not provide any generally applicable, affirmative protection for employee privacy.").

95. Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001). *But see* US v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007) ("However, privacy expectations may be reduced if the user is advised that information transmitted through the network is not

Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA)[96] and the Stored Communications Act (SCA),[97] both of which grant employers the right to monitor employees' e-mail communications as long as the monitoring occurs in the ordinary course of business.[98] The majority of case law interpreting the ECPA has found that employers can monitor employees' e-mail messages with or without consent, and even without notice.[99]

---

confidential and that the systems administrators may monitor communications transmitted by the user."); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Matikas v. Univ. of Dayton, 788 N.E.2d 1108, 1115 (Ohio App. 2003) (holding an employer accessing employee's private information on employer's computer is actionable).

96. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.). The ECPA, enacted nearly a decade before the creation of the World Wide Web, did not anticipate the contemporary monitoring technology which primarily involves the Web, *see* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) (stating that "the difficulty [in deciding how the ECPA must apply to contemporary technology] is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [this] secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results."). *See also* United States v. Ropp, 347 F. Supp. 2d 831, 833 (C.D. Cal. 2004) (quoting United States v. Councilman, 373 F.3d 197, 200 (1st Cir. 2004) ("[T]he language of the [Wiretap Act] makes clear that Congress meant to give lesser protection to electronic communications than wire and oral communications. Moreover, at this juncture, much of the protection may have been eviscerated by the realities of modern technology. [In fact] . . . the language may be out of step with the technological realities of computer crimes.")).

97. Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. § 2701 (2000)).

98. *See* Daniel B. Garrie, *The Legal Status of Software*, 23 J. MARSHALL J. COMPUTER & INFO. L. 711, 732–35 (2005); Daniel B. Garrie, Matthew J. Armstrong & Donald P. Harris, *Voice Over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?*, 29 SEATTLE U. L. REV. 97, 108–11 (2005).

99. *See, e.g.*, Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins., 352 F.3d 107, 115 (3d Cir. 2003); United States v. Angevine, 281 F.3d 1130, 1134–35 (10th Cir. 2002) (holding that the professor, who had entered a conditional plea for downloading child pornography to his workplace computer, had no expectation of privacy in his use of his public employer's computer, especially since the university's usage and monitoring policy was displayed upon login); KLA-Tencor Corp. v. Murphy, 717 F. Supp. 2d 895, 903 (N.D. Cal 2010); United States v. Weaver, 636 F. Supp. 2d 769, 770 (C.D. Ill. 2009); *In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 512 (S.D.N.Y. 2001); United States v. Bunnell, No. CRIM.02-13-B-S, 2002 WL 981457, at *2 (D. Me. May 10, 2002) ("A [public university] student has no generic expectation of privacy for shared usage on the university's computers.").

These judicial and congressional actions have expanded employers' ability to monitor employee's electronic communications without violating federal privacy laws.[100] Because employers have access and control over employee's electronic communications, employers are now in a position to minimize digital sexual harassment in the workplace.[101] For example, employers can block e-mails containing sexually explicit terms and restrict wallpaper settings on corporate computers so users cannot display inappropriate or offensive material; they might also monitor employee use of social networking sites; and they could review phone calls, text messages, and data use on a company-issued mobile phone.[102] The ability and the right to monitor all employee digital transmissions places employers in an ideal position to take simple, proactive measures to prevent most instances of digital sexual harassment.

The rights and abilities of employers to read digital communications sent and received by employees should compel courts to extend the holdings of *Ellerth* and *Faragher*, as well as the *Blakey* line of cases. Because employers who use blocking and monitoring technology have notice of potential digital sexual harassment before it reaches the intended recipient, employers should bear the burden to provide reasonably sufficient technical protection that limits exposure to such sexual harassment.[103]

---

100. *See supra* notes 95–99 and accompanying text.

101. *See supra* notes 72–76.

102. The author believes that there is a difference between what can be called "internet monitoring" and what can be called "social network monitoring." Social network monitoring—when done at work—falls clearly under internet monitoring. The use of a social network by an employee on a work computer involves access to the site via the internet and is part of internet monitoring. Instead, the author views "social network monitoring" as browsing through an employee's Facebook page or Twitter stream, etc. or conducting a search of an employee's name to discover information. *See further* John Browning, *Employers Face Pros, Cons With Monitoring Social Networking*, HOUSTON BUS. J., (Feb. 27, 2009), http://www.bizjournals.com/houston/stories/2009/03/02/smallb3.html ("On Oct. 31, 2007, Kevin Colvin told his employers at Boston's Anglo Irish Bank that he had to miss a day of work due to an emergency at home in New York. The next day, Colvin's manager happened to check the employee's Facebook profile, where Colvin had thoughtfully posted a photograph from a Halloween party he had attended the previous night, featuring him in a sparkly green fairy costume, complete with wand and a can of beer. Colvin's manager replied to an e-mail from his soon-to-be ex-employee, attaching the photo of Colvin in drag—and blind copying the entire office—and stating 'Thanks for letting us know—hope everything is okay in New York (cool wand).' Colvin was fired for lying.")

103. *See generally* United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); United States v. Butler, 151 F. Supp. 2d 82, 84 (D. Me. 2001) (finding student had no objective expectation of privacy in using university computers even absent evidence of a university policy giving notice of right

Unfortunately, courts have not bridged the gap between employers' freedom to monitor employee acts and employers' responsibility to prevent employee acts capable of causing harm. More precisely, many courts have yet to address whether an employer should be entitled to plead an affirmative defense to digital sexual harassment claims when the employer has failed to monitor the digital work environment, prevent digital sexual harassment, or institute mechanisms to facilitate employee complaints of digital sexual harassment.[104]

B. The Current Affirmative Defense Framework Undermines both Congressional and Judicial Policies

Although the Supreme Court in *Ellerth*[105] and *Faragher*[106] sought to compel employers to take a preventive approach to eliminate sexual harassment in the workplace, an employer pleading the affirmative defense may be able to avoid accountability for hostile digital work environments. The failure to require preemptive policies in the digital sphere is particularly inappropriate when employers have effective notice of sexually harassing communications.[107] The inappropriateness of this position also violates the Supreme Court's intent to compel employers to take a proactive role in preventing workplace sexual harassment. Moreover, the docket of both state and federal courts is likely to grow until the

---

or intent to monitor use). *Contra* Robbins v. Lower Merion Sch. Dist., No. 10-CV-0665 (E.D. Pa. May 14, 2010) (discussed *supra* note 90).

104. *See supra* notes 53–57. *See also* Doe v. XYC Corp., 887 A.2d 1156, 1169–70 (N.J. Super. Ct. App. Div. 2005) (holding that an employer might avoid vicarious liability when one of its employees transmits child pornography at work and the employer had policies against such activities). In *Doe*, the employer knew of the illegal activities and did little to nothing to shut them down or discipline the employee. *Id.* at 1158. The appellate court remanded the case for a jury trial but likely would have dismissed the employer from the case had management enforced its Internet policy. *See id.*

105. Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765 (1998).

106. Faragher v. City of Boca Raton, 524 U.S. 775, 807 (1998).

107. The EEOC declared that twelve Minneapolis librarians were subjected to a sexually hostile work environment when they were exposed to pornography accessed on the Internet by library patrons. *See, e.g.*, *EEOC Rules in Minneapolis PL Complaint*, AM. LIBR. ONLINE (May 28, 2001), http://www.ala.org/ala/alonline/currentnews/newsarchive/2001/may2001 (follow "EEOC Rules in Minneapolis PL Complaint" hyperlink). If courts agree with the EEOC, all libraries, public and private, will need to ban Internet access to "offensive" sites or face hostile environment liability. *See, e.g.*, *Five More Minneapolis Librarians File Discrimination Charges*, AM. LIBR. ONLINE (May 29, 2000), http://www.ala.org/ala/alonline/currentnews/newsarchive/2000/may2000/fivemoreminneapolis.htm.

issues arising from digital sexual harassment are addressed.[108] Courts should therefore apply the *Faragher* and *Ellerth* affirmative defense to protect employees in the digital workplace by creating an efficient and effective legal framework to address digital sexual harassment claims. While a judicial approach to the problem would not preclude legislative action, the Supreme Court's willingness to address sexual harassment in cases such as *Meritor* and *Ellerth* indicates the courtroom as the natural locus for the framework's development.

The existing affirmative defense focuses on the employer's remedial measures and the employee's availment of these corrective opportunities. This assessment approach, although perhaps effective in the physical workplace, does not account for the technology available in the digital workplace today. Employers in the digital workplace have the ability to "know everything" and can control digital communications to stop sexual harassment before it occurs. The increased monitoring capabilities of employers in the digital workplace call for a modification of the affirmative defense in cases of digital sexual harassment.[109]

C. The Affirmative Defense in the Digital Workplace

Employers should be required to institute more than remedial policies in order to plead the affirmative defense if they already use a wide

108. Digital sexual harassment is not limited to the workplace and numerous organizations are taking steps to combat its presence in all areas of life. *See MTV Launches 'A Thin Line' To Stop Digital Abuse*, MTV (Dec. 3, 2009), http://www.mtv.com/news/articles/1627487/20091203/story.jhtml. For this initiative, MTV partnered with Facebook, MySpace, the Family Violence Prevention Fund, WiredSafety, the Anti-Defamation League, Blue Shield of California Foundation, LoveIsRespect.org, the National Teen Dating Abuse Helpline, the National Network to End Domestic Violence, Liz Claiborne Inc., DoSomething.org, Break the Cycle, Ruder Finn, Teenangels, and PBS's "Frontline." *See About A Thin Line*, A THIN LINE, http://www.athinline.org/about (last visited Feb. 2, 2012).

109. While the affirmative defense is available to employers in the context of vicarious liability for supervisor misconduct in hostile work environment sexual harassment claims (or claims in which no tangible employment action results), the presence of employer monitoring and blocking technology is also relevant in cases of coworker and third party sexual harassment. First, an employer can guard against harassing conduct by subordinate or common employees using digital technology just as easily as it can against such conduct by supervisors. It would thus appear inappropriate to uphold the two-tiered liability for these classes. Second, as noted above, in the context of coworker or third party sexual harassment, the employer is liable if it knew or should have known of the sexual harassment and failed to take effective remedial action. Arguably, armed with the technological capability to do so, an employer will not be able to satisfy the first prong of this test, as it either knew or should have known of the conduct.

and complex array of advanced technology to monitor employees' transmissions. Because many employers already have the ability to prevent digital sexual harassment facilitated by e-mail, internet, and desktop monitoring software, they should be required to take such preemptive measures.[110]

The affirmative defense should be modified in two respects in cases of digital sexual harassment. First, it should focus on the employer's preventive efforts rather than corrective measures.[111] Second, it should reduce or eliminate the employee's obligation to take advantage of these preventive opportunities, as employees are often unaware of or unable to access monitoring and blocking software.[112]

III. A Proposed Test to Address Sexual Harassment in a Hostile Digital Workplace

Courts should permit employers to plead the affirmative defense in the digital workplace under a limited set of circumstances. Whether a particular case falls into this category should be determined by applying the Digital Workplace Defense Test (DWDT).[113]

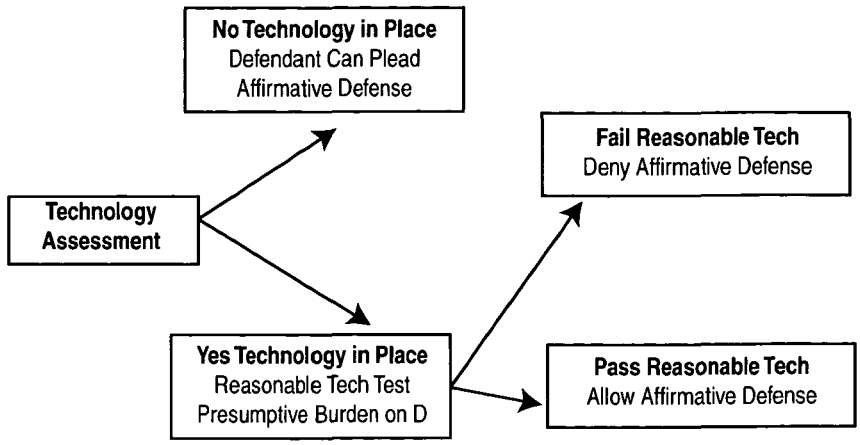
110. *See generally* Joan E. Feldman & Larry G. Johnson, *Lost? No. Found? Yes. Those Computer Tapes and E-mails Are Evidence*, 17 GEN. PRAC. SOLO & SMALL FIRM DIVISION MAG. 2 (Mar. 2000), *available at* http://www.americanbar.org/newsletter/publications/gp_solo_magazine_home/gp_solo_magazine_index/feldman.html; Matthew Fordahl, *Screening of Instant Messaging on Rise*, CHI. TRIB., Apr. 15, 2002, at 6.

111. This is not to suggest that corrective measures will no longer be relevant. In some circumstances, an employer may have the ability to monitor digital communications without the ability to block them. In these instances, the employer's prompt and effective action to address the conduct may demonstrate that it exercised due care.

112. Again, employee actions may nevertheless be relevant. If an employee fails to act with reasonable care in taking advantage of other employer safeguards to either prevent sexual harassment that could have been avoided or to notify the employer of the sexual harassment, the employer's liability may be affected. In other words, while the employee will not have access to, and will often be unaware of, the employer's monitoring and blocking software, the employee should still be required to exercise due care in situations not involving an adverse or tangible employment action.

113. *See supra* note 41, at 90–96 (discussing the Digital Workplace Defense Test).

FIGURE 1
DWDT ANALYSIS



In applying the DWDT, a court should first examine the defendant employer's technological infrastructure to determine whether its existing information technology was capable of monitoring and blocking the digital communications responsible for the sexual harassment claim. If the court ascertains that the technology lacked this capability,[114] the court should allow the defendant to plead the affirmative defense.[115] If the court finds that the employer had and deployed monitoring and blocking information technology capable of detecting and blocking content typical of sexual harassment, it must then determine whether the employer took reasonable steps to monitor and block the communications in question. At this stage, the employer has the burden of proving that it took reasonable efforts to prevent the communications based on

114. Companies usually block all communications that they know fall outside the bounds of acceptable communications in the workplace and monitor employee communications. *See* David F. Linowes & Ray C. Spencer, *Privacy: The Workplace Issue of the '90s*, 23 J. MARSHALL L. REV. 591, 597–615 (1990) (discussing the history of suits brought by employees for invasion of privacy); Gary T. Marx, *The Case of the Omniscient Organization*, HARV. BUS. REV. 12 (Mar.-Apr. 1990) (describing use of new electronic devices to monitor employees outside of traditional "workplace," including monitoring in one's home and car). A company may elect to monitor and then block employee communications depending on the specifics of the company information technology policies. See Julia Turner Baumhart, *The Employer's Right to Read Employee E-Mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923, 936 (1992); see also James J. Ciapciak & Lynne Matuszak, *Employer Rights in Monitoring Employee E-Mail*, FOR THE DEF., Nov. 1998, at 17, 17–20.

115. The genesis of this Article came from the Author's extensive work implementing information technology systems, as he questioned the concept of privacy in light of an employer's unbridled access to all digital communications that employees transmitted via company system components.

the capabilities and normal use of its information technology systems. If the employer cannot establish that its use of monitoring and blocking technology was reasonable, the court should deny the affirmative defense.

Under the framework of this test, the availability of the affirmative defense is contingent on the presence and use of technological systems that are capable of monitoring and blocking digital communications. By placing the burden on the defendant, the court would properly hold employers responsible for the alleged hostile work environments that they control. This approach reflects the reality that, unlike in the physical workplace, preventive measures can effectively eliminate sexual harassment in the digital workplace.

A. Review of an Employer's Technological Systems

In the first step of DWDT analysis, a court should determine whether the employer's technological infrastructure had the capability to monitor and block the particular digital communications alleged in the plaintiff's action.[116] To determine this, the court should explore various aspects of a defendant's technological environment, including infrastructure and policies.[117] The court should address six potentially applicable issues: (1) whether the defendant routinely protects sensitive and confidential information; (2) whether the defendant employs real-time tracking technology to monitor digital activity within its infrastructure; (3) whether the defendant tracks employee activity based on some form of unique ID; (4) whether the defendant monitors suspicious activity; (5) whether the defendant routinely reviews the alerts generated by its logging systems; and (6) whether the defendant uses early end-user monitor management technology.

First, the court should ask whether the defendant protects valuable digital information such as financial data, customer records, or sensitive intellectual property.[118] The court should be mindful that an employer who protects its digital information is likely to monitor its web applications because early detection enables the defendant to avert serious

116. *See* Lynda M. Applegate, James I. Case, Jr., and D. Quinn Mills, *Information Technology and Tomorrow's Manager*, HARV. BUS. REV., AT 128 (Nov.-Dec. 1988).

117. *See* Karen Nussbaum, Editorial, *Workers Under Surveillance*, COMPUTERWORLD, Jan. 6, 1992, at 21.

118. *See generally* Carl Botan, *Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects*, 63 COMM. MONOGRAPHS 293 (1996).

economic damage.[119] For example, employers in the media industry protect their media with both physical and digital technologies, often using some form of encryption and an access monitoring tool, to ensure that employees do not make unauthorized copies of the media for prerelease.

Second, the court should consider whether the defendant employs any real-time suspicious activity and policy violation detection technologies.[120] Some financial institutions, for example, implement instant messaging systems with real-time logging capabilities[121] that not only enable the institutions to comply with the message storage requirements that are established under the Sarbanes-Oxley Act but also allow them to track instant message conversations as they occur.[122] The court should examine whether the defendant's inaction with respect to digital sexual harassment is reasonable in light of the specific capabilities of its monitoring technology.[123] When such technology is actively used, the court should further explore the process and design of the system, focusing on whether the defendant monitors and blocks communications.[124]

Third, the court should examine whether the defendant utilizes user tracking technology capable of recording employees' actions with respect to a particular Web-based tool set, such as the "research trail"

---

119. *See generally* Philip Brey, *Worker Autonomy and the Drama of Digital Networks in Organizations*, 22 J. BUS. ETHICS 15 (1999); *Vision & Values: Better World—Our Commitment to Society*, BRITISH TELECOM (2001), *available at* http://www.btplc.com/Societyandenvironment/PDF/2001/vision_values.pdf.

120. *See generally* Bill Bruck, *How Companies Collaborate Sharing Work Online* (2001), *available at* http://consortium.caucus.com/pdf/collaboration.pdf; Collaborative Strategies, *Electronic Collaboration on the Internet and Intranets: How Major Corporations Are Leveraging IP Networks for Competitive Advantage* (2001).

121. *See* Roger Harris, *IM: When Time Matters*, HISPANIC BUS., Nov. 2002, at 34, *available at* http://www.hispanicbusiness.com/news/newsbyid.asp?id=7679&cat=Magazine&more=/magazine.

122. *See* Doug Henschen, Penny Lunt Crosman and Ralph Gammon, *Brave New World: Three Trends Redefining Content Management*, TRANSFORM MAG., Apr. 2004, at 16, 16–18, 20–22, 24.

123. *See* W. Michael Hoffman, Laura P. Hartman, and Mark Rowe, *You've Got Mail . . . and the Boss Knows: A Survey by the Center for Business Ethics of Companies' Email and Internet Monitoring*, 108 BUS. & SOC'Y REV. 285, 302 (2003).

124. *See generally*, AMA/ePolicy Inst. Research, *2007 Electronic Monitoring & Surveillance Survey* (2008), *available at* http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf (citing another AMA study and stating that concern "over litigation and the role electronic evidence plays in lawsuits and regulatory investigations has spurred more employers to monitor online activity. Data security and employee productivity concerns also motivate employers to monitor Web and e-mail use and content. Workers' e-mail and other electronically stored information create written business records that are the electronic equivalent of DNA evidence.").

provided by Westlaw.[125] When an employer uses such tracking devices, the court should ascertain whether the employer could have reasonably modified this monitoring and tracking technology to protect employees from sexual harassment in the digital workplace.[126]

Fourth, the court should determine whether the defendant uses real-time technology to monitor its systems for suspicious behavior related to the activities of its users.[127] For example, when a user mistypes his or her password three times, the system may flag the account or send an alert in real-time to a monitoring party. Such technology assists banks in preventing fraud or abuse of financial accounts and is common in the financial sector.[128]

Fifth, the court should review all of the defendant's logging systems.[129] Financial and medical organizations rely heavily on these systems to access data that enables forensic computer experts to construct an audit trail and deliver evidence of transactions.[130] Hospitals also often use this technology to track the protection of patients' digital records and demonstrate that the records are released only to authorized parties.[131]

---

125. *See* Westlaw, http://www.westlaw.com.

126. *See generally* Joey F. George, *Computer-Based Monitoring: Common Perceptions and Empirical Results*, 20 MIS Q. 459 (1996); Terri L. Griffith, *Monitoring and Performance: A Comparison of Computer and Supervisor Monitoring*, 23 J. APPLIED SOC. PSYCHOL. 549 (1993).

127. *See* Martin Butler, Op-Ed., *Staff Left in the Dark Over Monitoring Technologies*, COMPUTER WKLY., May 4, 2004, at 24.

128. *See generally* E.L. Lesser & J. Storck, *Communities of Practice and Organizational Performance*, 40 IBM SYS. J. 831 (2001).

129. *See generally* Simson L. Garfinkel, Op-Ed., *Private Matters: Could Your Organization's Privacy Practices Stand the Scrutiny of a Newspaper Exposé?*, CIO, Jun. 1, 2000, at 178; Il-Horn Hann et al., *Online Information Privacy: Measuring the Cost-Benefit Trade-Off*, INT'L CONF. ON INFO. SYS., 2002, at 1–2, *available at* http://www.comp.nus.edu.sg/~ipng/research/privacy_icis.pdf.

130. *See* Hoffman et al., *supra* note 123, at 290–92.

131. V. John Ella, *Unauthorized Access to Medical Records Under Company Policy and HIPAA Supports Denial of Unemployment Benefits*, WORKPLACE PRIVACY DATA MANAGEMENT & SECURITY REPORT (Apr. 7, 2011), http://www.workplaceprivacyreport.com/2011/04/articles/hipaa-1/unauthorized-access-to-medical-records-under-company-policy-and-hipaa-supports-denial-of-unemployment-benefits/; William Maruca, *California Hospitals Fined for Employees' Unauthorized Access of Patient Records*, HIPAA, HITECH & HIT (June 11, 2010) http://hipaahealthlaw.foxrothschild.com/2010/06/articles/privacy/california-hospitals-fined-for-employees-unauthorized-access-of-patient-records/. *See also* Erin Eiselein, *Unauthorized File Access: How to Avoid Lawsuits* (Jan. 2008), http://www.dgslaw.com/attorneys/ReferenceDesk/Eiselein_UnauthorizedFileAccess.pdf.

Sixth, the court should determine whether the defendant uses a form of early end-user management monitoring technology.[132] This technology monitors end-users from the end users' location.[133] For example, global companies with worldwide customers use tools that monitor the location from which their customers communicate.[134] Employers frequently use this technology to ensure that employees perform work off-site and that clients receive authorized services.[135]

These six elements are intended only as guidelines for courts, since different companies combine them uniquely and in addition to other forms of technology.[136] Regardless of the individual characteristics of the different tools and their uses, however, these guidelines can help determine the degree of actual tracking, monitoring, and blocking of digital activity in light of the capabilities of an employer's particular technological system.

Courts should apply a reasonableness standard in their analysis of employers' blocking and monitoring capabilities.[137] Although a malleable concept, courts are nonetheless often required to use a reasonableness standard.[138] In applying the standard to cases of digital sexual harassment, courts should be mindful of the costs and efforts associated with, and the employer's knowledge of, the employer's respective monitoring capabilities.[139] More precisely, courts should make fact-specific inquiries on a case-by-case basis, considering factors such as the size of the company, the number of employees, the ease and economy with which the system can be used or modified to monitor and prevent sexual harassment, the employer's awareness of sexual harassment acts, and the volume of the digital transmissions the employer must track.[140] Finally, courts

132. *See* Jay Mellman, *Where IT, Business Meet*, COMM. NEWS, Aug. 2005, at 38, 39–40, *available at* http://www.comnews.com/stories/articles/0805/0805where_IT.htm.

133. *See id.*

134. *See* Dawn S. Onley, *Technology Gives Big Brother Capability: New Technology Allows Companies to Monitor Employees' Whereabouts to Improve Productivity*, HR MAG., July 2005, at 99, 99–101.

135. *See* Mellman, *supra* note 132, at 39–40.

136. *See generally* Urofsky v. Gilmore, 216 F.3d 401 (4th Cir. 2000); Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, 5 CHI LETTERS 129 (Apr. 5–10, 2003), *available at* http://www.cs.colorado.edu/~palen/Papers/palen-dourish.pdf.

137. *See generally* Paul Attewell, *Big Brother and the Sweatshop: Computer Surveillance in the Automated Office*, 5 SOC. THEORY 87 (1987).

138. The reasonable person standard is commonplace in tort, criminal law, and commercial law. *See, e.g.*, U.C.C. § 2-504 (2003) (make contract for transportation of goods "as may be reasonable").

139. *See* Hoffman, *supra* note 123.

140. In essence, the analysis resembles a cost/benefit analysis that examines the reasonableness of preventing sexual harassment in the context of a particular employer's technological capabilities and current use of such technology. For example, if an

should closely scrutinize defendants who use technology that complies with the Sarbanes-Oxley Act,[141] HIPAA,[142] or other legislatively mandated tracking or monitoring requirements.[143] In such cases, monitoring and tracking technology will almost certainly be in place.[144]

When a court finds that a defendant does not possess the necessary technological infrastructure, the court should permit the defendant to plead the affirmative defense as it currently operates, with the focus placed on corrective procedures and preventive measures. When the infrastructure is in place but has not been used to prevent sexual harassment, the affirmative defense should also be permitted, except when the plaintiff's claim presents clear and convincing evidence that the defendant deliberately decided not to use the existing technology. For example, if a plaintiff produces e-mails establishing that the decision was driven by a desire to avoid losing the right to plead the affirmative defense, the court should deny the defendant the right to assert the affirmative defense notwithstanding the technological systems in place. This exception is necessary because courts should sanction defendants who purposely expose their employees to a hostile digital workplace. After finding that the defendant's infrastructure was capable of blocking and monitoring the alleged digital communications, the court must then determine whether the defendant took reasonable steps to block or monitor the communications.[145]

---

employer currently uses e-mail monitoring technology and would not incur additional cost to monitor e-mails for inappropriate and offensive communications, it would be reasonable to impute liability or limit the employer's ability to use an affirmative defense.

141. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15 USC, and 18 USC)

142. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26 U.S.C., 29 U.S.C., and 42 U.S.C.).

143. Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (codified as amended in scattered sections of 15 U.S.C.).

144. *See generally* Jeremy U. Blackowicz, Note, *E-Mail Disclosure to Third Parties in the Private Sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80 (2001).

145. *See e.g.*, Doe v. XYC Corp, 887 A.2d 1156, (N.J. 2005). In *Doe*, the court looked into three areas to determine if the monitoring was legal. First, the court looked to whether the employer had the capability to monitor. *See id.* at 1164 (holding that the suspect's "immediate supervisor, [searched through the employee's] computer while he was at lunch and clicked on 'websites visited.' . . . [N]one of the sites identified were actually explored and no further action was taken to determine the nature of Employee's pornographic related computer activities. Instead, [the supervisor] was simply instructed to tell Employee to stop whatever he was doing. Thus, defendant's capability to monitor Employee's activities on his work computer was clearly established."). The court then looked to whether the employee had a legitimate expectation of privacy. *See id.* at 1166 (finding that the employee's "office, as with

B. Determination of Whether the Employer Took Reasonable Efforts to Prevent the Receipt or Transmission of the Digital Communications

In the second step of the DWDT analysis, the court should use the information acquired in the first step to determine whether the company took reasonable measures to track digital communications unrelated to the sexually harassing communications. The court may find it appropriate to appoint an independent third party, similar to an expert called to resolve digital discovery disputes, to determine whether the defendant used its existing technology in a reasonable manner to protect the digital workplace. As mentioned above, the court must perform fact-specific analysis in each case, considering both fiscal costs and corporate policies, to determine the practicability of the defendant's implementation of its technological system.

CONCLUSION

Sexual harassment and hostile work environments violate an individual's right not to suffer discrimination in the workplace. Because employers cannot control the actions of all their employees, business associates, or customers and cannot compel them use their preventive procedures, the Supreme Court adopted equitable principles in permitting an affirmative defense. Today, however, courts have yet to fully appreciate an employer's ability to take reasonable preventive measures to protect the digital workplace.[146] This creates a disincentive for employers use of these digital measures and is inconsistent with the congressional mandate to prioritize avoiding harm over the providing

---

others in the same area, did not have a door and his computer screen was visible from the hallway, unless he took affirmative action to block it. Under those circumstances, we readily conclude that Employee had no legitimate expectation of privacy that would prevent his employer from accessing his computer to determine if he was using it to view adult or child pornography."). Finally, the court analyzed whether the employer had a right to search the office to investigate an employee's computer use. *See id.* at 1166 (concluding that the employer, "through its supervisory/management personnel, was on notice that Employee was viewing pornography on his computer and, indeed, that this included child pornography [and thus had a duty to investigate].").

146. *See, e.g.*, Adam C. Losey, *Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 FLA. L. REV. 1179 (2008); Cicero H. Brabham, Jr., Note, *Curiouser and Curiouser: Are Employers the Modern Day Alice in Wonderland? Closing the Ambiguity in Federal Privacy Law as Employers Cyber-Snoop Beyond the Workplace*, 62 RUTGERS L. REV. 993 (2010).

redress.[147] Given employers' expansive monitoring of employees' digital communications in general, it is reasonable for courts to require the monitoring of communications that are of a sexually harassing nature. The courts, therefore, should modify the affirmative defense to ensure protection of the workplace for employees and to create an effective legal framework to address digital sexual harassment claims.

147. Employer reasons for monitoring are diverse and important:

> Electronic monitoring allows employers to make significant gains in the areas of productivity, quality, and safety. Monitoring enhances productivity by facilitating more efficient resource scheduling, more immediate feedback, and more meaningful evaluations. Quality likewise is improved, and customers benefit from better service and lower prices. Monitoring is key to some safety initiatives, and better safety means lower insurance premiums and workers' compensation payouts. Payroll and equipment costs can also be reduced by monitoring employees for personal use of company equipment and for taking excessive breaks. It has been estimated that employees wasted 170 billion dollars of employer time in one year alone. Further savings may be realized by curbing theft and legal liability.
>
> In one year, it is estimated that employees stole the equivalent of 370 billion dollars from their employers. Monitoring can be used to detect illegal or wrongful deeds so that the offenders may be punished. For example, the data flow in and out of a company can be watched to find employees transmitting sensitive data or hackers attempting to crack into the system. E-mail within the workplace also can be monitored to detect electronic harassment. Alternately, monitoring may be used proactively to minimize *respondeat superior* liability to detect a problem before it happens. As a final incentive, the law sometimes requires employers to monitor employees.

Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 319–20 (2002) (citations omitted). *See also* Jill S. Chanen, *The Boss is Watching*, A.B.A. J., Jan. 2008, at 48, *available at*: http://www.abajournal.com/magazine/article/the_boss_is_watching/ (discussing the multitude of issues facing employers and employees with workplace privacy and monitoring).