Sexual Harassment: Limiting the Affirmative Defense in the Digital Workplace

Donald P. Harris  
*James E. Beasley School of Law, Temple University*

Daniel B. Garrie  
*Rutgers University School of Law*

Matthew J. Armstrong  
*Rutgers University School of Law*

Follow this and additional works at: [https://repository.law.umich.edu/mjlr](https://repository.law.umich.edu/mjlr)  
Part of the [Civil Rights and Discrimination Commons](https://repository.law.umich.edu/mjlr), [Labor and Employment Law Commons](https://repository.law.umich.edu/mjlr), [Law and Gender Commons](https://repository.law.umich.edu/mjlr), and the [Science and Technology Law Commons](https://repository.law.umich.edu/mjlr)

Recommended Citation  
Available at: [https://repository.law.umich.edu/mjlr/vol39/iss1/4](https://repository.law.umich.edu/mjlr/vol39/iss1/4)

This Article is brought to you for free and open access by the University of Michigan Journal of Law Reform at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in University of Michigan Journal of Law Reform by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.
Digital communications sexual harassment is on the rise. Such harassment occurs through sexually offensive and unwarranted e-mails, placing harassing messages on electronic bulletin boards, and other forms of harassment that occur through the Internet. To date, courts have remained silent on the issue of sexual harassment by digital communications. Should this type of harassment be treated any differently than harassment that occurs in the physical space? The somewhat surprising answer is yes.

This Article advocates applying a new judicial framework for addressing digital communications sexual harassment. This new framework accounts for the real-world technology in the digital workplace and the legal framework that courts have constructed in connection with affirmative defenses to harassment. An employer's ability to monitor and block digital communications and thus prevent sexual harassment is the fundamental difference between digital and physical sexual harassment and the underlying reason for treating them differently and for modifying the affirmative defense. The Article proposes that when an employer fails to utilize available technology to prevent sexual harassment, the affirmative defense should be either modified or altogether unavailable. Adopting this approach, courts would appropriately place an affirmative obligation on employers with blocking and monitoring technology to take reasonable preventative measures to prevent digital workplace harassment.
I. Introduction

Sexual harassment law has greatly evolved over the last few decades. Specifically, harassment claims have expanded to include employer liability for co-worker harassment, supervisor harassment, and, most recently, third party harassment. Correspondingly, courts have provided employers with specific defenses against such liability. For example, an employer escapes liability if the employer takes preventative and corrective measures reasonably calculated to end the harassment. Such absolution is justified because in many instances, the employer is unable to prevent the harassment from occurring but is able to take subsequent measures to ensure that the harassment does not continue or recur.

This judicial treatment, however, provides little comfort to a harassment victim. The ideal solution would be to prevent harassment from occurring in the first instance. The Supreme Court agrees; it has held that employers should take preventive measures to ensure a harassment-free workplace consistent with Title VII of the Civil Rights Act of 1964 and its policy of encouraging the creation of antiharassment policies and effective grievance mechanisms. While providing this type of environment is not always possible in the physical workplace—hence providing the need for the corrective measures affirmative defense—it is possible in the digital workplace, where communication occurs more regularly through e-mail, the Internet, instant messaging, and other digital means.

Increasingly, sexual harassment conduct includes actions through these digital communications. Unlike with physical har-

---

3. See Kaplowitz & Harris, supra note 1, at 36.
4. Id. at 38.
5. Faragher, 524 U.S. at 806; Ellerth, 524 U.S. at 765.
assment claims, employers have access to technology capable of preventing digital communication harassment claims. In particular, companies can deploy existing information technology ("IT") with which they can monitor and block offending digital communications. Equipped with this technology, employers are able to, and often already do, monitor employee communications. Employers do so for various reasons, including protecting trade secrets, monitoring productivity, and enforcing corporate information technology use policies. In light of these uses, and more importantly, the legal sanction of these uses, employers should monitor their networks for offensive e-mails or communications that constitute harassment, thereby securing a harassment-free workplace. Employer liability thus should turn on whether the employer took reasonable precautions in view of the available technology. The outcome of that assessment should have a direct bearing on the employer's ability to claim an affirmative defense to employee allegations of digital workplace harassment.

This Article addresses sexual harassment in the modern digital arena. Specifically, it offers a new framework for courts to analyze digital sexual harassment claims. Part II of this Article briefly reviews the legal remedies for sexual harassment and the employer's affirmative defense, including the underlying rationale for the defense. Part III provides a critique of the defense when it is applied to the digital workplace environment. The failure of the employer to capitalize upon and utilize the available technology to prevent sexual harassment is cause to modify or make unavailable the affirmative defense. Finally, Part IV offers a new test—the Digital Workplace Defense Test—that courts should invoke when reviewing an affirmative.

In essence, the modified test and framework provide that courts should permit the affirmative defense in the digital workplace only under limited circumstances. Accordingly, courts first should examine the defendant employer's technology infrastructure to determine whether the defendant's existing information technology was capable of monitoring and blocking the digital

8. Id.
9. See discussion infra Part III.A.
11. Id. at 713.
12. Id. at 725-26.
communications comprising the harassment claim. If the employer does not possess the requisite technological capabilities, the employer should be permitted to plead the affirmative defense. If, however, the court finds that the defendant possessed such capabilities, the court then should explore whether or not the defendant took reasonable steps to monitor and block the offensive digital communications or whether the defendant can articulate a rational reason for not utilizing readily available technology to prevent workplace digital harassment. A critical factor here is whether the employer utilizes such technology for other non-harassment related uses. If the court concludes that the defendant did not take reasonable steps, the court should not allow the defendant to plead the affirmative defense. Adopting this approach, courts would appropriately place an affirmative obligation on employers who possess blocking and monitoring technology to take reasonable preventive measures to prevent digital workplace harassment.

II. HOSTILE WORK ENVIRONMENT AND GENDER DISCRIMINATION

Claims about gender discrimination derive from Title VII of the Civil Rights Act of 1964. Congress enacted Title VII to protect employees from discrimination based on gender, race, or religion in the workplace. Title VII establishes two different theories of liability based on gender discrimination and sexual harassment: (1) Hostile work environment; and (2) Quid pro quo, or discriminatory acts having tangible employment consequences.

13. See discussion infra Part IV.A.
14. See Rogers v. EEOC, 454 F.2d 234, 238 (5th Cir. 1971); Snyder v. Guardian Auto. Prods., Inc., 288 F. Supp. 2d 868, 874 (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).
15. See Rogers, 454 F.2d at 238; Snyder, 288 F. Supp. 2d at 874.
18. Id.
19. Id.
A. Review of Legal Remedies

Courts first recognized the hostile work environment cause of action in race-discrimination cases beginning in the early 1980s. A hostile work environment is created when conduct by a supervisor, co-worker, or third party occurs that is sufficiently severe or pervasive to alter the conditions of an individual's employment and create an abusive working environment. In *Meritor Savings Bank v. Vinson*, the United States Supreme Court, recognizing that sexual harassment constitutes a form of gender discrimination and is therefore prohibited by Title VII, extended the hostile work environment cause of action to include sex discrimination. 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 supervisor, co-worker, or third party. When harassment is alleged based on conduct by a co-worker or third party, the employer is liable only if the plaintiff can prove that (1) the employer knew of or should have known of the harassment, and (2) the employer failed to take prompt and effective remedial action reasonably calculated to end the harassment—in essence a negligence standard. As to supervisor harassment, the Court declined "to issue a definitive rule on employer liability" when supervisors create hostile work environments. Rather, the Court simply stated that it "agree[d] with the EEOC that

---

21. See generally Kaplowitz & Harris, *supra* note 1, at 33.
23. See *id.* at 73; *see also* Broderick v. Ruder, 685 F. Supp. 1269 (D.D.C. 1988) (finding supervisors' behavior created a hostile environment).
24. *Faragher v. City of Boca Raton*, 524 U.S. 775, 793-801 (1998); *Meritor*, 477 U.S. 57; *see also* Kaplowitz & Harris, *supra* note 1, at 33-34.
25. 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 employer's response to complaint of sexual harassment fell short of prompt remedial action reasonably calculated to end the harassment where 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 1, at 36.
26. *Meritor*, 477 U.S. at 65-66 (citing *Firefighters Inst. for Racial Equal. v. City of St. Louis*, 549 F.2d 506, 514-15 (8th Cir. 1977); *Gray v. Greyhound Lines*, 545 F.2d 169, 176 (D.C. Cir. 1976); Rogers v. EEOC, 454 F.2d 234, 238 (5th Cir. 1971)), 454 F.2d at 238. The Court articulated 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." *Id.* at 65.
27. *Id.* at 72.
Congress wanted courts to look to agency principles for guidance in this area."

The lack of a definitive rule on this point initiated twelve years of controversy and disagreement in the lower circuit courts. These courts sought to establish a standard for employer liability based on the Supreme Court's broad recommendation to apply agency principles. To summarize the various circuit court approaches, courts have held employers vicariously liable for supervisor misconduct under three different theories: (1) the supervisor was "aided by" within the scope of his or her employment; (2) the supervisor was "aided by" the agency relationship in committing the harassment; or (3) the employer had actual or constructive knowledge of the harassment and failed to remedy it. In addition to agency principles, courts also have held employers liable on negligence grounds for failing to prevent harassment.

In order to resolve the disagreement among the circuit courts, the Supreme Court established a new standard for employer liability in two groundbreaking decisions, Faragher v. City of Boca Raton and its companion case, Burlington Industries, Inc. v. Ellerth. In these cases, the Court set forth two different standards for employer liability. First, the Court held that if supervisor harassment is not accompanied by an adverse official act or "tangible employ-

28. Id. With regard to 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.
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 co-workers 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 (2nd 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.").
ment action," such as discharge, demotion, or undesirable reas-
ignment, the employer still may be held liable. In such situations,
the employer may raise an affirmative defense to such liability. The
affirmative defense must consist 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 provided by the employer or to avoid
harm otherwise."\textsuperscript{35}

Next, the Court held that if the supervisor harassment is accom-
panied by an adverse official act then the employer is strictly
liable.\textsuperscript{34} Most notably, the Court held that the affirmative defense is
not available to an employer when a "tangible employment action"
occurrents.\textsuperscript{35} When a tangible adverse employment action accompanies
the harassment, strict liability is appropriate—and the affirmative
defense is appropriately unavailable—for a variety of reasons, in-
cluding: (1) that a supervisor’s decision "merges" with the
employer, and his act becomes that of the employer; (2) the super-
visor acts within the scope his or her authority when he or she
hires, fires, or demotes the employee; and (3) the supervisor is
aided by the agency relation in discriminating against the em-
ployee.

\textbf{B. Rationale Behind the Supreme Court’s Creation
of the Affirmative Defense}

The Supreme Court reasoned that creating the employer’s af-
firmative defense provides an incentive for employers to take both
preventive and remedial measures to limit occurrences of sexual
harassment in the workplace.\textsuperscript{36} Examples of such measures include
instituting a grievance procedure, educating employees and super-
visors about sexual harassment, and ensuring that employees are
notified of their rights regarding harassment.

In holding that employers can be held vicariously liable for su-
pervisors’ conduct, the Court recognized that employers are in a

\textsuperscript{33} Faragher, 524 U.S. at 807; Ellerth, 524 U.S. at 765.
\textsuperscript{34} Faragher, 524 U.S. at 808; Ellerth, 524 U.S. at 765.
\textsuperscript{35} Faragher, 524 U.S. at 790–91.
\textsuperscript{36} See Petrosino v. Bell Atl., 385 F.3d 210, 226 (2d Cir. 2004); Pfeiffer v. Lewis County,
position to prevent sexual harassment—a clear goal of Title VII. However, the Court also recognized that employers are not the only actors that can minimize harassment. Thus, while the first prong of the affirmative defense imposes an affirmative obligation on employers to prevent the harassment from occurring, the second prong imposes an obligation on employees to take actions to minimize any harm caused to them.

C. The Affirmative Defense Setting Today

While the Court's holding is not an explicit mandate for employers to adopt internal anti-harassment policies and procedures, the Court's pronouncement provides a noteworthy incentive by granting employers possible immunity if they do implement such policies and procedures. In explaining why employer liability might appropriately be applied for supervisor misconduct under certain circumstances, the Court noted that the different treatment between supervisors on the one hand, and co-workers and third parties on the other, is justified because a supervisor "[n]ecessarily draw[s] upon his superior position" in harassing the victim, and the employer has a greater opportunity to guard against supervisor misconduct. The Court refused, however, to impose "automatic liability" for supervisor harassment, stating that under certain conditions it may be inappropriate, for instance when the employer exercised due care to avoid harassment and to eliminate it when it occurred.

In 2004, in Pennsylvania State Police v. Suders, the United States Supreme Court reaffirmed the affirmative defense in the context

37. 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))).
38. See, e.g., Slay v. Glickman, 137 F. Supp. 2d 743, 752 (S.D. Miss. 2001) (granting employer’s motion for summary judgment, concluding that 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); 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).
40. Id. at 805.
of a constructive discharge claim. In *Suders*, a female police dispatcher for the Pennsylvania State Police filed a claim against her employer alleging both sexual harassment and gender discrimination.\(^{42}\) *Suders* claimed constructive discharge by alleging that relentless sexual harassment by her supervisors left her no option but to resign from her position.\(^{43}\) Reversing the trial court's decision, the Third Circuit held that *Suder's* constructive discharge constituted an adverse employment action, and therefore, under the *Faragher* and *Ellerth* framework, the employer was strictly liable and was not permitted to assert the affirmative defense.\(^{44}\)

The Supreme Court reversed, holding that while some constructive discharge cases amount to official employer action, not all constructive discharges result from a supervisor's official act. Accordingly, the Court concluded that the employer is prohibited from relying on the affirmative defense only when a supervisor's official act precipitates a constructive discharge. Where, however, there is no official act underlying the constructive discharge, the employer is entitled to assert the affirmative defense.\(^{45}\) *Suders* thus reinforces the role of the affirmative defense in the physical workplace; it does not, however, answer the question of whether the affirmative defense should be permitted in the digital workplace.\(^{46}\)

III. CRITIQUE OF THE AFFIRMATIVE DEFENSE IN THE DIGITAL WORKPLACE

Digital workplace harassment arises when employees use e-mail or the Internet to sexually harass other employees or to create hostile work environments.\(^{47}\) Very few cases have addressed employer liability for such acts. In *Owens v. Morgan Stanley & Co.*, the court held that a single incident of inappropriate e-mail was not sufficient to establish a claim even though unchecked offensive e-mail communications circulating within the workplace could constitute

---

42. *Id.* at 133.
43. *Id.*
44. *Id.* at 139.
45. *Id.* at 148.
46. See *id.*
47. See 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).
harassment. In *Strauss v. Microsoft Corp.*, the court held that jokes and sexual parodies, in addition to other remarks, e-mailed by a supervisor to employees were admissible and relevant evidence of sexual harassment.

In *Blakey v. Continental, Inc.*, the New Jersey Supreme Court found that a harassed female employee had a valid harassment claim where the allegedly defamatory and sexually harassing material was posted on an electronic bulletin board. Although the employees could access the bulletin board only through the Internet, and the employer, Continental, did not maintain the bulletin board, the court found that Continental had a duty to remedy the harassment and correct off-site harassment by co-workers. The court found that the employer bulletin board forum was sufficiently integrated into the workplace and Continental had notice of the harassment. *Blakey* stresses that an employer’s responsibility to prevent sexual harassment and hostile work environments may extend to both the physical and digital workplaces. Under *Blakey*, employers are obligated to take affirmative steps to halt employee-to-employee digital harassment once the employer has knowledge of harassment.

The court stopped short of placing an affirmative obligation on employers to prevent sexual harassment by having employers monitor digital communications. The *Blakey* court stated that while “employers do not have a duty to monitor private communications of their employees,” employers “do have a duty to take effective measures to stop co-employee harassment when the employer knows or has reason to know” of such harassment. *Blakey* limited its reach due to “grave privacy concerns.” However, recent deci-

50. *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.
51. *Id.* at 543, 551–52, 558.
52. *Id.* at 551.
53. *Id.* at 551–52.
54. *Id.* 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).
55. *Blakey*, 751 A.2d at 551.
sions and legislative enactments have reduced privacy concerns and suggest extending Blakey.

A. Monitoring Technology in the Workplace

Courts have recognized an employer's right to monitor employees' e-mail messages and use digital technologies to protect trade secrets. In addition, courts have consistently found that employees do not have an objectively reasonable expectation of privacy when employers have e-mail policies that notify employees that the employer may monitor their e-mail or Internet use. Employers have the right to invade employees' digital work spaces because employers have legitimate interests in all communications transmitted on their digital networks. For instance, an employer has the right to observe employees' transmitted digital communications to ensure work productivity, to prevent trade secret disclosure, to prevent transmission of defamatory statements, and to prevent transmission of unauthorized or illegal material over the employer's digital communication network.

In monitoring employees, the vast majority of large employers use digital tracking technology. According to a recent Washington Internet Daily release, eighty percent of major U.S. companies at least sometimes record and review employees' electronic communication or browser use. Sixty-seven percent of employers have disciplined at least one employee for improper or excessive use of e-mail or Internet access; thirty-one percent have fired employees

56. Id.; see also Eric P. Robinson, Big Brother or Modern Management: E-mail Monitoring in the Private Workplace, 17 LAB. LAW. 311, 325–26 (2001).


58. See 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").

59. Morris, supra note 10, at 702.

60. Id.


62. Lawyer; Employers Fighting Net Abuse Must Mind Privacy, WASH. INTERNET DAILY, Apr. 24, 2002, available at http://www.wrf.com/ (search "employers fighting net abuse"; then follow article hyperlink under "In the News").

63. Id.
for such conduct. It is estimated that more than three-quarters of major U.S. corporations record and review employee communications and activities on the job, including but not limited to, telephone calls, e-mail, Internet communications, and computer files. E-mail monitoring by employers is a necessity as well as a legally recognized right. Courts have granted employers this right to enable them to 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.

Many companies utilize software to monitor and/or block their employee’s use of the corporate technology infrastructure. SilentRunner is illustrative of such software. While most lawyers and employees have never heard of SilentRunner, many companies and governmental agencies use the program to monitor their agents

64. Id.
67. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002); Greenfield & Davis, supra note 7, at 348.
70. See Jeffrey Benner, Privacy at Work? Be Serious, Wired News, Mar. 1, 2001, http://www.wired.com/news/business/0,1367,42029,00.html; see also Benner, supra note 69 (“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 twenty-one ‘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 twenty-one, including one Vice President, resigned after being identified.”).
and employees. According to TruSecure spokeswoman Susan Lee, SilentRunner provides constant employee monitoring for nearly four hundred companies. Organizations using SilentRunner and similar software, such as Deloitte & Touche, have adopted top-secret attitudes towards their employees regarding their use of the product. Maintaining secrecy about employee monitoring software enables companies to avoid scrutiny from groups concerned about the erosion of privacy in the workplace. While the efforts of some companies to maintain secrecy about their monitoring software may imply that such monitoring is indeed immoral, dishonest, or unethical, whether it is in fact such turns on the employee’s reasonable expectations. In situations where the employer’s policies make it clear to employees that such monitoring takes place, the employee has no or very little expectation of privacy. Where no such policy is made clear to employees, the question is more open to debate.

In addition to employer's ability to monitor employee digital transmissions, employers often possess a high degree of control over employee computer desktops. This control is meant to help employee productivity by ensuring that a uniform technical environment exists. For example, ActivatorDesk’s Enterprise Desktops Controller monitors employee computing activities and compares those activities to a list of approved activities. If an employee performs non-previously approved activities, "ActivatorDesk can

72. Benner, supra note 69.
75. Benner, supra note 69 ("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.").
76. 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.
77. Id.
instantly implement a 'lock-down policy'” while sending network administrators an e-mail alerting them of the violation. Another example is WinWhatWhere’s Investigator, which offers “Stealth WebCam Monitoring,” to snap images with computer cameras enabling the employer to tie computer usage to specific employees. WinWhatWhere’s Investigator also offers key-phrase alerts, which monitors computers for specific phrases and instantly notifies system administrators if a restricted phrase is spotted.

In sum, the majority of large corporate employers in the United States currently use digital monitoring and blocking software. With this software these employers have the ability to observe and block inappropriate digital communications over corporate IT networks before the intended recipient receives them. Currently, employers have utilized this power without also being required to protect their employees. As a result, employees are relinquishing privacy rights without receiving any benefit of employer protection in return. Due to the judicially recognized diminished expectation of privacy in the workplace, employees are only entitled to bring suit when an intrusion infringes upon intensely private matters or when the employer has failed to inform them of the monitoring.

In Leventhal v. Knapek, the Second circuit illustrated this principle. Here, the court held that an employee does not have a reasonable expectation of privacy with respect to his digital activities in the workplace. In support of the same principle, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA), and the Stored Communications Act (SCA), granting employers the right to monitor employees’ e-mail messages. The ECPA and SCA permit an employer to monitor e-mail communications, as long as the monitoring occurs in the ordinary course of business. The majority of case law interpreting the ECPA has found

79. Id.; see also Wallace Immen, Workplace Privacy Gets Day in Court, GLOBE & MAIL, Apr. 28, 2004, at C1.
80. See Delio, supra note 78.
81. Id.
83. 266 F.3d 64 (2d Cir. 2001).
84. Id. at 74.
that employers can monitor employee e-mail messages with or without consent, even without notice.\(^7\)

The combined actions of Congress and the courts have effectively expanded employer abilities to monitor employee electronic communications without violating federal privacy laws.\(^8\) Because employers now have access to, and control over, employee electronic communications, they have the ability to greatly minimize instances of digital sexual harassment in the workplace.\(^9\) For example, employers can block e-mails containing sexually explicit terms and restrict wallpaper settings on corporate computers so that users cannot display inappropriate or offensive material. The ability and the right to monitor all employee digital transmissions places employers in an ideal position to take simple proactive preventive measures that may prevent the majority of instances of digital sexual harassment in the workplace.

The Ellerth and Faragher decisions and the Blakey line of cases should be extended as a result of employers' rights and abilities to read digital communications sent and received by employees. Employers using blocking and monitoring technology have effective notice of potential workplace sexual harassment before the intended recipient receives it.\(^9\) As a result, the employers should bear the burden of providing reasonably sufficient technical protection to limit exposure to digital workplace sexual harassment. Unfortunately, however, courts have not yet bridged the gap between employer freedom to monitor employee acts and employer responsibility to monitor employee acts. More precisely, courts have yet to address whether an employer should be entitled to plead an affirmative defense for digital sexual harassment when the employer fails to monitor the digital work environment, prevent digital sexual

---

87. See, e.g., Theofel v. Farey-Jones, 359 F.3d 1066, 1075 (9th Cir. 2004); Fraser v. Nationwide Mut. Ins. Co., 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); 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.”).

88. See supra notes 83–87 and accompanying text.

89. See supra notes 63–67 and accompanying text.

90. See generally 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 or intent to monitor use).
harassment, or institute mechanisms to facilitate employee complaints pertaining to digital sexual harassment.91

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

In Ellerth92 and Faragher,93 the Supreme Court sought to compel employers to take a proactive role in preventing workplace sexual harassment. Today, an employer pleading the affirmative defense is able to avoid being held accountable for hostile digital work environments created by the transmission of sexually harassing material over corporate IT networks. By not requiring preventive policies, courts deny employees the benefit of receiving assistance before sexual harassment occurs. This is particularly inappropriate when the employers have effective notice of sexually harassing communications through the use of monitoring software.94 This result violates the U.S. Supreme Court’s intent, as stated in Ellerth and Faragher and discussed in Blakey, to compel employers to take a proactive role in preventing workplace sexual harassment.95 In addition, the docket of both the state and federal courts is likely to grow until issues arising from digital harassment are effectively addressed. Courts, therefore, should modify the Faragher and Ellerth affirmative defense to protect employees in the digital workplace by creating a more efficient and effective legal framework to handle digital sexual harassment claims. Of course, this does not preclude legislative action. The courtroom does, however provide an obvious arena for this change, evidenced by the Court's keenness to address these issues in cases such as Meritor and Ellerth.

The current framework of the affirmative defense focuses on the employer’s corrective measures and the employees’ actions in avail-

91. See supra notes 48–51 and accompanying text.
94. The EEOC has 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.
95. See supra note 54 and accompanying text.
ing themselves of the corrective opportunities provided by the employer. As applied in the digital workplace, the affirmative defense is flawed in that it does not account for today's technology. Unlike the physical workplace, employers in the digital workplace have the ability to "know everything." In addition, employers in the digital realm can control digital communications to prevent sexual harassment. Such differences call for the Court to modify the affirmative defense in the digital workplace.

C. The Affirmative Defense in the Digital Workplace

The affirmative defense in the digital workplace should require companies to institute more than mere remedial policies in situations where the employer already utilizes a wide and complex array of e-snooping technology to monitor their employee transmissions.\textsuperscript{96} Because many employers have the ability to prevent digital sexual harassment accomplished through the use of e-mail, Internet, and desktop monitoring software, employers should be required to take such preventative measures.\textsuperscript{97}

The affirmative defense should be modified in two respects. First, the defense should focus on the employer's preventative measures, rather than corrective measures.\textsuperscript{98} Second, the defense should reduce (or eliminate) the employee's obligation to take advantage of preventative opportunities, as employees will often not be aware

\textsuperscript{96} While the affirmative defense is available to employer's 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 also is relevant in co-worker and third party sexual harassment. First, from the perspective of harassing conduct committed using digital technology, the employer can guard against the misbehavior of subordinate or common employee class just as easily as it can against supervisor class. It would thus appear inappropriate to uphold the two-tiered liability for these classes. Second, as noted above, in the context of co-worker or third party harassment, the employer is liable if it knew or should have known of the 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.

\textsuperscript{97} See discussion supra Part IIIA.


\textsuperscript{99} This is not to suggest that corrective measures will no longer be relevant. In some circumstances, the employer may have the ability to monitor digital communications without the ability to also block such communications. In these instances, the employer's prompt and effective action to address the conduct may demonstrate that it exercised due care.
of or have access to the monitoring and blocking software in order
to take advantage of it. 100

IV. A PROPOSED TEST ADDRESSING SEXUAL HARASSMENT IN
A HOSTILE DIGITAL WORKPLACE

The courts should permit the affirmative defense in the digital
workplace in a limited set of circumstances. The circumstances
should be determined by applying the Digital Workplace Defense
Test (DWDT).

Diagram I

DWDT Analysis

To determine an employer’s ability to invoke the affirmative de-
fense, the court must first examine the defendant’s technology
infrastructure to determine whether the defendant’s existing in-

100. Again, employee actions may nevertheless be relevant. If the employee fails to act
with reasonable care in taking advantage of other employer safeguards to either prevent
harassment that could have been avoided or notify the employer of harassment, the em-
ployer’s liability may be affected. In other words, while the employee will not have access to,
and often be unaware of, the employer’s monitoring and blocking software, the employee
still should be required to exercise due care in situations not involving an adverse or tangi-
ble employment action.
formation technology could have monitored and blocked the digital communications responsible for the sexual harassment claim. If the court ascertains that the defendant lacked the ability to monitor and block digital communications, the court should allow the defendant to plead the affirmative defense.

If, however, the court finds that the employer possessed monitoring and blocking capabilities, it then must examine whether or not the defendant took reasonable steps to monitor and block these digital communications. At this step, the defendant has the burden of proving that it employed reasonable efforts to block sexually harassing digital communications based on the capabilities and normal use of its information technology systems. If the defendant is unable to overcome this burden, the court should reject the defendant's affirmative defense. If, on the other hand, the defendant meets this burden by establishing that its use of blocking and monitoring technological systems was reasonable, the court should allow the defendant to plead the affirmative defense.

Under this analytical framework, the availability of the affirmative defense is contingent on the presence and use of technological systems that are capable of monitoring and blocking the responsible digital communication. By placing the burden on the defendant, the court properly holds employers responsible for the alleged hostile work environments that they control. This simply reflects the reality that, unlike in the physical workplace, in the digital workplace, preventive measures can eliminate harassment when the employer has blocking and monitoring technology.


102. The genesis for this Article came from Mr. Garrie'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.
A. Review of an Employer’s Technology Set

In performing the first step of the analysis, a court should examine whether the defendant’s technological infrastructure had the capability of blocking and monitoring the digital communications alleged in plaintiff’s action. In examining this, the court should explore various aspects of a defendant’s technological environment, including technological infrastructure and policies. When applicable, a court should address the following six issues.

First, a court should ask whether the defendant protects its valuable digital information such as financial data, customer records or sensitive intellectual property. In such situations, the court should be mindful that a defendant employer who protects its digital information would likely be monitoring its Web applications because early detection enables the defendant to prevent serious economic damage. For example, an employer in the media industry will protect its media by implementing both physical and digital technologies to ensure that employees do not make unauthorized copies of the media for pre-release. In this situation, the employer will likely be protecting the digital medium with some form of encryption and an access monitoring tool that will help prevent such a scenario from arising.

Second, the court should look to whether the defendant utilizes some form of real-time suspicious activity and policy violation detection technologies. Instant messaging systems in some financial institutions offer an example of an employer utilizing real-time tracking technology. Such employers implement messaging systems that have real-time logging capabilities, which, for example,


enable them to comply with the message storage requirements that are established under Sarbanes-Oxley. These systems provide the employer with the ability to track instant message conversations in real-time. When employers deploy such technology, the courts should examine whether the employer's inaction with respect to the digital workplace is reasonable respective to the monitoring technology being used. When such technology is being utilized the court should further explore the process and design of the system focusing on whether the defendant both monitors and blocks communications.

Third, the court should examine whether the defendant utilizes some form of user tracking. The "research trail" that is provided by Westlaw (a Web enabled legal research system) provides an example of this sort of tracking technology. This technology enables the employer to record the employee's actions with respect to a particular Web-based tool set. Again, when an employer utilizes such tracking devices, the court should ascertain whether the employer could have reasonably modified this monitoring and tracking technology to protect the digital workplace.

Fourth, the court should determine whether the defendant is monitoring its systems using real-time technology for suspicious user behavior. The monitoring technology that is triggered when a user's password is frozen is an example of such technology. 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. This type of monitoring technology is common in the financial sector to assist banks in preventing fraud or abuse of financial accounts.

Fifth, the court should review all of the defendant's recording systems. Such technology is relied upon heavily by financial and

---

110. See W. Michael Hoffman et al., 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).
115. See generally Simson L. Garfinkel, Privacy Matters, CIO MAG., June 1, 2000, at 178; II-Horn Hann et al., Online Information Privacy: Measuring the Cost-Benefit Trade-Off, INT'L CONF.
medical organizations. In these fields, having access to such data to enable computer forensic experts to construct an audit trail and deliver sufficient evidence of transactions is very important. Such technology is also commonly deployed in hospitals where the patient’s records must be protected; the hospital is often required to track and demonstrate that the digital records are released only to authorized parties.

Sixth, the court should determine whether the defendant utilizes a form of early end-user-management monitoring technology. Such technology monitors end-users from the end users’ location. For instance, global companies with worldwide customers use tools that enable them to monitor the location from where their customers communicate. Employers frequently use this technology when its employees are working off-site to ensure that its employees are performing the work as promised and the client is receiving authorized services.

Because companies utilize a unique blend of these elements, in addition to other forms of technology, these six points are intended only as guidelines for the courts. Regardless of the specific technology and its uses, these guidelines help the court focus on the degree of tracking, monitoring, and blocking technology that is utilized by the company.

When performing this analysis, courts should ensure that they are applying a reasonableness standard in evaluating the defendant’s technological blocking and monitoring capabilities. While “reasonableness” is a malleable concept, courts are nonetheless often required to use such a standard. This standard should be mindful of the associated costs, efforts, and the defendants’ knowl-
edge of their respective monitoring capabilities in their digital workplace. More precisely, a court should make a fact-specific inquiry, on a case-by-case basis, considering such factors as the size of the company, the number of employees, the ease and economy with which the system can be utilized/modified to monitor and prevent harassment, the employer’s knowledge of acts of harassment, and the volume of the digital transmissions the employer must track, as well as other factors. Finally, courts should use heightened awareness when reviewing defendants utilizing technology that complies with either the Sarbanes-Oxley Act, HIPAA, or other legislatively mandated tracking or monitoring requirements. In such cases, it is almost certain that monitoring and tracking technology is in place.

When the court finds that the necessary technological infrastructure is not in-place, it should permit the defendant to plead the affirmative defense as it currently operates. Here, the focus is appropriately on corrective measures and other types of preventative measures such as education and notice. The only exception would be when the plaintiff’s claim alleges and presents clear and overwhelming evidence that the defendant decided not to utilize blocking and monitoring technology to preserve the ability to use the affirmative defense for digital workplace harassment. For instance, if a plaintiff produces e-mails establishing that the defendant’s decision was driven by their desire to avoid losing the right to plead the affirmative defense, the courts 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 deliberately expose their employees to a hostile digital workplace. Upon finding that the defendant’s technological infrastructure was capable of both blocking and monitoring the alleged digital communications, the analysis resembles a cost/benefit analysis that examines the reasonableness of preventing harassment in the context of a particular employer’s technological capabilities and current use of such technology. For example, if an 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 impose liability or limit the employer’s ability to use an affirmative defense.

| 123. See supra note 115. |
| 124. See supra note 115. |
the court must then examine whether the defendant took reasonable steps to block or monitor the alleged digital communications.128

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

In the second step of this analytical framework, the court should utilize information previously gathered to assess the defendant's technological systems to determine whether the company took reasonable measures to block and monitor other digital communications unrelated to the sexually harassing communications. The court may find it useful to appoint an independent third-party, similar to the expert utilized in digital discovery disputes, to ascertain whether the defendant utilized its technology in a reasonable manner to protect the digital workplace.

As mentioned above, in assessing the reasonableness of an employer's conduct, the court must perform a fact-specific analysis on a case-by-case basis. A court should consider both fiscal costs and corporate policies when ascertaining whether the implementation of such technological systems would have been pragmatic.

V. Conclusion

Workplace sexual harassment and hostile work environments violate an individual's constitutional right not to suffer discrimination in the workplace. The Supreme Court, therefore, acted in both a socially responsible and ethical manner when recognizing hostile work environment harassment. Because employers are not clairvoyant and cannot control the actions of all of their employees, business associates, or customers, and cannot force them to utilize their preventive procedures, the Court adopted equitable principles in permitting employers to assert an affirmative defense. Today, courts have yet to fully appreciate or take into account an employer's ability to take reasonable preventive digital measures in protecting the digital workplace. This not only provides a disincentive for employers to utilize digital measures, but also is

128. See supra p. 90 and Diagram I: DWDT Analysis.
inconsistent with the congressional mandate to avoid harm rather than provide redress. Given the expansive monitoring by employers of employee digital communications, it is reasonable for the courts to require those same systems to monitor digital communications that are of a sexually harassing nature. The courts, therefore, should modify the affirmative defense. This will not only ensure protection of the digital and physical workplace for employees, but also create an efficient and effective legal framework to address digital sexual harassment claims.