2008

The Electronic Workplace: To Live Outside the Law You Must Be Honest

William A. Herbert

THE ELECTRONIC WORKPLACE: TO LIVE OUTSIDE THE LAW YOU MUST BE HONEST

BY
WILLIAM A. HERBERT*

I. INTRODUCTION

The use of new communication technologies in the performance of work continues to grow at an exponential pace, resulting in the creation of massive amounts of workplace electronic data. According to the United States Department of Labor's Bureau of Labor Statistics, in October 2003, 55.5 percent of all employees in the United States used a computer at work. Over three quarters of those employees utilized workplace computers to access the internet and to send and receive emails.[1] American employees spend approximately one quarter of their workday writing and reading email.[2] A Canadian study found that 60 percent of all employees engage in personal web

* Deputy Chair and Counsel for the New York State Public Employment Relations Board (PERB). The opinions expressed in this article are the personal views of Mr. Herbert and do not reflect the views of PERB. Many of the ideas and the analysis set forth in this article are an outgrowth of thought-provoking discussions with various individuals over the years: Douglas E. Dexter, Wayne Gold, H. David Kelly, Norma G. Meacham, Miguel Ortiz, and Amelia K. Tuminaro. The opinions expressed in this article, along with any mistakes and omissions, are exclusively my own.

1. *See* U.S. DEP'T OF LABOR, BUREAU OF LABOR STATISTICS, COMPUTER AND INTERNET USE AT WORK (2003) *available at* <http://www.bls.gov/news.release/ciuaw.t01.htm> (last visited Feb. 1, 2008).

2. DAVID SHIPLEY & WILL SCHWALBE, SEND: THE ESSENTIAL GUIDE TO EMAIL FOR OFFICE AND HOME 8 (2007).

surfing while at work.[3]

Employer concerns regarding employee productivity, along with fears associated with potential litigation and regulatory requirements such as the Sarbanes-Oxley Act of 2002, have led the vast majority of employers to issue computer use policies and utilize various means to monitor employee email, instant messaging, and internet surfing. Many employers have also installed filters to restrict employee access to particular websites.[4] In one study, more than 25 percent of the employers surveyed had terminated employees for misusing either email or the internet.[5]

Electronic technology has enabled the growing decentralization of the workplace, with some employees integrating their personal computer equipment with their employer's equipment. The advent of laptop computers and personal digital assistants (PDAs) provides increased flexibility with respect to work location and hours. Inherent in this technologically based decentralization is the blurring of the lines between the workplace and home and between work and rest.[6] For example, a 2007 poll found that 20 percent of those polled either worked or contacted their offices through laptops and cell phones while on vacation.[7]

The separate and unrelated legal efforts to compel former White House aide Karl Rove and New Jersey Governor Jon S. Corzine to release copies of email from private email accounts are indicative of the reality that business and personal communications are becoming integrated and also the subject of various demands for disclosure.[8]

3. Dave Chalk, Becoming *Big Brother at Work*, GLOBE & MAIL, July 21, 2006, *available at* <http://www.theglobeandmail.com/servlet/story/RTGAM.20060721.gtchalkjuly21/BNStory/Technology/einsider/> (last visited Feb. 1, 2008).

4. AMERICAN MANAGEMENT ASS'N, 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY: MANY COMPANIES MONITORING, RECORDING, VIDEOTAPING—AND FIRING—EMPLOYEES (2005), *available at* <http://www.amanet.org/press/amanews/ems05.htm> (last visited Feb. 1, 2008).

5. *Id*.

6. *See* BRUCE BARRY, SPEECHLESS: THE EROSION OF FREE EXPRESSION IN THE AMERICAN WORKPLACE 18 (2007); Katherine V.W. Stone, *Employee Representation in the Boundaryless Workplace*, 77 CHI.-KENT L. REV. 773, 816 (2002).

7. Alan Fram, *Poll: 1 in 5 Bring Laptop on Vacation to Stay in Touch,* SEATTLE POST - INTELLIGENCER, *available at* <http://seattlepi.nwsource.com/business/318231_vacationpoll02.html> (last visited Feb. 1, 2008).

8. Michael Abramowitz & Dan Eggen, *White House E-Mail Lost in Private Accounts*, WASH. POST, Apr. 12, 2007, at A4 *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2007/04/11/AR2007041102167.html> (last visited Feb. 1, 2008); Tom Hester Jr., *Government Battles to Keep Email Secret*, S.F. CHRON., March 16, 2008, *available at* <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/03/16/MN66VH9PB.DTL&hw=How+Government+Battles+to+Keep+Email+Secret&sn=001&sc=1000> (last visited July 15, 2008).

The emails sought from both Governor Corzine and Mr. Rove were sent and received from non-governmental email accounts, but the substance of the communications allegedly touched upon their official duties.

The electronic merger of work and recreation does not appear to be diminishing the subjective expectation of workplace computer users that they have a protected zone of personal privacy.[9] The integration of employer computers with personal electronic communication devices is creating complex legal issues regarding the balance between employee and employer rights and legal responsibilities.[10]

One core legal issue in both the private and public sectors is whether and under what circumstances an employee may have an enforceable expectation of privacy in email and websites visited. Another core issue is whether and to what extent the National Labor Relations Act (NLRA)[11] and similar public sector collective bargaining laws place limits on the lawful scope of employer computer use policies and practices. An additional issue is whether and under what circumstances an employer may have a legal duty to monitor an employee's workplace computer activities to avoid harm to a third-party.[12]

A three-year old study by the American Management Association and the ePolicy Institute found that 20.1 percent of employers have been ordered by a court or administrative agency to produce copies of employee emails.[13] The probative value of email to factual disputes in litigation has resulted in a massive increase in e-discovery demands. Electronic communications have the potential to reveal direct evidence relating to the motivation behind an employment decision or provide the proverbial "smoking gun." With lawyers and litigants sifting through the digital haystack of stored

9. Elaine Ki Jin Kim, *The New Electronic Discovery Rules: A Place For Employee Privacy*, 115 YALE L.J. 1481, 1485 (2006).

10. H. Christopher Boehning & Daniel J. Toal, *Electronic Discovery: Lines Blur between Business, Personal Data*, N.Y. L.J., Aug. 28, 2007, at 5.

11. 29 U.S.C. §§ 151-69 (2000).

12. *See* Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005) (holding that a complaint by a third-party stated a cause of action in tort against an employer when the complaint alleged that the third-party was harmed as the direct result of the employer failing to properly supervise an employee by investigating the employee's downloading of child pornography at work).

13. AMERICAN MANAGEMENT ASS'N & THE EPOLICY INSTITUTE, 2004 WORKPLACE E-MAIL AND INSTANT MESSAGING SURVEY SUMMARY, *available at* <http://www.epolicy institute.com/survey/index.html> (last visited Feb. 1, 2008).

electronic documents, it is inevitable that employee private communications will be examined and possibly utilized by parties in litigation.

The recent e-discovery amendments to the Federal Rules of Civil Procedure increase the probability that employee email will be the subject of regular if not uniform discovery demands in labor and employment litigation. A 2007 survey of small litigation firms by the American Bar Association's Legal Technology Resource Center found a steep rise over the past year in the number of firms that have made e-discovery demands.[14] Although the federal civil procedure e-discovery rules focus on critical questions such as cost allocation and privileged communications, they do not provide any explicit protections for the privacy interests of individual employees.[15] At least one commentator has argued that federal judges can aid in enhancing employee electronic privacy by considering privacy as a factor in applying the e-discovery standards.[16]

Practical problems associated with email use include excessive use, miscommunication, arguments, and disruptions. As a result, some individuals are deciding to go on an email diet.[17] New Jersey Governor Corzine's announcement of his intention to discontinue utilizing email, in response to litigation seeking to force the release of his private emails, may be emblematic of a new trend toward a more moderate use of electronic communications.[18]

To compound the problems associated with email overuse, studies are beginning to suggest the potential for electronic addiction that is leading some users to reexamine their behavior.[19] In July 2007,

14. Catherine Sanders Reach, *ABA Poll Shows Increase in Tech Use*, N.Y. L.J., Nov. 20, 2007, at 5.

15. *See generally* Cameron G. Shilling*, Electronic Discovery: Litigation Crashes into the Digital Age*, 22 LAB. LAW. 207 (2006).

16. Kim, *supra* note 9, at 1486-88.

17. Jennifer Saranow, *How Email Junkies Do in Withdrawal*, WALL ST. J.,, Feb. 14, 2007, at A1; Mike Musgrove, *E-Mail Reply to All: 'Leave Me Alone'*, WASH. POST, May 25, 2007, at A01, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2007/05/24/AR2007052402258.html> (last visited Feb. 1, 2008). The growing problems associated with the overuse of electronic communication devices have led various prominent technology companies to form an organization, the Information Overload Research Group, to examine various technological and cultural means of responding to these problems. Matt Richel, *Lost in E-Mail*, *Tech Firms Face Self-Made Beast*, N.Y TIMES, June 14, 2008, at 1. The organization's website includes links to research materials on email overuse, as well as, the distractions and interruptions caused by information technology. <http://www.iorgforum.org/> (last viewed June 22, 2008).

18. David W. Chen, *Facing a Lawsuit, Corzine Swears Off E-Mail*, N.Y. TIMES, July 12, 2007, at B1, *available at* <http://www.nytimes.com/2007/07/12/nyregion/12corzine.html?ex=1341892800&en=fd62e6a233981236&ei=5088&partner=rssnyt&emc=rss> (last visited Feb. 1, 2008).

19. *See* Matt Richtel, *It Don't Mean a Thing if You Ain't Got That Ping*, N.Y. TIMES, Apr.

Time Warner/AOL issued a press release entitled "Think You Might Be Addicted to Email? You're Not Alone," which set forth the findings from AOL's third annual survey regarding email addiction and suggested means of responding to the addiction.[20]

The recent publication of *Send: The Essential Guide to Email for Office and Home* is indicative that electronic communications have begun to overwhelm both the work environment and home life.[21] The authors of the book identify various benefits of email: it is an efficient and economical means of communication that enables the forwarding of electronic documents worldwide. Further, email permits the inclusion of earlier emails, as well as the automatic retention of sent and received emails.[22] At the same time, the authors articulate eight reasons for deciding not to utilize email including two factors that touch upon electronic privacy. Emails can be forwarded to unintended recipients and the automatic retention of electronic communications eliminates even the possibility of plausible deniability.[23]

There are other legal complications that can arise from the use of email in litigation and the workplace. In 2005, a California employment attorney learned firsthand the pitfalls connected with failing to check his email. After filing a lawsuit on behalf of a client in federal court, a District Court judge issued an order to show cause scheduling a hearing on why the lawsuit should not be dismissed.[24] The order was sent to the parties via email rather than regular mail. Plaintiff's counsel did not become aware of the order or the hearing until after the lawsuit was dismissed, because he did not check his email

22, 2007, at 5; Jean Chatzky, *Confessions of an E-mail Addict*, MONEY, Mar. 1, 2007, at 28, *available at* <http://money.cnn.com/2007/02/22/magazines/moneymag/chatzky.moneymag/index.htm> (last visited Feb. 1, 2008).

20. Times Warner, Press Release, Think You Might Be Addicted to E-mail? You're Not Alone (July 26, 2007), *available at* <http://www.timewarner.com/corp/newsroom/pr/0,20812,1647308,00.html> (last visited Feb. 1, 2008). The proactive steps taken by Time Warner/AOL are prudent in light of the growing concerns relating to the potential for electronic addiction. In a 2008 editorial in the *American Journal of Psychiatry*, a doctor has proposed adding internet addiction as a recognized mental disorder in the future *Diagnostic and Statistical Manual of Mental Disorders (DSM) V* that is being developed by the American Psychiatric Association. The editorial makes a reference to statistics stemming from a South Korean study on the topic. Jerald J. Block, M.D., *Issues for DSM-V: Internet Addiction*, 165 AM. J. PSYCHIATRY 306 (2008), *available at*: <http://ajp.psychiatryonline.org/cgi/content/full/165/3/306?eaf> (last visited June 23, 2008).

21. SHIPLEY & SCHWALBE, *supra* note 2.

22. *Id.* at 17-20.

23. *Id*. at 22-29.

24. Calderon v. Int'l Bhd. Elec. Workers, 508 F.3d 883, 883 (9th Cir. 2007).

regularly.[25] After a motion to vacate the default was denied, an appeal to the Ninth Circuit Court of Appeals resulted in a decision reinstating the lawsuit because the District Court rules at the time did not authorize the use of email for service.[26] In addition, the decision contained an unusual apology to the parties and an admonishment to the District Court judge.[27]

Reliance on email by an employer as a means to communicate workplace policies or to announce bad news such as layoffs can be ineffective. General Dynamics learned this lesson. In 2001, General Dynamics distributed a mass email to its employees aimed at establishing a new workplace agreement under Federal Arbitration Act,[28] which was intended to constitute a waiver by the employees of their statutory right to pursue discrimination claims in federal and state court.[29] The email included a link to the employer's new policy but did not require a response, and the company chose not to monitor whether employees accessed the linked policy.[30] A few years later when General Dynamics attempted to enforce the "agreement" by requiring a terminated employee to arbitrate an employment discrimination claim, the First Circuit Court of Appeals held that the distribution of the company's email message was insufficient to establish a binding agreement waiving the employee's statutory right to pursue his claim in court.[31]

In contrast, a Georgia company's imposition of a similar mandatory arbitration procedure on its employees was found to be an enforceable agreement because it was distributed to the employees via email, regular mail, the intranet, and through a posting.[32] In addition, the company's letter explicitly stated that the new mandatory arbitration procedure constituted a condition of continued employment.[33]

In 2002, Seventh Circuit Court of Appeals Judge Richard Posner,

25. *Id.* at 883-84.

26. *Id.* at 884.

27. *Id.* Nevertheless, the Ninth Circuit underscored that "[w]hen the rules change, so as to make electronic notice sufficient, counsel will then be on notice that they need to check their emails just as carefully as they now check their regular mail."

28. 9 U.S.C. §§ 1-16 (2000).

29. Campbell v. Gen. Dynamics Gov't Sys. Corp., 407 F.3d 546, 547-48 (1st Cir. 2005).

30. *Id.* at 548-49.

31. *Id.* at 555-56.

32. Caley v. Gulfstream Aerospace Corp, 428 F.3d 1359 (11th Cir. 2005).

33. *Id.* at 1374-75. The Eleventh Circuit distinguished the holding in *Campbell* factually and legally, based on Georgia law. *Id.* at 1375 n.18.

in *Muick v. Glenayre Electronics*,[34] summarized employer fears underlying workplace computer use policies and analyzed those policies under common law principles. Judge Posner stated that the employer's laptops were its property and that

> it could attach whatever conditions to their use it wanted to. They didn't have to be reasonable conditions but the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.[35]

Although such *dicta* may constitute an overly broad legal view with respect to employer rights, it does help frame the issues connected with the respective rights of employers and employees in the electronic workplace.

In many ways, United States labor and employment law sleep-walked into cyberspace. Although there is wide societal recognition that new technologies are leading to the diminishment of personal privacy, there has not been an equal demand for changes in the legal paradigm.[36] The growth of electronic communications has coincided with the hegemony of deregulation ideology over the past thirty years.[37] During this period, there has not been a frank and open public dialogue relating to national labor law policy or the role of collective bargaining.[38] As a result, there has been very little legislative or administrative movement on the federal or state level aimed at creating a balanced approach to the respective interests of employers and employees regarding the use of workplace computer systems.[39] As rapidly as technology has overtaken the workplace, American labor law, along with workplace property, contracts, and privacy law,

34. 280 F.3d 741(7th Cir. 2002).

35. *Id.* at 743.

36. Some United States Supreme Court justices who are frequently labeled as conservative have articulated concerns relating to the adverse impact new technologies are having on privacy. *See*, *e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 541 (2001) (Rehnquist, C.J., dissenting). Judicial recognition of the growing diminishment of protected privacy, however, has not led to a large body of court decisions evaluating electronic privacy issues with contemporary lenses. *Cf.* Kyllo v. US, 533 U.S. 27 (2001).

37. SHIPLEY & SCHWALBE, *supra* note 2, at 8, 20-22.

38. Wilma B. Liebman, *Decline and Disenchantment: Reflections on the Aging of the National Labor Relations Board*, 28 BERKELEY J. EMP. & LAB. LAW 569, 589 (2007).

39. At the same time, Congress has enacted laws criminalizing certain activities on the internet, such as the distribution of child pornography. *See* Child Pornography Prevention Act, 18 U.S.C. § 2252A (2000). As will be seen, *infra* Part III, the vast majority of cases in the past decade regarding electronic workplace privacy involving the internet stem from cases involving federal prosecutions for the downloading of pornography at work.

remains virtually unchanged.

Although economic pressures are beginning to compel calls for more governmental regulation in areas such as food and toy safety, it remains to be seen whether a similar reevaluation of legal principles and analysis will take place in the field of labor and employment law in response to the development of the electronic workplace.[40] Without legislative or administrative study, discernment, and regulation in the area, it is probable that the legal framework regarding workplace electronic communications will continue to be developed through *post hoc* court and administrative decisions in the context of the Fourth Amendment to the United States Constitution,[41] common law, the Electronic Privacy Communications Act of 1986 (ECPA),[42] and the NLRA.

As will be seen below, almost ten years ago, the Office of General Counsel of the National Labor Relations Board (NLRB General Counsel) began to articulate an important new legal concept of a "virtual workplace" under the NLRA, which prohibited overbroad non-solicitation computer use policies where email is the primary means of communication between employees.[43] Under this legal theory, the rights granted employees under the NLRA would limit the common law managerial rights of employers when it comes to employee use of workplace computers or systems during non-work periods. This legally creative administrative effort to adapt the NLRA to the electronic workplace was substantially rejected by a majority of the National Labor Relations Board (Board) in its recent decision in *Guard Publishing Company d/b/a The Register-Guard*.[44] The content and scope of the Board majority's decision led the dissent to describe the NLRB as an administrative Rip Van Winkle which has "been asleep for the past 20 years" during the technological metamorphosis

40. Jane Zhang, *Food Makers Get Appetite for Regulation,* WALL ST. J., Sept. 17, 2007, at A2; Eric Lipton & Louise Story, *Toy Makers Seek Standards For U.S. Safety*, N.Y. TIMES, Sept. 7, 2007, at C1.

41. The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV.

42. Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 1367, 2510-21, 2701-11, 3117, 3121-27 (2000)).

43. NLRB Gen. Couns. Adv. Mem. (Pratt & Whitney) 12-CA-18446, 18772, 18745 & 18863 (Feb. 23, 1998), *available at* <http://www.nlrb.gov/index.aspx> (under Research tab, and under Memos on the drop down menu, select Advice Memos link from the Memos menu, select the year 1998 and click Go to browse, scroll down the alphabetical list and select Pratt & Whitney).

44. 351 N.L.R.B. No. 70 (Dec. 16, 2007).

of the workplace.[45]

Despite employee perceptions to the contrary, interpretations of constitutional, common law, and statutory provisions establish only minimal employee rights relating to email and internet use in the workplace. In light of this gap between perception and legal reality, "it is time the American people had an open and honest debate on the relative importance of privacy and security."[46] Without a reasoned and nuanced debate and discussion in legislatures, in the public square, and in the office, employee workplace computer use will continue to live outside the scope of legal protections.

This article will examine various legal issues relating to the use of computer-based electronic technologies in the workplace. Specifically, the article will discuss employee internet and email use at work under the Fourth Amendment, common law torts,[47] the ECPA, and the NLRA.

The article begins with a discussion of the 1987 United States Supreme Court plurality decision in *O'Connor v. Ortega,*[48] which sets the judicial framework for analyzing the scope of employee privacy protections in the electronic workplace in the public sector under the Fourth Amendment and highlights a central role played by workplace computer policies and practices in limiting an enforceable expectation of privacy.

After analyzing *O'Connor*, the article discusses federal and state laws relating to employer computer monitoring. It then reviews in Section III the legal implications of employee internet access in the workplace, focusing on the growing body of appellate precedent in the area of workplace computer privacy under the Fourth Amendment. Part IV considers the legal issues that have arisen in connection with workplace email and compares United States precedent to a 2007 decision by the European Court of Human Rights. In the final part, this article analyzes the impact of the recent Board decision in *Register-Guard*,[49] on efforts to reinterpret the NLRA to render it relevant to the contemporary workplace. The article concludes with a call for integrity-based solutions, including legal changes and employer policies that balance employer interests

45. *Id.* at 12.

46. David B. Rivkin, Jr. & Lee A. Casey, *Surveillance Showdown*, WALL ST. J., Sept. 24, 2007, at A19.

47. *See* RESTATEMENT (SECOND) OF TORTS §§ 317, 652B (1977).

48. 480 U.S. 709 (1987).

49. 351 N.L.R.B. No. 70 (Dec. 16, 2007).

and employee privacy rights, thereby encouraging the most beneficial use of technology without sacrificing important zones of privacy in our society.

II. THE LEGAL FRAMEWORK FOR WORKPLACE PRIVACY

In *O'Connor*, the Supreme Court was called upon to determine the applicability of the Fourth Amendment to a California public hospital's extensive investigatory search of a physician's office while he was on administrative leave.[50] The investigation included the search and seizure of the employee's personal items that were in his desk and file cabinets that he did not share with any other employee.[51]

The *O'Connor* plurality determined that the applicable test for determining whether the Fourth Amendment is implicated by a public employer's search of a workplace is whether the employee had a reasonable expectation of privacy. In so holding, the Court rejected the argument by the Solicitor General and the State of California that, as a matter of law, public employees cannot have a reasonable expectation of privacy in their workplace.[52] The reasonable expectation of privacy standard stems from the concurrence by Justice John M. Harlan in *Katz v. United States*,[53] in which he described the applicable test in the following manner:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person [has] exhibited an actual (subjective) expectation of privacy and second, that the expectation be one that society is prepared to recognize as "reasonable."[54]

The reasonable expectation of privacy test is equally applicable when courts examine whether a government search of a private

50. *O'Connor*, 480 U.S. at 712-13.

51. *Id.* at 713, 718.

52. *Id.* at 717. In contrast, in *Garcetti v. Cebbalos*, 547 US 410 (2006), the Court adopted an absolute rule that speech by a non-academic public employee while performing his or her employment duties is unprotected under the First Amendment. It remains to be seen whether the *Garcetti* strict employee/citizen dichotomy will be extended to Fourth Amendment analysis in future cases involving electronic privacy in public employment. *See generally* Sheldon H. Nahmod, *Public Employee Speech, Categorical Balancing and § 1983*: *A Critique of* Garcetti v. Ceballos, 42 U. RICH. L.REV. 561 (2008); Paul M. Secunda, *Reflections on the Technicolor Right of Association in American Labor and Employment Law*, 96 KY. L.J. 343 (2008). However, based on the distinct interests protected by the respective amendments, as well as the legal principles applied to each, a strong argument can be made that a public employee's "papers, and effects" inside an employee's office and computer are subject to certain Fourth Amendment protections against an unreasonable search and seizure.

53. 389 U.S. 347 (1967).

54. *Id.* at 361.

workplace violated an employee's Fourth Amendment rights. In 1968 in *Mancusi v. DeForte*,[55] the Supreme Court concluded that an employee working in a labor union's headquarters had a reasonable expectation of privacy with respect to papers kept in an office, even though the office was shared with co-workers and accessible to others.[56]

Under *O'Connor*, whether an expectation of privacy in the workplace will be deemed reasonable and therefore enforceable under the Fourth Amendment will depend on a case-by-case analysis of the actual office practices and procedures and may be further reduced by legitimate employer regulation.[57] In conflict with the conclusion in *Mancusi,* the *O'Connor* plurality found that among the workplace practices that can render an expectation of privacy unreasonable is the accessibility of the area in question to co-workers or others.[58]

In other words, an enforceable expectation of privacy will not be found under *O'Connor* in situations where co-workers or the employer regularly access an office, desk, cabinet, or locker. If an employee wishes to maintain an enforceable privacy interest in the workplace, he or she will have to take affirmative steps, such as using a lock on a desk or locker. Although *O'Connor* did not involve the search of a workplace computer, the articulated principles indicate that with certain affirmative steps, such as the use of a personal password to deny access to the computer, files and/or folders by others, an employee may retain an enforceable zone of computer privacy.

Another means of eliminating an enforceable expectation of privacy under *O'Connor* is through an employer policy or regulation.

55. 392 U.S. 364 (1968).

56. *Id.* at 369-70.

57. *O'Connor*, 480 U.S. at 717.

58. It is notable that Justice Scalia, in his concurrence in *O'Connor,* rejected the plurality's conclusion that co-worker accessibility can form the basis for concluding that another employee lacked Fourth Amendment protections:

> It is privacy that is protected by the Fourth Amendment, not solitude. A man enjoys Fourth Amendment protection in his home, for example, even though his wife and children have the run of the place – and indeed, even though his landlord has the right to conduct unannounced inspections at any time. Similarly, in my view, one's personal office is constitutionally protected against warrantless intrusions by the police, even though employer and co-workers are not excluded.

Id. at 730.

In concluding that the employee had a reasonable expectation of privacy, the *O'Connor* plurality noted:

> that there was no evidence that the Hospital had established a reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desk or file cabinets . . . although the absence of such a policy does not create an expectation of privacy where it would not otherwise exist.[59]

After determining that the employee had a reasonable expectation of privacy, the *O'Connor* plurality proceeded to determine whether a public employer was obligated to obtain a warrant prior to conducting a workplace search, as well as the appropriate standard for determining whether the search was reasonable under the Fourth Amendment. Based on what it described as public sector workplace realities that require supervisors and co-workers to enter workspaces to complete their tasks, the Court concluded that the Fourth Amendment did not require a public employer to obtain a search warrant prior to conducting a workplace search or seizure.[60] Similarly, based on the obligation of public employers to provide efficient and effective governmental services, the plurality found that probable cause was an inappropriate standard by which to judge workplace searches because "public employers must be given wide latitude to enter employee offices for work-related, non-investigatory reasons."[61] Instead, the plurality set forth a "reasonableness under all circumstances" test for determining whether a public employer's actions constituted an unreasonable search under the Fourth Amendment.[62]

One of the central principles stemming from *O'Connor* is that an effective means for an employer to diminish, if not eliminate, an enforceable expectation of privacy in the workplace is through the implementation and circulation of an explicit computer use policy informing employees that all computer use will be monitored and accessed by the employer and that such use will not be considered confidential.[63] In addition, automatic screen warnings, upon logging in, can help to ensure that an employee's subjective expectation of

59. *Id.* at 719.

60. *Id.* at 719-21.

61. *Id.* at 723.

62. *Id.* at 725.

63. *See* U.S. v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007); U.S. v. Angevine, 281 F.3d 1130, 1134-35 (10th Cir. 2002); U.S. v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); Kelleher v. City of Reading, Civ. Action No. 01-3386, 2002 U.S. Dist. LEXIS 9408 (E.D. Pa. May 29, 2002); Doe v. XYC Corp., 887 A.2d 1156, 1166 (N.J. Super. Ct. App. Div. 2005).

privacy will be found unreasonable by a court.[64]

In 1986, Congress enacted the ECPA, the most significant federal legislation relevant to the electronic workplace. The statute provides another strong legal incentive for employers to codify and circulate computer use policies to meet one of the statutory exemptions and thereby avoid liability. The ECPA contains two distinct titles: Title I contains prohibitions against the "interception" of electronic communications;[65] Title II, the Stored Communications Act, limits the accessibility to electronically stored communications.[66] Both titles include a consent exception applicable to the workplace.[67] An employer can avoid liability under either title by unilaterally imposing, as a term and condition of employment, a broad computer use policy reserving to the employer the right to intercept, monitor, and access emails and other files contained on a workplace computer.[68]

At least two states, Delaware and Connecticut, have enacted legislation regulating employer monitoring of employee email and internet access.[69] Both statutes compel employers to provide additional notice to employees prior to any monitoring to avoid modest fines.

64. *See* U.S. v. Greiner, 235 Fed. Appx. 541 (9th Cir. 2007).

65. Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 1367, 2510-21, 2701-11, 3117, 3121-27 (2000)). Section 2510(4) defines the term "intercept" to mean the intentional "aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." In order to satisfy the definition, the electronic communication must be acquired during transmission. *See* U.S. v. Steiger, 318 F.3d 1039, 1047-50 (11th Cir. 2003); Fraser v. Nationwide Mut. Ins. Co., 352 F. 3d 107, 113-14 (3d Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).

66. 18 U.S.C. §§ 2701-11 (2000). In *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008), the Ninth Circuit ruled that a company providing contractual pager services to a California municipality violated the SCA when the company provided the city with transcripts of text messages to and from a police officer without obtaining his individual consent. The company released the transcripts at the city's request as part of the city's investigation into the police officer's overuse of text messaging. At the time, the city lacked an official text message policy which stated that the city would be monitoring and auditing the content of text messages. Rather, under the city's unofficial policy, the content of text messages were not monitored or audited.

67. 18 U.S.C. §§ 2511(2)(d), 2701(c)(2) (2000).

68. *See* Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993); Griggs-Ryan v. Smith, 980 F.2d 112 (1st Cir. 1990); Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); Watkins v. L. M. Berry & Co., 704 F.2d 577 (11th Cir. 1983); George v. Carusone, 849 F. Supp. 159 (D. Conn. 1994). In *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996), the court held that an employer could, without violating ECPA Title II, retrieve pager text messages stored on its computer system because the employer "is the 'provider' of the 'electronic communications service' at issue here" and "service providers [may] do as they wish when it comes to accessing communications in electronic storage."

69. DEL. CODE ANN. tit. 19, § 705 (2007); CONN. GEN. STAT. § 31-48d (2007).

Under the Delaware statute, employers are prohibited from engaging in any monitoring or interception unless the employer either provides a daily electronic notice that employee email and internet use is subject to monitoring or interception or has obtained signed employee acknowledgement of the receipt of the employer's computer monitoring policy.[70] In Connecticut, employers, in general, are obligated to provide notice prior to engaging in computer use monitoring. The statute contains broad exceptions including permitting monitoring without notice when the employer has reasonable grounds to believe that an employee is engaging in conduct that violates the law, workplace rules, or the rights of the employer or co-workers, or creates a hostile work environment.[71]

The introduction of a computer use policy in the workplace can form an important evidentiary foundation for an employer's effort to terminate or otherwise discipline an employee who has statutory or contractual tenure protections or is subject to a just cause provision of a collective bargaining agreement.[72] At the same time, an employer policy or practice that explicitly permits employee private email communications, including a system for distinguishing between public and private emails, can form the basis for an enforceable expectation of privacy.[73]

As will be seen in Part V, the NLRA has the potential to constitute the primary statutory limitation on a private employer imposing and applying a computer use policy in a workplace. For example, an employer may have a statutory obligation to negotiate with an incumbent union the terms of a computer use policy. Despite the United States Supreme Court's recognition that the Board must reappraise employee rights under the NLRA in response to technological workplace advances, however, various recent Board decisions demonstrate an unwillingness to adopt a modern approach to the NLRA in response to the massive expansion of workplace email and internet use.[74]

70. DEL. CODE ANN. tit. 19 § 705(b)(2) (2007).

71. CONN. GEN. STAT. § 31-48d (2007).

72. *See*, *e.g.*, Wagner v. Roth, 780 N.Y.S.2d 42 (N.Y. App. Div. 3d Dep't 2004) (termination of a state manager for using employer's computer to send sexually explicit email and visiting offensive websites was upheld based on the fact that the employee was on notice of the computer use policy).

73. U.S. v. Heckenkamp, 482 F.3d 1142, 1145 (9th Cir. 2007); Haynes v. Office of the Attorney Gen., 298 F. Supp. 1154, 1162 (D. Kan. 2003).

74. NLRB v. J. Weingarten, Inc., 420 U.S. 251, 265 n.10, 266 (1975); *see*, *e.g.*, Guard Pub. Co. d/b/a The Register-Guard, 351 N.L.R.B. No. 70 (Dec. 16, 2007); Trs. of Columbia Univ., 350

III. INTERNET WANDERING @ WORK

Prior to discussing the legal issues associated with email, this article turns to the legal implications of workplace computer policies relating to accessing the internet. Unlike the contemporary importance of email in most workplaces, extensive access to the internet is rarely integral to most jobs. Despite this fact, some employers have chosen to grant all or most employees complete access to the internet. Based on the web's ability to deliver a greater amount of information and entertainment than cable television and radio combined, it is predictable that internet access can lead inevitably to web wandering during the workday.

Like other benefits at work, internet access can easily be misused by even the most productive employees. The technological construct of internet access and use renders it a natural and powerful distractive magnet away from work duties. For an unproductive employee, the grant of incidental personal internet access can be a policy that will lead to additional problems for both the employee and employer. In such situations, the computer screen can constitute a modern day wall for a contemporary Bartleby to stare at instead of performing assigned work tasks that he or she would prefer not to do.[75]

Determining when and how to draw the line in workplace policies and practices regarding internet use can be difficult. Once internet access has been broadly granted, a decision to eliminate such access can result in workplace demoralization. Nevertheless, computer use policies, along with firewalls, filters, and other software, can play an important role in limiting unproductive internet use and quicken the discovery of employee misconduct. For example, New Hampshire expanded the installation of internet filters in computers in smaller state agencies to block employee access to websites for shopping, gambling, and pornography.[76] Prior to activating the filters, an individualized internet inventory was conducted through current monitoring to determine which internet sites an employee needs to perform his or her duties.[77]

N.L.R.B. No. 54 (Aug. 9, 2007); Amcast Automotive of Ind., 348 N.L.R.B. No. 47 (Sept. 29, 2006).

75. HERMAN MELVILLE, BARTLEBY, THE SCRIVENER: A STORY OF WALL STREET (Hesperus Classics 2007) (1853).

76. Lauren R. Dorgan, *State Limits Web for Employees*, CONCORD MONITOR, Aug. 27, 2007, *available at* <www.concordmonitor.com/apps/pbcs.dll/article?AID=/20070827/FRONTPAGE/708270314>.

77. *Id.*

It is telling that most judicial decisions examining the legal rights associated with employee access to the internet are in the context of criminal prosecutions for the downloading of child pornographic images in the workplace. The growing number of appellate decisions analyzing workplace computer privacy in the context of child pornography prosecutions stems from the concerted federal prosecutorial effort to respond to the increased distribution of such images via the internet.[78] According to one study, over two-thirds of all pornography downloads take place during the workday.[79]

Except in the most extreme cases, it is improbable that employment litigation and disputes will arise from employees accessing news, financial, or sports websites on an intermittent basis. It is more likely that the development and application of legal principles surrounding employee access to the internet will continue to take place in the context of unlawful employee misconduct. This reality provides little hope that the judiciary will be developing a nuanced legal balance between the interests of employers and employees regarding access to the internet at work.

A workplace policy stating that the employer will access and monitor all internet activities on its computer network eliminates, in virtually all cases, a legally enforceable employee expectation of privacy in the websites visited and images viewed. Policies permitting remote monitoring of all computers integrated into an employer's system may enable employers to monitor lawfully an employee's internet activities while at home using a personal computer or laptop that is integrated into the employer's system. It is doubtful that most employers will explicitly reserve such a right in their policies or actually engage in such monitoring. Nevertheless, fear of litigation, regulatory requirements, and concerns regarding employee misconduct may compel some employers to expressly include remote monitoring of integrated personal computers in their computer use policies. Precedent being developed in the area of child pornography and other internet related criminal activities may form the legal framework in future cases for courts to uphold monitoring of employee computer activities outside of the workplace if the

78. Jerry Markon, *Crackdown on Child Pornography*, WASH POST, Dec. 15, 2007, at A1, *available at* <http://www.washingtonpost.com/wp-dyn/content/article/2007/12/14/AR2007121402257.html>.

79. Dave Chalk, *Becoming Big Brother at Work*, THE GLOBE & MAIL, July 21, 2006, *available at* <http://www.theglobeandmail.com/servlet/story/RTGAM.20060721.gtchalkjuly21/BNStory/Technology/einsider/>.

computer policy gives proper notice.

In the past two years, the Ninth Circuit Court of Appeals has issued three decisions examining the legality of the search of Montana employee Jeffrey Ziegler's workplace computer.[80] In 2001, Ziegler was employed by a Montana company that provides services relating to the internet.[81] The company had in place a firewall on its computer system enabling it to block employee access to inappropriate websites. In addition, the company had a clear computer use policy prohibiting personal use of the workplace computer and provided training to employees regarding the company practice of monitoring internet use.[82]

Following a tip from co-workers, the FBI commenced an investigation regarding a company employee who was downloading child pornography on the company's computer. After contact from the FBI, the employer's internet administrator conducted remote monitoring of Ziegler's computer and concluded that Ziegler was the employee downloading the obscene images. In addition, the company began to monitor Ziegler's internet use by copying Ziegler's office computer's cache files, resulting in the discovery of additional pornographic images.[83] Following a conversation between the FBI agent and company representatives, company employees entered Ziegler's locked private office and made two copies of his office computer's hard drive. Thereafter, the company voluntarily turned over the hard drives to the FBI without issuance of a search warrant.[84] Two years later, Ziegler was indicted for the possession of child pornography.[85] Ziegler appealed the denial of his motion to suppress the images on Fourth Amendment grounds to the Ninth Circuit.[86]

In 2006, the Ninth Circuit issued its initial decision affirming the denial of the suppression motion on the ground that he lacked a reasonable expectation of privacy regarding the content of his workplace computer's hard drive.[87] In support of its decision, the Ninth Circuit panel noted that the computer was company owned and the company had a policy and practice of monitoring internet access

80. *See* U.S. v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).
81. *Id.* at 1185-86.
82. *Id.* at 1191-92.
83. *Id*. at 1185-86.
84. *Id.* at 1186-87.
85. *Id.* at 1187 n.5.
86. *Id.* at 1188.
87. 456 F.3d 1138 (9th Cir. 2006), *superseded by* 474 F.3d 1184 (2007).

and prohibiting the use of the computer for personal purposes.[88] Although the employer's ownership of the computer was a factor in its decision, the panel emphasized in a footnote that the property interest must be combined with other factors to defeat a reasonable expectation of privacy.[89]

In response to Ziegler's petition for a panel rehearing, in January 2007, the Ninth Circuit panel withdrew its earlier decision and issued a new decision concluding that Ziegler had a reasonable expectation of privacy in his office and its contents, based on the holding in *Mancusi v. DeForte*.[90] The factors that formed the basis for the new determination were that Ziegler kept his office locked and that he did not share it with co-workers.[91] Nevertheless, the circuit panel again affirmed the district court's conclusion that Ziegler's Fourth Amendment rights had not been violated by the search because his employer legally consented to the search of the hard drive which remained in its control. In reaching its holding on the employer's lawful consent, the panel cited to the exact same factors that it had relied upon in the earlier decision as to whether he had an enforceable expectation of privacy: the employer's regular monitoring of employee internet use; employee computer training; and an employee manual placing employees on notice that office computers were owned by the employer and subject to monitoring through remote electronic access.[92]

Thereafter, a *sua sponte* call for a rehearing *en banc* by a Ninth Circuit judge was denied.[93] Judges Fletcher and Kozinski issued dissents from the denial of the rehearing, questioning the soundness of the panel's conclusion that the employer's computer use policy gave the employer the authority to consent to the search of Ziegler's office and computer.[94]

88. 456 F.3d at 1146.

89. *Id.* at 1146 n.11. In contrast to Fourth Amendment cases like *Ziegler*, where courts have found that an employer's property interest in a computer system is only one factor in determining whether an employee has an enforceable privacy interest, the Board in *Register-Guard* recently found that employer ownership of the computer is sufficient to substantially negate the applicability of the NLRA to employee email communications. *See infra* Part V.

90. *Ziegler*, 474 F.3d 1184, 1185, 1189-90 (9th Cir. 2007).

91. *Id.* at 1189-90.

92. 474 F. 3d at 1191-92.

93. 497 F.3d 890 (9th Cir. 2007).

94. *Id.*; *see also* U.S. v. Greiner, 235 Fed. Appx. 541, 542 (9th Cir. 2007) ("[t]hrough acquiescence in his employer's established computer-use policy, Greiner had consented that his employer might permit his office, and the workplace computer within that office, to be searched."); *cf.* Trulock v. Freeh, 275 F.3d 391 (4th Cir. 2001) (consent to search an individual's

In *United States v. Heckenkamp*,[95] the Ninth Circuit determined the scope of privacy protections relating to personal computers connected to a network system. In that case, the court held that a University of Wisconsin student had an objectively reasonable expectation of privacy with respect to his personal computer situated in his dormitory room even though the computer was connected to the university's network system.[96] In reaching its conclusion, the panel cited the university computer policy, which did not include a notice of a general monitoring practice but affirmatively stated that the university would access a networked computer only in situations when it was necessary to protect the university's computer system. Although the student had a reasonable expectation of privacy, the court concluded, nevertheless, that the university's remote and warrantless search of the student's computer was reasonable under the Fourth Amendment because the university had a special need to secure one of its mail servers that was being hacked. Implicit in *United States v. Heckenkamp* is a finding that a computer use policy can eliminate an enforceable expectation of privacy even with respect to downloaded data on a personal computer located in private quarters, if that computer is integrated into a larger computer system.

The adverse impact of integrating a personal computer into an employer's network is further demonstrated by the decision in *United States v. Barrows*.[97] When Michael Barrows, the Glencoe, Oklahoma City treasurer, decided in 2005 to temporarily relocate his personal computer to a public area in City Hall to perform his job duties, he probably perceived his action as demonstrating his commitment to public service. After all, both he and the city clerk had previously shared a single municipal computer to access city records. By adding his personal computer and connecting it to the municipal computer network, Barrows and the city clerk were able to simultaneously perform their computer based job duties.[98] In enhancing City Hall productivity, it probably never occurred to Barrows that his generosity and informality regarding the use of his personal computer would result in a federal court concluding that he had no reasonable

computer files cannot be obtained from someone else unless that person shares authority to access the files, including if necessary the required passwords, and such consent must be voluntary).

95. 482 F.3d 1142, 1145 (9th Cir. 2007).

96. *Id.* at 1146-47.

97. 481 F.3d 1246 (10th Cir. 2007).

98. *Id.* at 1247.

expectation of privacy regarding the content of his personal computer.[99]

In a 2007 decision, the Tenth Circuit concluded that Barrows lacked a reasonable expectation of privacy because he failed to take appropriate steps to limit third-party access to his personal computer files, such as installing a password system for those files or simply turning the computer off.[100] The court reasoned that Barrows' computer was utilized in a public place within City Hall, where the "chances a passerby might spy snatches of personal material over his shoulder, or sit down to use his computer having honestly mistaken it for a city one, were appreciable."[101] Therefore, the Court of Appeals affirmed the denial of Barrows' motion, under the Fourth Amendment, to suppress the child pornography images found on his personal computer.[102]

A few years before Barrows' actions, another Oklahoma public employee, state university architecture professor Eric Angevine, may have had a similarly erroneous sense of workplace electronic privacy, especially after he deleted 3000 pornographic images of young boys previously downloaded onto his office computer.[103] Following his arrest, however, Angevine was unable to persuade the Tenth Circuit that those downloaded pornographic images should be suppressed. The appellate panel concluded that he lacked Fourth Amendment protections regarding the content of his workplace computer.[104] The Tenth Circuit, in applying the *O'Connor* standards, concluded that Angevine lacked a reasonable expectation of privacy based on the university's computer use policy and practices, the university's ownership of the office computer and computer files, and the failure of Angevine to take steps aimed at limiting access to the downloaded images.[105] The university's broad policy and practice placed employees on notice that their internet use was subject to auditing and monitoring, with the university retaining the right to access the computers during investigations. The university's practice included maintenance of logs indicating when data has been deleted and computer screen warnings reiterating the consequences of computer

99. *Id.* at 1248-49.
100. *Id.*
101. *Id.* at 1249.
102. *Id*.
103. U.S. v. Angevine, 281 F.3d 1130, 1132 (10th Cir. 2002).
104. *Id.* at 1134-35.
105. *Id.*

misuse.[106]

When University of Nebraska employee Gerald Biby refused to sign a consent form to permit his employer access to his workplace computer files to gather relevant documents for a commercial arbitration, Biby probably felt that he was relying on constitutional principles.[107] Unfortunately for Biby, his university employer did not share his perspective regarding the scope of protected privacy. A few weeks later, Biby was given a direct order to provide immediate access to various documents on his computer. The following day, university representatives came to his office and announced that they would be searching his computer files, whether or not Biby consented.[108]

After reviewing Biby's computer files and email, the university terminated him based on its conclusion that he had engaged in misconduct.[109] After his termination, Biby commenced a federal lawsuit alleging that the university's search of his office computer was unconstitutional.[110] In affirming the grant of summary judgment to the university, the Eighth Circuit concluded that the university's computer policy gave employees like Biby notice that office computers were subject to search if the school had a legitimate reason. Furthermore, the Court of Appeals concluded that the university's search was reasonable because the electronic documents seized were needed for a pending arbitration and that the scope of the computer search was limited through the use of key words relevant to the issues in the arbitration.[111]

Similarly, the Eighth Circuit found, based on the employer's computer policy, that a 2002 search of a Missouri state employee's workplace computer did not violate the employee's Fourth Amendment rights.[112] In a remote search of the state employee's computer, as part of an investigation into his distribution of non-work related email, the employer found proof that the employee had accessed pornographic websites.[113] Following the initial discovery of

106. *Id.* at 1134.

107. Biby v. Bd. of Regents, 419 F.3d 845, 847-48 (8th Cir. 2005).

108. *Id.* at 848-49.

109. *Id.* at 849.

110. *Id.*

111. *Id.* at 850-51.

112. U.S. v. Thorn, 375 F. 3d 679, 684-85 (8th Cir. 2004), *vacated on other grounds* 543 U.S. 1112 (2005).

113. *Id.* at 681.

the visits to the pornographic websites, the employee's office computer was seized for an examination of the images that he had downloaded.[114] In denying the employee's effort to suppress those computer images, the Eighth Circuit concluded that the employee lacked a reasonable expectation of privacy, based on the state agency's explicit policy prohibiting unauthorized computer use, which placed employees on notice that they did not have any personal privacy protections with respect to the computers and preserved the agency's right to access all agency computers.[115]

In another child pornography prosecution of a public employee, the Fourth Circuit reached a similar conclusion regarding an employee's lack of a reasonable expectation of privacy based on the federal agency's computer use policy.[116] In that case, the agency's policy stated that all agency computers were subject to audit, inspection, and monitoring regarding both internet and email use.[117]

Decisions by the Fifth and Second Circuits provide examples in which workplace realities can result in findings that employees have a reasonable expectation of privacy with respect to the content of their workplace computers. In *United States v. Slanina*, Texas city fire marshal Wesley Slanina was assigned a city computer at his City Hall desk.[118] The computer had access to the internet, but was not connected to the city computer network.[119] Without his employer's knowledge, Slanina installed a screen saver protected by a password as well as a BIOS password to protect the computer's hard drive.[120] Despite the passwords, at all times the employer's information technology staff had access to the computer for upgrading and for networking purposes.[121]

After Slanina transferred to a new fire station, his work computer was relocated to his new private office. When a staff person attempted to connect Slanina's office computer to the city network, he was stymied by the passwords placed on the computer. Following a request from the city, Slanina provided the necessary password, resulting in the discovery that he had been utilizing his office

114. *Id.* at 681-82.
115. *Id.* at 683.
116. U.S. v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).
117. *Id.*
118. 283 F.3d 670, 672 (5th Cir. 2002).
119. *Id.* at 671-72.
120. *Id.* at 672.
121. *Id.* at 676.

computer to download pornographic images.[122]

After examining the relevant policies and practices in Slanina's workplace, the Fifth Circuit determined that Slanina had a reasonable expectation of privacy in the content of his computer files.[123] Among the factors considered by the Fifth Circuit were: Slanina worked in a private office; access to his assigned computer by co-workers was not routine; and the city had failed to circulate a policy prohibiting the use of workplace computers for personal use and placing employees on notice that computer use would be monitored.[124] Nevertheless, the Fifth Circuit held that Slanina's Fourth Amendment rights were not violated by the city's warrantless search because the search was reasonably related to conducting a workplace investigation into misconduct.[125]

In *Leventhal v. Knapek*, the Second Circuit concluded that a state employee who was found to have used his office computer to conduct a private business practice had a reasonable expectation of privacy regarding the content of the computer.[126] In reaching its conclusion, the Second Circuit cited to the fact that the employee did not share the office or his computer with co-workers and to the absence of a practice or procedure of routine accessing or monitoring of workplace computers.[127] As in *United States v. Slanina*, however, the Second Circuit panel concluded that the warrantless search did not violate the Fourth Amendment because the search was reasonably related to a disciplinary investigation based on a specific report that the employee was misusing the computer for personal business.[128] Both *Slanina* and *Knapek* reinforce the importance of employer policies and practices in determining whether an employee has an enforceable expectation of privacy in the context of disciplinary investigations.

A 2005 New Jersey state appellate decision, *Doe v. XYC Corp.*,[129] demonstrates that when an employer fails to monitor employee internet use consistent with its computer use policy and after

122. *Id.* at 672.
123. *Id.* at 677.
124. *Id.* at 676-77.
125. *Id.* at 677-81.
126. 266 F.3d 64, 73-74 (2d Cir. 2001).
127. *Id.* at 73-74.
128. *Id.* at 75-77.
129. 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005); *see also* Jamila Johnson, *Employee Internet Misuse: How Failing to Investigate Pornography May Lead to Tort Liability*, 4 SHIDLER J.L. COM & TECH. 1 (2007).

receiving information about an employee misusing the workplace computer, the employer can face civil liability to a third-party harmed by an employee's conduct. In *Doe*, the court held that a complaint by a third-party stated a cause of action against an employer based on the common law duty of care under the *Restatement (Second) of Torts* which requires an employer to supervise its employees to curtail harm to third-parties.[130]

The lawsuit in *Doe* was commenced on behalf of the stepdaughter of a company employee, whose nude photographs were uploaded onto child pornography websites by the employee utilizing a company computer.[131] The complaint alleged that the employee had sexually abused the stepdaughter and that if the employer had timely investigated the employee's earlier pornographic internet activity, which took place over a four-year period, the sexual abuse would have been discovered sooner.[132] The complaint further alleged that although the company had a computer use policy, it failed to take appropriate action against the employee after receiving complaints and specific information regarding the employee's pornographic internet habits.[133] These allegations were found to be sufficient to state a claim against the employer based on its failure to act.[134]

In summary, employers have strong legal incentives and obligations to establish and enforce computer use policies regarding access to the internet. Such policies and practices result in the virtual elimination of any protected legal rights of employees with respect to internet access. In many ways, this state of law is counterintuitive to workplace practices that grant wide internet access during the workday, along with the magnetic pull, if not the addictive quality, of the internet. The notable gap between legal reality and actual office practices strongly supports the use of internet use audits by employees aimed at narrowing the websites deemed necessary for each employee's work duties, as well as completely eliminating access for some employees when appropriate.

IV. EMAIL @ WORK

This article now turns to a legal discussion of workplace email.

130. 887 A.2d at 1158; RESTATEMENT (SECOND) OF TORTS § 317 (1977).
131. *Id.* at 1160.
132. *Id.* at 1158-61.
133. *Id.*
134. *Id.* at 1164-70.

Unlike broad internet access, email use has become an essential communication tool in the modern workplace. It has been estimated that American employees spend 25 percent of the workday sending and responding to email.[135] During the eight years of the Clinton Administration, government officials created thirty-two million emails.[136]

Overuse of email can have negative consequences for employers and employees alike, including miscommunication and employee alienation, as well as workplace disruptions. Replacing direct oral communications during meetings and teleconferences with email can undermine a positive workplace culture. Despite the adverse impact email can have on workplace culture, few employers proactively address the issue of email overuse or conduct trainings on email etiquette.

It is ironic that the only known decision that encourages employees to communicate with each other through face-to-face interactions rather than email is a recent decision interpreting the NLRA, a law enacted to protect private sector employees when they engage in various forms of protected union and concerted activities. In *Register-Guard,*[137] the Board majority ruled that employees of a newspaper lacked an NLRA right to utilize an employer's workplace email system to solicit support for the union, in part because there were no existing obstacles to them speaking directly with each other during break times. In contrast, while employers are free to deny email access for speech generally protected under the NLRA, the "employer may use its own equipment to send antiunion messages."[138]

Other legal developments relating to email have been, in general, inconsistent with the subjective sense of solitude and intimacy associated with email use. This false sense of entitlement to a zone of workplace privacy is due to the perception that email has the same legal protections associated with regular mail and telephone use.

Like many contemporary employees utilizing email in the workplace, when A. Orlando Jackson deposited a sealed envelope at a New York City post office in February 1877 he probably had no idea that this simple act would lead to severe adverse consequences. Jackson was arrested for the crime of mailing circulars with

135. SHIPLEY & SCHWALBE, *supra* note 2, at 8.
136. *Id.*
137. 351 N.L.R.B. No. 70, at 6-7 (Dec. 16, 2007).
138. *Id.* at 9 n.17.

information about various lotteries in violation of a federal criminal prohibition.[139] Following his arrest, Jackson filed a writ of habeas corpus in federal court, seeking his freedom based on a claim that the federal law was unconstitutional.[140] After the writ was denied, Jackson appealed his case to the Supreme Court.

In 1878, the Supreme Court issued a unanimous decision upholding the constitutionality of the law and Jackson's incarceration.[141] In reaching its decision, the Court drew a distinction between congressional power to exclude certain subjects from the mail and the Fourth Amendment prohibition against warrantless searches and seizures. The Court recognized that the content of letters and materials contained in sealed mail packages cannot be lawfully examined without a warrant:

> No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail; and all regulations adopted as to mail matter of this kind must be in subordination to the great principle embodied in the fourth amendment of the Constitution.[142]

At the same time, the Court reasoned that the police can lawfully gather evidence through other means, such as information on the exterior of the envelope.[143] The limit to the constitutionally protected privacy interests connected with regular mail has resulted in a series of Supreme Court decisions holding that an individual lacks Fourth Amendment protections regarding the content of a letter after it is received by a third-party.[144] These holdings are premised on the proposition that the sender has assumed the risk that the third-party recipient will share the content of the letter with the government or others.

In contrast to the recipient of a regular letter, a recipient of an email has the capability of forwarding email to an unlimited number of recipients throughout the world. An email sender, therefore, assumes a greater risk of third-party access to the content of the email than a regular letter writer.[145] The greater risk is magnified when a

139. In re Jackson, 13 F. Cas. 194 (S.D.N.Y. 1877).

140. *Id.*

141. In Re Jackson, 96 U.S. 727, 737 (1878).

142. *Id.* at 733.

143. *Id*. at 735.

144. *See* SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); U.S. v. Jacobsen, 466 U.S. 109, 117 (1984); U.S. v. Miller, 425 U.S. 435, 444 (1976).

145. In our modern times, of course, a recipient of a letter can transform it into an electronic document with a scanner and distribute it in various ways: as an attachment to an email; as the content of an email; or by posting it on a website or a blog.

poorly worded email written by a supervisor or manager critical of staff is widely distributed. Such wide distribution can cause disharmony and demoralization, as well as bad publicity.[146] This greater risk is demonstrated by the recent embarrassment and possible employment difficulties for a particular employee of JP Morgan Chase, whose email from work to friends, relating to a Craigslist.com personal ad, wound up posted on various blogs.[147]

Many court decisions on privacy claims regarding the content of sent email have concluded that the sender lacks a reasonable expectation of privacy once the email has been sent or posted.[148] In 2001, the Sixth Circuit Court of Appeals observed that users of an electronic bulletin board:

> would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting. They would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient; at this moment, the e-mailer would be analogous to a letter-writer, whose "expectation of privacy ordinarily terminates upon delivery" of the letter.[149]

In *Smyth v. Pillsbury Co.*,[150] an employee's common law intrusion on seclusion tort[151] claim was dismissed for failure to state a cause of

146. Peter Applebome, *School Chief's Embarassment Is a Lesson for Itchy E-Mailers*, N.Y. TIMES, Oct. 25. 2007, at B1.

147. Andrew Adam Newman, *Acquisitive Craigslist Post Reddens Faces All Around*, N.Y. TIMES, Oct. 8. 2007, at C6.

148. *See* U.S. v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (reasonable expectation of privacy is diminished by the transmission of emails that have already been received); U.S. v. Maxwell, 45 M.J. 406, 417-19 (C.A.A.F. 1996); Culbreth v. Ingram, 389 F. Supp. 2d 668 (E.D. N.C. 2005). In *U.S. v. Forrester*, 512 F.3d 500, 509-10 (9th Cir. 2008), the Ninth Circuit held that a computer user lacked an expectation of privacy with respect to the to/from addresses of his email, the IP addresses of the websites he visited and the amount of electronic data that was transmitted to and from his account. In reaching its conclusion, the circuit court applied Supreme Court precedent holding that police use of a pen register to obtain the telephone numbers dialed from a phone did not violate the Fourth Amendment because when making a call to a third party, the telephone company has knowledge of the number dialed. Smith v. Maryland, 442 U.S. 735, 742 (1979). The Ninth Circuit reasoned that email users have implied knowledge that when they send and receive emails, emails addresses are used by the internet company to rout the email. 513 F.3d at 510.

149. Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (citations omitted). In contrast, in *United States v. Charbonneau*, 979 F. Supp. 1177 (S.D. Ohio 1997), the court found a reasonable expectation of privacy in email sent from an individual's AOL personal email account but did not find a similar protected expectation in the email sent to a chat room.

150. 914 F. Supp. 97 (E.D. Pa. 1996).

151. The *Restatement (Second) of Torts* § 652B (1977) sets forth the definition for the tort of intrusion on seclusion:

> [o]ne who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Unlike a public employee, who may have a claim against an employer for an invasion of

action, based on a finding that the employee lacked a protected privacy interest connected with email sent on employer's computer system. In dismissing the complaint, the District Court stated:

> Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.[152]

In 2006, the United States Court of Appeals for the Armed Forces ruled that a lance corporal had a reasonable expectation of privacy with respect to her personal emails sent and received on a military computer located in Marine Corps headquarters.[153] In *United States v. Long,* the military appellate court, applying the principles of *O'Connor v. Ortega*, reached its conclusion based on the particular practices and procedures within that military branch's headquarters. Under the office practices, each individual computer user was required to use a unique personal password to gain access that had to be updated regularly and the office email monitoring policy was limited.[154] Although all military computers have a log-on banner stating that information maintained on the computers is subject to monitoring, including personal information, the court concluded the banner message did not defeat an enforceable expectation of privacy based on the practices in the particular military headquarters.[155] Whether the military precedent in *United States v. Long* will constitute persuasive authority with respect to civilian workplace

workplace privacy under the Fourth Amendment and 42 U.S.C. § 1983 (2000), a private sector employee can litigate a breach of workplace privacy claim only if the relevant state recognizes a common law right to privacy tort. Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7th Cir. 2002). Among the states that have recognized a common law right to privacy are Pennsylvania, South Dakota, Texas, and New Hampshire. *See* Remsburg v. Docusearch, 816 A.2d 1001 (N.H. 2003); Doe v. Kohn, Nast & Graf, 862 F. Supp. 1310 (E. D. Pa. 1994); Roth v. Farner-Bocken Co., 667 N.W.2d 651 (S.D. 2003); K-Mart Corp. v. Trotti, 677 S.W.2d 632 (Tex. App. 1984). In addition, California's constitutional right to privacy provision has been interpreted to permit lawsuits challenging privacy intrusions by private entities. *See* CAL. CONST. art. 1 § 1; Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994).

152. *Smyth*, 914 F. Supp. at 101; *see also* Thygueson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004) (employee lacked a reasonable expectation of privacy regarding emails received and sent from office computer); Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343 (D. Mass. May 7, 2002) (use of individual password on company computer system to save emails found to be insufficient to create reasonable expectation of privacy); McLaren v. Microsoft, No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103 (Tex. App. May 28, 1999) (dismissing privacy tort complaint concluding that the employee lacked a reasonable expectation of privacy in his email even though they were stored under a private password with employer's consent).

153. *See* United States v. Long, 64 M.J. 57, 64 (C.A.A.F. 2006).

154. 64 M.J. at 60, 64.

155. *Id.* at 60, 64-65.

email remains to be seen. It is reasonable to expect, however, that civilians working in an at-will context should have greater privacy rights than individuals working in a military workplace.

In *Quon v. Arch Wireless Operating Co.*,[156] the Ninth Circuit Court of Appeals examined whether a California police officer had privacy protections under the Fourth Amendment with respect to the content of text messages utilizing a pager provided by the city. In *Quon*, the city contracted with a private company for a pager system to be utilized by police officers. Under the contract, each pager was allotted 25,000 characters and the city were responsible to pay the company for any use beyond that amount. The pager system enabled police officers to engage in two way text messaging. The system was based upon radio transmissions received and sent by a receiving station owned by the company with the content of each message stored and archived on the company's computer server.

In implementing the system, the city did not promulgate a formal pager use policy or inform the police officers that the existing computer use policy was fully applicable to the pagers. Instead, an informal pager policy and practice was developed by the lieutenant in charge of the pagers for when a police officer's personal texts resulted in use beyond the contractual limit for text message characters. Under the informal policy and practice, the content of the text messages were not audited so long as the individual officer paid the overages. Eventually, the lieutenant became frustrated with dunning police officers. The lieutenant's frustration resulted in the police chief directing the lieutenant to request from the company the transcripts of a police officer's text messages. Following an audit of those messages, the police department found that the police officer had been using the pager to send personal text messages including some that were sexually explicit.

Based on the informal policy and practice developed by the lieutenant, the Ninth Circuit concluded that the police officer had a reasonable expectation of privacy with respect to the content of his text messages even though the lieutenant was not an official policymaker. In addition, the Ninth Circuit held that the police department's search was not reasonable under the Fourth Amendment based upon the limited purpose for the search: to determine whether the police officer was responsible to pay for the

156. 529 F.3d 892 (9th Cir. 2008).

overages. Relying on *O'Connor*, the circuit panel found that the department had a number of less intrusive means to satisfy the department's expressed need for the information.

The analysis utilized by a Sixth Circuit panel in *Warshak v. United States*[157] may also have a profound impact on future cases involving workplace email privacy claims. Although the decision was subsequently vacated a majority of the court sitting *en banc*, on the basis of standing and ripeness, the initial June 2007 panel decision is a significant development in the judicial analysis of privacy rights associated with email. In its initial decision, the Sixth Circuit examined the scope of protected email privacy in the context of reviewing an injunction which enjoined, on due process grounds, the enforcement and application of a provision of the ECPA's Stored Communications Act.[158] The provision in question permits the issuance of court order, without notice to a subscriber, requiring the release of stored email and other documents maintained by an internet service provider (ISP).[159]

In evaluating the merits of plaintiff's claim regarding his protected privacy interests in the stored email, the original Sixth Circuit panel determined that although an email has been sent, the sender retains a reasonable expectation of privacy regarding the content of emails that are stored with an ISP.[160] The panel reached its holding by combining constitutional privacy principles relating to regular mail and to telephone use. In rejecting the government's argument that individuals do not have a reasonable expectation of privacy in stored email because ISPs utilize software to scan email for pornography and computer viruses, the Sixth Circuit panel, echoing the distinction set forth in *In Re Jackson,* stated: "In fact, these screening processes are analogous to the post office screening packages for evidence of drugs or explosives, which does not expose the content of written documents enclosed in the packages."[161]

157. 490 F.3d 455 (6th Cir. 2007), *vacated in part by* No. 06-4092, 2008 WL 2698177 (6th Cir. June 11, 2008).

158. Pub. L. No. 99-508, 100 Stat. 1848 (codified at 18 U.S.C. §§ 1367, 2510-21, 2701-11, 3117, 3121-27 (2000)).

159. 18 U.S.C. § 2703(d) (2000). In contrast to other subsections in 18 U.S.C. § 2703 that require prior notice to a subscriber before the enforcement of a search warrant or administrative subpoena to an ISP for access to electronic records including the content of email, 18 U.S.C. § 2703(d) sets forth a procedure for issuance of a court order to an ISP without notice to the subscriber.

160. *Warshak*, 490 F.3d at 473-74.

161. *Id.* at 474.

The Sixth Circuit panel concluded that the content of email stored by an ISP has privacy protections based on a societal expectation that an ISP will not access the content of subscriber email. In describing this societal expectation regarding ISP non-access to email content, the court analogized email to the telephone:

> The content of e-mail is something that the user "seeks to preserve as private," and therefore "may be constitutionally protected." *Katz*, 389 U.S. at 351. It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past. See *Katz,* 389 U.S. at 352 ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.")[162]

In contrast, the majority of the Sixth Circuit *en banc* panel rejected the notion of a universal societal expectation that an ISP will not access the content of e-mail. Citing to the diversity of actual and potential provisions in ISP agreements, the majority concluded that whether a reasonable expectation of privacy exists will be dependent on the terms of the applicable ISP agreement in each case.

If the original legal analysis in *Warshak* is sustained, it is probable that efforts will be made to extend it to stored employee email on employer mail servers as well as back-up tapes. In particular, *Warshak* may become the legal framework for employee challenges to electronic discovery requests and discovery orders that fail to place the employee on notice. Whether the *Warshak* analysis is extended to the employment context will depend on judicial acceptance of a societal expectation that employers will not, or should not, access the content of stored personal employee email.

Unlike most ISPs, workplace computer use policies frequently place employees on notice that they should not expect any privacy with respect to the content of their email at work. Nevertheless, the growing integration of personal computers with workplace computers may result in future court decisions concluding that personal email sent from the employee's personal computer, but stored on the employer's computer system, is entitled to some privacy protections under the Fourth Amendment or common law.

In April 2007, the European Court of Human Rights in *Copland*

162. *Id*. at 473.

v. United Kingdom[163] was called upon to determine the scope of privacy protections relating to workplace email under Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The European Court concluded that a British public college had violated the rights of employee Lynette Copland when it engaged in the monitoring of her email, internet, and telephone use. Under Article 8, the applicable standard is whether the governmental actions challenged constituted an interference with an individual's right to respect for his or her private life and correspondence.[164]

Ms. Copland is a British public college administrative assistant who learned of the surveillance when her stepdaughter was requested by the college to provide information regarding certain emails.[165] The employer acknowledged that the surveillance had taken place, but sought to justify its actions on the ground that it was seeking to determine whether Ms. Copland was engaging in excessive personal use of the college's equipment.[166] In addition, the college argued that the surveillance did not violate her rights under Article 8 because the monitoring did not include the reading of the content of her emails or of the websites she visited. Instead, the monitoring was limiting to keeping track of the addresses, dates, and times of Ms. Copland's email and internet use.[167] The European Court rejected that argument, concluding that the collection and storage of personal information relating to her email and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of Article 8.[168] The European Court's recognition of privacy protections for the email and internet addresses is far broader than rights recognized by

163. [2007] Eur. Ct. H.R. No. 62617/00, *available at* <http://cmiskp.echr.coe.int/tkp197/view.asp?action=html&documentId=815061&portal=hbkm&source=externalbydocnumber&table=F69A27FD8FB86142BF01C1166DEA398649>.

164. Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedom states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Convention for the Protection of Human Rights and Fundamental Freedom art. 8, Nov. 4, 1950, Europ. T.S. No. 5.

165. *Copland*, [2007] Eur. Ct. H.R. No. 62617/00 ¶¶ 1-12.

166. *Id.* ¶¶ 13, 32-35.

167. *Id.* ¶ 32.

168. *Id.* ¶¶ 41-49.

American courts under the Fourth Amendment.[169]

A recent New Jersey decision highlights that the scope of protected electronic privacy can be broader under a state constitution than under the Fourth Amendment. In *State v. Reid*[170] an employee, at home on disability leave, used her own personal computer to change her employer's shipping address to a non-existent address on a suppler's website. After the employee was indicted for computer theft, she moved to suppress her subscriber identification information obtained from her ISP through a subpoena duces tecum rather than a warrant based on probable cause. In affirming the grant of the motion to suppress, the New Jersey Supreme Court held that under the New Jersey Constitution, an individual has a reasonable expectation of privacy with respect to his or her subscriber identity. In reaching its decision, the New Jersey appellate court analogized identification information of a subscriber, held by an ISP, with telephone billing information and bank records which prosecutors may obtain only through issuance of a warrant under the New Jersey state constitution. In contrast, the Tenth Circuit Court of Appeals held that a computer user lacks a reasonable expectation of privacy in internet subscriber information under the Fourth Amendment.[171]

The New York Court of Appeals decision in *Thyroff v. Nationwide Mutual Insurance Co.,*[172] may bolster future common law claims relating to workplace email. The decision's broad *dicta* may set the stage for a future balanced analysis regarding the respective rights of employers and employees with regard to the content of stored email on workplace computers:

> Computers and digital information are ubiquitous and pervade all aspects of business, financial and personal communication activities. Indeed, this Opinion was drafted in electronic form, stored in a computer's memory and disseminated to the Judges of this Court via email. We cannot conceive of any reason in law or logic why this process of virtual creation should be treated any differently from production by pen on paper or quill on parchment. A document stored on a computer hard drive has the same value as a paper document kept in a file cabinet.[173]

169. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979); U.S. v. Forrester, 512 F.3d 500 (9th Cir. 2008). Left open by the European Court's decision is the question of whether the employer would have avoided liability under Article 8 through issuance of a policy announcing email and internet monitoring.

170. 945 A.2d 26 (N.J. 2008).

171. U.S. v. Perrine, 518 F.3d 1196 (10th Cir. 2008).

172. 864 N.E. 2d 1272 (N.Y. 2007).

173. *Id.* at 1277-78.

The decision in *Thyroff* resolved an issue of New York law: whether the common law tort of conversion was applicable to intangible property such as electronic documents and email.[174] Thyroff had worked as an insurance agent for a large insurance company pursuant to a written agreement. Under that agreement, he leased computer hardware and software known as agency office-automation system from the company. He utilized the system to send and receive personal emails unrelated to his business, which were stored on the computer. Each night, the insurance company would automatically upload on to its centralized computer all of the electronic data maintained by Thyroff. After twelve years as an agent, Thyroff was terminated; the company repossessed the computer hardware, and denied him access to his electronic records and personal data.[175] Thyroff commenced a lawsuit in federal court that included a common law claim of conversion of his electronic data including his personal emails. The Second Circuit certified to the New York Court of Appeals the legal question of whether an action for conversion can lie for electronic data.[176]

In concluding that the common law tort of conversion is applicable to stored personal email and other electronic documents,[177] the New York Court of Appeals broke new ground in the area of electronic workplace law and established precedent that may have major consequences in other aspects of New York law. Unlike the common law of other states, New York recognizes very few exceptions to the at-will doctrine and does not recognize a right to privacy.[178] Based on the at-will doctrine, a lawsuit challenging a termination will usually be dismissed at the pleading stage unless the complaint alleges a prohibited form of discrimination or retaliation. *Thyroff* suggests, however that, although New York law does not grant many non-statutory bases for challenging a termination, or grant broad privacy protections, an employee may retain a property interest in personal electronic documents and email stored on the employer's computer. As will be seen, New York's recognition of an individual property interest in personal electronic documents and

174. *Id.* at 1276-77.

175. *Id*. at 1273.

176. *Id.*; *see* Thyroff v. Nationwide Mut. Ins. Co., 460 F.3d 400 (2d Cir. 2006).

177. *Id.* at 1277-78.

178. *See* Horn v. N.Y. Times, 790 N.E.2d 753 (N.Y. 2003); Howell v. N.Y. Post, 612 N.E.2d 699, 703 (N.Y. 1993); Jones v. Capital Cities/ABC Inc., 874 F. Supp. 626 (S.D.N.Y. 1995); N.Y. CIV. RIGHTS LAW §§ 50, 51 (2007).

email on an employer's computer system may have significance in the future application of the Board's property law analysis in *Register-Guard.*[179]

Another important state appellate case considering workplace email in the context of property law is *Intel v. Hamidi.*[180] In that California case, an employer commenced a common law trespass action against a former employee, seeking to enjoin him from continuing to send emails to his former co-workers at the workplace.[181] In ultimately denying the injunction, the court concluded that the employer had failed to demonstrate sufficient economic injury caused by the former employee sending emails to former co-workers, noting that receipt of unsolicited email is as burdensome as receiving unsolicited telephone calls at work.[182] Nevertheless, the court noted that email "like other forms of communication, may in some circumstances cause legally cognizable injury to the recipient or to third parties and may be actionable under various common law or statutory theories."[183]

At the same time that courts have concluded that computer use policies and practices can diminish enforceable privacy expectations under the Fourth Amendment, the ECPA, and the common law, the statute that has the most significant potential impact on workplace email policies and practices is the NLRA.

V. THE NLRA'S RELEVANCE TO WORKPLACE COMPUTER USE POLICIES AND PRACTICES

As Professor Jeffrey M. Hirsch has noted, any major transformation in the law, is by definition, extraordinary.[184] It is even more extraordinary that the current provisions of the NLRA, originally enacted in 1935 in the midst of the New Deal and the ascendancy of the Congress of Industrial Organizations, may constitute the most promising framework for the potential development of a balanced administrative legal approach to workplace computer policies and practices.

179. *See infra* notes 229-33 and accompanying text.

180. 71 P.3d 296 (Cal. 2003).

181. *Id.* at 299-300.

182. *Id.* at 300.

183. *Id.*

184. Jeffrey M. Hirsch, *The Silicon Bullet: Will the Internet Kill the NLRA?*, 76 GEO. WASH. L. REV. 262 (2008).

As a practical matter, unless Congress decides to amend the ECPA to mandate a new legal balance between employee and employer interests in the electronic workplace, application of established legal principles under NLRA will remain the primary focus for the possible development of a nuanced approach to those conflicting interests.[185]

Expectations that the NLRA will play that core role in the immediate future, however, should be kept to a minimum. Even with respect to its remedial powers, the Board has refused to require employers to electronically post or circulate the agency's posting that was a part of the ordered remedy for the employer's NLRA violation.[186] Based on the ubiquity of email and intranets in workplaces, electronic postings or distribution may constitute the most efficient means of informing the workforce of the Board's order. The Board's lack of will to require an electronic distribution of its own orders is symptomatic of the problems associated with administrative legal efforts aimed at making the NLRA a relevant legal reality in the computer based workplace.

In a recent article, Board member Wilma B. Liebman articulated various reasons for a diminished sense of expectation that the Board will reevaluate the NLRA in such a manner as to make the statute relevant to the contemporary workplace:

> In this historical context, American labor law, enacted when the prototypical workplace was the factory, and the rotary telephone was "the last word in desktop technology," increasingly appears out of sync with changing workplace realities. Yet the Board itself has

185. Various federal and state collective bargaining laws in the public sector may impact email policies and practices of state and local governments. The applicable standards for protected activities under such laws are analogous to the NLRA. Nevertheless, interpretations of such laws can and do differ from Board decisions in many substantive areas due to differences in statutory language, legislative intent as well as the distinct mission of public employers. In 2001, the Michigan Employment Relations Board rejected an argument that public employees under Michigan's public sector law have a *per se* right to utilize the employer's email system for union activity. However, it did conclude that the county employer was not entitled to discriminate against union-related emails. Oakland County, 15 Mich. Pub. Emp. Rep. (LRP) ¶ 33,018 (2001). In New York, PERB upheld the lawfulness of discontinuing a state union activist's office and home connections to the state's email network after the employee failed to follow a directive that he discontinue sending union- related mass emails to the membership. In re Pub. Emp. Fed., AFL-CIO, 33 N.Y. Pub. Emp. Rep. (LRP) ¶ 3046 (2000), *conf. sub nom*, Benson v. Cuevas, 741 N.Y.S.2d 310 (App. Div. 3d Dep't 2002). In *Int'l Union of Operating Engineers, Local 542 v. Upper Southampton Township*, 36 Penn. Pub. Emp. Rep. 112 (2005), the Pennsylvania labor relations board found that a town did not have to negotiate a computer use and telephone policy because the policy did not impact the employees' fundamental interests in wages, hours and working conditions.

186. Nordstrom, Inc. 347 N.L.R.B. No. 28 (May 31, 2006); Nat'l Grid USA Serv. Co., Inc., 348 N.L.R.B. No. 88 (Dec. 11, 2006).

> made little sustained effort to adjust its legal doctrines to preserve worker protections in a ruthlessly competitive economy. In short, labor law policymakers and enforcers have done too little, too late.[187]

The recent Board decision in *Register-Guard*,[188] in which members Liebman and Walsh dissented, confirms some of the points raised by member Liebman in her article. Over thirty years ago, the Supreme Court expressly embraced the importance of the Board reinterpreting the NLRA in the face of technological advances in the workplace.[189] *Register-Guard* constitutes a significant blow to attempts to persuade the Board to reevaluate the NLRA in such a manner as to make the statutory rights granted relevant and applicable to the massive growth of computer-based workplace communications.

Despite the proliferation of email as the prevalent means of employee communications in many workplaces, *Register-Guard* has substantially rejected the application of rights granted to employees under Section 7 of the NLRA[190] to computer use policies and practices. This current state of the law is particularly significant to the growing number of decentralized workplaces and mobile vocations where employees do not physically interact with each other during the workday, but communicate through employer laptops and other portable electronic devices.

The facts in *Register-Guard* are not complex. Approximately 150 employees of the Eugene, Oregon newspaper, *Register-Guard*, are represented by the Eugene Newspaper Guild. The newspaper maintains a computer use policy containing the following non-solicitation provision:

> Company communication systems and the equipment used to operate the communication systems are owned and provided by the Company to assist in conduct in the business of The Register-Guard. Communications systems are not to be used to solicit or proselytize for commercial ventures, religious or political causes,

187. Liebman, *supra* note 38, at 576 (citations omitted).

188. 351 N.L.R.B. No. 70 (Dec. 16, 2007).

189. NLRB v. J. Weingarten, Inc., 420 U.S. 251, 265 n.10, 266 (1975).

190. 29 U.S.C. § 157 (2000). Section 7 states:

> Employees shall have the right to self-organize, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection, and shall also have the right to refrain from any or all of such activities except to the extent that such right may be affected by an agreement requiring membership in a labor organization as a condition of employment as authorized in section 158(a)(3) of this title.

outside organizations, or other non-job-related solicitations.[191]

With the knowledge and acquiescence of the newspaper, employees have utilized the workplace email system for a large variety of non-work related subjects.

In May 2000, the union president, who was employed by the newspaper, sent an email to unit members from her work station computer during her break. The substance of the email sought to clarify certain information contained in the employer's earlier email surrounding a recent union rally. In response to her use of the newspaper's computer system, the union president received a disciplinary warning. A few months later, the union president received a second disciplinary warning after she sent two additional union-related emails to union members in the workplace from the union's office, located off the newspaper's premises.

For approximately ten years, prior to *Register-Guard*, the NLRB's General Counsel had been advocating in favor of applying well-established NLRA principles to computer use policies that would limit the lawful scope of employer computer anti-solicitation policies and practices.[192] In *Register-Guard*, the General Counsel unsuccessfully attempted to persuade the Board for the first time to conclude that an employer's computer use anti-solicitation policy was overbroad and therefore violative of the NLRA[193] The foundation of the General Counsel's legal argument was premised on the distinct legal approaches developed under NLRA between solicitation and distribution by employees while on the employer's property.

The earliest application of the General Counsel's legal theory was set forth in the 1998 advice memorandum in *Pratt & Whitney*.[194] The advice memorandum in that case was in response to a request from an NLRB Regional office for an opinion as to whether a complaint should issue with respect to an unfair labor practice charge challenging an employer's policy prohibiting all non-work related

191. 351 N.L.R.B. No. 70, at 2.

192. NLRB Gen. Couns. Adv. Mem. (Pratt & Whitney) 12-CA-18446, 18772, 18745 & 18863 (Feb. 23, 1998), *available at* <http://www.nlrb.gov/index.aspx> (under Research tab, and under Memos on the drop down menu, select Advice Memos link from the Memos menu, select the year 1998 and click Go to browse, scroll down the alphabetical list and select Pratt & Whitney).

193. 351 N.L.R.B. No. 70, at 5.

194. NLRB Gen. Couns. Adv. Mem. (Pratt & Whitney) 12-CA-18446, 18772, 18745 & 18863 (Feb. 23, 1998), *available at* <http://www.nlrb.gov/index.aspx> (under Research tab, and under Memos on the drop down menu, select Advice Memos link from the Memos menu, select the year 1998 and click Go to browse, scroll down the alphabetical list and select Pratt & Whitney).

email on workplace computers.[195]

In *Pratt & Whitney*, a union seeking to represent unorganized engineering employees had filed a charge challenging the employer's computer use policy prohibiting the use of email for non-business and personal use. The engineering employees used workplace email as their primary means of communication and spent a significant amount of their work time utilizing the workplace computers. In addition, when employees were off premises, they utilized employer-provided laptops to access their email. The General Counsel advised that a complaint should be issued based on the frequency with which employees utilized the employer's computers and computer network. Under the General Counsel's analysis, email should be treated as a form of solicitation due to its instantaneous and reciprocal qualities.[196]

Based on the regularity of employees at Pratt & Whitney communicating with each other electronically, the memorandum concluded that the employer's computer system constituted a virtual work area where employees were entitled to engage in concerted activity, rendering the employer's anti-solicitation policies presumptively unlawful under *Republic Aviation Corp. v. NLRB*.[197] In *Republic Aviation Corp.*, the Supreme Court upheld a Board determination that an employer's anti-solicitation policy prohibiting concerted activities inside the employer's work areas during non-working time was presumptively unlawful under the NLRA. This presumption may be overcome if the employer demonstrates that the policy is necessary to maintain production or discipline.[198]

It has been long recognized that communication between employees on the job is essential to the exercise of the associational rights granted under the NLRA.[199] In decisions subsequent to

195. *Id.*

196. *Id.* If email is considered to constitute distribution, it would be subject to the holding in *Stoddard-Quick Manufacturing Co*. 138 N.L.R.B. 615 (1962) where the Board found that employers have far greater rights to limit the distribution of literature in the workplace.

197. NLRB Gen. Couns. Adv. Mem. (Pratt & Whitney) 12-CA-18446, 18772, 18745 & 18863; *see also* Republic Aviation Corp. v. NLRB, 324 U.S. 793 (1945). In other advisory memoranda the Division of Advice concluded that policies prohibiting electronic "chain letters" and mass emails did not violate the NLRA because such restrictions are content-neutral, are applicable to electronic messages, and are based on evidence demonstrating "significant interference" with business operations. NLRB Gen. Couns. Adv. Mem. (Express Scripts, Inc.) 28-CA-19605 (February 24, 2005), *available at* <http://www.nlrb.gov/shared_files/Advice%20Memos/2005/28-CA-19605(02-24-05).pdf>; *Boeing Co*., 19-CA-28900, et al. (May 4, 2004), *available at* <http://www.nlrb.gov/shared_files/Advice%20Memos/2006/19-CA-28900(05-04-04).pdf>.

198. 324 U.S. at 803.

199. Beth Israel Hospital v. NLRB, 437 U.S. 483, 491 (1978).

Republic Aviation Corp., the Supreme Court has reiterated that when Section 7 activities are conducted by employees who are lawfully present on the employer's property, the "employer's management interests, rather than his property interests" are involved.[200] In contrast, the Board and the courts have applied a significantly different balance in cases where non-employees have attempted to access an employer's real property to engage in Section 7 activities. In non-employee access cases, the Board will balance the NLRA statutory rights against the employer's property interests.[201] In such cases, access by non-employees to facilities is not legally mandated "when other means are readily available."[202]

In *Register-Guard*, the General Counsel argued before the Board that the newspaper's computer use policy was overbroad based on the holding in *Republic Aviation Corp* and its progeny.[203] The argument was premised on the fact that the newspaper's employees utilize their workplace email system in a regular and continuous manner to engage in interactive communications with co-workers. Based on this substantial use, the Board was urged to find that the newspaper's computer system constituted a work space where electronic solicitations under Section 7 during non-work periods are presumptively lawful under the NLRA. Therefore, unless the newspaper demonstrated to the Board that the anti-solicitation policy is necessitated by a managerial need to maintain production or discipline, the newspaper's computer use policy was unlawfully overbroad.[204]

In response, the newspaper contended that the Board should reject the General Counsel's legal argument, asserting that its common law property right to control its equipment outweighs any claimed statutory right under the NLRA for employees to use the computer system. In support of this argument, the employer cited to a series of prior Board decisions that the employer conceded constituted the Board's "absolutist pro-employer property rights position."[205]

200. Eastex. Inc. v. NLRB, 437 U.S. 556, 571-72 (1978); Hudgens v. NLRB, 424 U.S. 507, 521-22, n.10 (1976).

201. *See* Jeffrey M. Hirsch, *Taking State Property Rights Out of Federal Labor Law*, 46 B.C. L. REV 891 (2006).

202. Lechmere, Inc. v. NLRB, 502 U.S. 527 (1992); NLRB v. Babcock & Wilcox Co., 351 U.S. 105, 114 (1956).

203. 351 N.L.R.B. No. 70, at 4.

204. *Id.* at 4-5.

205. Brief in Support of Respondent's Exceptions to the Decision of the Administrative

Underscoring the importance of the issues raised in *Register-Guard*, multiple nationwide organizations representing employer and employee interests filed *amici* briefs, and some of those organizations participated in the March 2007 oral argument before the Board, along with the NLRB's General Counsel and the attorneys representing the employer and the union.

On a Sunday in mid-December 2007, the Board issued its long awaited decision in *Register-Guard*.[206] In a 3-2 decision, the majority adopted the absolutist property rights position urged by the employer and rejected the statutory argument asserted by the General Counsel.

Relying on prior Board decisions holding that employees did not have a statutory right to utilize certain types of employer-owned equipment such as a television, telephone, or bulletin board, the Board held that the employer's "basic property right" rendered the newspaper's computer use policy lawful.[207] The Board's decision contains a robust and all-consuming property rights perspective making anti-solicitation provisions of computer use policies presumptively lawful.

In reaching its holding, the Board majority explicitly rejected the applicability of the traditional statutory distinction between solicitation and distribution.[208] In addition, it rejected the dissent's contention that based on Supreme Court precedent; employee

Law Judge at 26, The Guard Pub. Co. d/b/a/ Register Guard, 351 N.L.R.B. No. 70 (Dec. 16, 2007) (S 36-CA-8743-1, 36-CA-8849-1, 36-CA-8789-1 & 36-CA-8842-1); *see* Mid-Mountain Foods, Inc., 332 N.L.R.B. 229 (2000) (employer video player); Honeywell, Inc., 262 N.L.R.B. 1402 (1982) (employer bulletin board); Union Carbide Corp., 259 N.L.R.B. 974, 980 (1981) *enforced in part,* Union Carbide Corp. v. N.L.R.B., 714 F.2d 657, 663-64 (6th Cir. 1983) (telephone); *see also* J.C. Penney, Inc., 322 N.L.R.B. 238 (1996), *enforced*. 123 F.3d 988 (7th Cir. 1997) (employer bulletin board); Champion International Corp. 303 N.L.R.B. 102 (1991) (employer copier equipment); Churchill's Supermarkets, Inc., 285 N.L.R.B. 138 (1987), *enforced.* 857 F. 2d 1474 (6th Cir.1988) (employer telephones); Health Co., 196 N.L.R.B. 134 (1972) (public address system).

206. The unusual Sunday decision was issued on the last day of the expired term of Board Chairman Robert J. Battista. Steven Greenhouse, *Labor Board Restricts Union Use of E-Mail*, N.Y. TIMES, Dec.23, 2007, at A28, *available at* <http://www.nytimes.com/2007/12/23/us/23 labor.html>. The decision was issued three days after Chairman Battista's testimony before Congress where he rejected criticism of the Board's recent decisions. *See The National Labor Relations Board: Recent Decisions and Their Impact on Workers' Rights, Before the S. Comm. on Health, Educ., Lab. and Pensions Subcomm. on Emp. and Workplace Safety and H. Comm. on Educ. and Lab. Subcomm. on Health, Emp., Lab. and Pensions*, 110th Cong., 1st Sess. (2007) (statement of Robert J. Battista, Chairman, National Labor Relations Board), *available at* <http://www.nlrb.gov/shared_files/Press%20Releases/2007/Battista_Oral_Congressional_State ment_final_v3_12_12_07.pdf>.

207. 351 N.L.R.B. No. 70 at 5-6.

208. *Id.* at 6 n. 9; *see* Eastex, Inc. v. NLRB, 437 U.S. 556, 571-72 (1978); Hudgens v. NLRB, 424 U. S. 507, 521-23 (1976).

computer use at the workplace implicates the newspaper's managerial interest rather than its property interest. Instead, the majority adopted a legal standard for computer use policies that is substantially similar to the one applied by the Supreme Court in *Lechmere, Inc. v. NLRB* to non-employee access to employer real property: if employees have the alternative means of engaging in face-to-face solicitation, the employer is not required to permit solicitations on its computer system.[209] At the same time, the majority expressly denied that it was applying *Lechmere*.[210]

In response to the dissent's reliance on *Republic Aviation Corp*., the Board concluded that the decision was inapplicable because the newspaper's policy did not regulate oral solicitation between employees in the workplace or even the distribution of literature.[211] In addition, the majority found that because the newspaper's employees are able to interact at work, and email does not constitute their sole means of communication, the employees had adequate means to engage in protected speech in the workplace:

> [W]e find that use of e-mail has not changed the pattern of industrial life at the Respondent's facility to the extent that the forms of workplace communication sanctioned in Republic Aviation have been rendered useless and the employee use of the Respondent's e-mail system for Section 7 purposes must therefore be mandated.[212]

Based on the Board's broad embrace of employer property rights to work-related electronic communication equipment, it is likely that in future cases the same Board majority would conclude that before employees may have a Section 7 right to utilize an employer's email system, there would need to be proof of explicit, if not intentional, workplace impediments to face-to-face discussions between employees, along with evidence demonstrating that email constitutes the sole means of communication between employees. In essence, an employer computer policy can be found to be overbroad under *Register-Guard* only if it is established that the employer's oral solicitation policy is overbroad under *Republic Aviation Corp.*

Nevertheless, the Board majority's factual finding may form the basis for distinguishing *Register-Guard* in future cases involving non-

209. 351 N.L.R.B. No. 70, at 7; *see* Lechmere, Inc. v. NLRB, 502 U.S. 527 (1992); NLRB v. Babcock & Wilcox Co., 351 U.S. 105, 114 (1956).

210. 351 N.L.R.B. No. 70 at 7 n.12, 11 n.25.

211. *Id.* at 7.

212. 351 N.L.R.B. No. 70, at 7.

unionized and decentralized workplaces where email has changed the pattern of work life for employees to the extent that oral solicitation under *Republic Aviation Corp* is unavailable. In a unionized workplace, the rules relating to employee breaks are frequently the subject of collective bargaining. Through negotiations or an enforceable past practice, the newspaper's employees in *Register-Guard* may have already established contractual rights providing greater autonomy and privacy for employees communicating during breaks, thereby enhancing the rights recognized under *Republic Aviation Corp.*[213]

As part of its property rights analysis, the Board did not engage in any analysis of applicable Oregon property law to the newspaper's computer equipment. The record in *Register-Guard* demonstrates that the employer enforced its computer use policy against solicitations sent by employees from both workplace computers and computers off of the employer's premises. Despite the majority's reliance on property law concepts, it failed to reference applicable state personal property and trespass law that may have been relevant to its analysis. The Board's lack of a state and local property law analysis in *Register-Guard* is significant. When balancing an employer's property interests under *Lechmere* both the Board and the courts analyze the applicable state and local property law.[214]

The Board's ability to determine state property law questions is subject to legitimate question.[215] Whether the Board is a suitable forum for decisions on state property law questions is particularly suspect in the context of workplace electronic communications. As discussed in Part IV, both New York and California appellate courts

213. Prior to *Register-Guard*, the Board had determined that an employer must negotiate in good faith with the incumbent union prior to introducing or substantively modifying a computer use policy because it constitutes a mandatory subject of bargaining. California Newspapers Partnership d/b/a ANG Newspapers, 350 N.L.R.B. No. 89 (2007); Associated Services for the Blind Inc, 299 N.L.R.B. 1150, 1158 (1990); Susan S. Robfogel, *Electronic Communication and the NLRA: Union Access and Employer Rights*, 16 LAB. LAW. 231, 235 (2000) ("[T]here can be little doubt that employer policies on e-mail and computer use are also mandatory subjects of bargaining."). As a matter of law, *Register-Guard* does not adversely impact the duty to negotiate a computer use policy. Nevertheless, the decision will, as a practical matter, impair the ability of a union to persuade an employer to include in its computer use policy the right of the union and employees to engage in Section 7 activities.

214. *See*, *e.g.*, Snyder's of Hanover, Inc. v. NLRB, 39 Fed. Appx. 730 (3d Cir. 2002); Indio Grocery Outlet, 323 N.L.R.B. 1138 (1997), *enforced sub nom*, NLRB v. Calkins, 187 F.3d 1080 (9th Cir 1999).

215. Hirsch, *supra* note 201, at 892. Professor Hirsch has proposed that the Board and the courts discontinue rendering determinations on state property law issues and instead adopt a legal presumption that an employer's actions beyond requesting the discontinuance of non-employee Section 7 activities on employer property violate the NLRA. *Id.* at 892-93.

have reinterpreted their respective state's common law to apply it to the computer age, with New York recognizing an individual property right to stored personal emails and other electronic documents.[216]

In the guise of interpreting the NLRA, the Board majority in *Register-Guard* appears to have established a national legal standard for workplace property law applicable to employer email systems at a time when the appropriate application of personal property law to electronic communications in most states is underdeveloped.[217] This administrative creation of a national workplace property standard, if sustained on appeal, raises obvious federalism issues and may provide support for future employer supremacy challenges to state legislation recognizing broader employee rights with respect to use of workplace electronic communication systems.

In dissent, members Liebman and Walsh supported the General Counsel's argument that the newspaper's computer policy was unlawfully overbroad.[218] The dissent criticized the majority's decision for failing to follow the reasoning in *Republic Aviation Corp* and for not appreciating the breadth of the radical reorganization of the workplace as a result of email. In addition, it challenged the majority's application of a broad property law analysis to the computer use policy rather than examining the employer's management interest in the policy.[219]

The major significance of *Register-Guard* decision is not limited to the Board's upholding of the newspaper's computer use policy. The majority also took the opportunity to alter substantially the applicable Board analysis with regard to claims of unlawful discriminatory enforcement of employer anti-solicitation policies. Before considering this new analysis, it is important to consider the standard applied by the Board in earlier discrimination cases.

Prior to *Register-Guard*, it was largely accepted that an employer policy or practice which permitted personal or other non-work related workplace communications utilizing employer property while prohibiting union-related communications constituted unlawful

216. Thyroff v. Nationwide Mut. Ins. Co., 460 F.3d 400 (2d Cir. 2006); *see also* Fashion Valley Mall LLC v. NLRB, 451 F.3d 241 (D.C. Cir. 2006); Fashion Valley Mall LLC v. NLRB, 172 P.3d 742 (Cal. 2007) (answering a certified state law question from an federal appellate court examining a challenge to a Board decision regarding Section 7 activities in a private mall).

217. In *Fashion Valley Mall*, 172 P.3d at 742, the California Supreme Court recently answered a certified state law question relating to that state's law from a federal appellate court examining a challenge to a Board decision. *See Fashion Valley Mall*, 451 F.3d at 241.

218. 351 N.L.R.B. No. 70, at 14.

219. *Id.* at 15, 17-18.

discrimination under the NLRA. For example, the Fourth Circuit Court of Appeals in *Media General Operations Inc. v. NLRB*[220] upheld a Board decision[221] that concluded that an employer's discriminatory enforcement of its computer use policy was unlawful. The case involved an unfair labor practice charge filed against a Virginia newspaper for prohibiting union representatives from using the newspaper's computer system for union business.[222] The human resources director announced the prohibition at a collective bargaining session.[223] The newspaper's computer use policy expressly prohibited employees from sending emails that were unrelated to the newspaper's activities. Like the facts in *Register-Guard*, the newspaper tolerated employee use of its computer system for circulation of non-business related topics.[224] Based on the newspaper's lax enforcement of its computer use policy against non-business related emails such as personal emails, the NLRB held that the prohibition against union related emails constituted unlawful disparate treatment in violation of the NLRA.[225]

Similarly, in *NLRB v. Honeywell, Inc.*,[226] the Eighth Circuit enforced a Board decision[227] that concluded that an employer's blanket policy prohibiting union materials on the employer's bulletin board was discriminatory under the NLRA because the company permitted employees to post other non-business related materials.[228]

220. 225 Fed. Appx. 144 (4th Cir.), *cert. denied sub nom.*, Richmond Newspapers Prof'l Ass'n v. Media Gen. Operations, Inc., 128 S. Ct. 492 (2007).

221. Media General Operations, Inc., 346 N.L.R.B. 74 (2005).

222. *Media Gen. Operations, Inc*., 225 Fed. Appx. at 146.

223. *Id.* at 146-47.

224. *Id.* at 146.

225. *Id.* at 148; *see also* Adtranz, ABB Daimler-Benz Transportation, N.A. Inc., 331 N.L.R.B. 291 (2000), e*nforced in part sub. nom.*, Adtranz ABB Daimler-Benz Transportation, N. A. v. N.L.R.B., 253 F. 3d 19 (D.C. Cir. 2001) (reaching a similar conclusion against an employer that maintained a broad ban on non-business use of the employer's computer communication system but permitted employees to use the employer's instant messaging system to communicate with each other about both work and non-work related matters); E.I. DuPont & Co., 311 N.L.R.B. 893, 919 (1993) (finding a violation when an employer maintained a discriminatory rule in a chemical plant that prohibiting the use of the e-mail system for the distribution of union literature, but permitted employer dominated safety committees to utilize the system to communicate with employees and allowed the email system to be used to distribute jokes, poems and comments on various non-work related subjects.); County of Onondaga, 33 N.Y. Pub. Emp. Rep. ¶4599 (2000) (finding public employer unlawfully transferred union president in retaliation for the distribution of an email to unit members regarding a pending grievance.)

226. 722 F.2d 405 (8th Cir.1983).

227. Honeywell, Inc., 262 N.L.R.B. 1402 (1982).

228. *Honeywell, Inc.*, 722 F.2d at 406-07; *see* Container Corp. of America, 244 N.L.R.B. 318 (1979).

In *Register-Guard*, the Board jettisoned its prior standards for establishing discriminatory enforcement of anti-solicitation policies and replaced it with a higher legal standard previously applied by the Seventh Circuit in two cases denying enforcement of certain aspects of Board orders.[229] Without explicit reference to the body of relevant Board decisions, including the Fourth Circuit's recent decision in *Media General Operations Inc. v. NLRB*, the Board concluded that the Seventh Circuit's analysis was more persuasive than the remaining body of relevant case law.[230]

Under the newly adopted Board standard, in order to constitute unlawful discrimination under the NLRA, the disparity of treatment "must be along Section 7 lines. In other words, unlawful discrimination consists of disparate treatment of activities or communications of a similar character because of their union or other Section 7-protected status."[231] Under this narrow standard, only disparate treatment with respect to activities similar to the exercise Section 7 rights can constitute unlawful discrimination under the NLRA. There is one major exception to this rule, however: the employer can use the computer system to distribute anti-union messages without any requirement that it permit employees or the union to respond.[232]

The standard adopted in *Register-Guard* allows employers to permit employees to engage in various forms of personal email while at the same time explicitly prohibiting email solicitation among employees regarding organizations, including the employees' union. As long as the employer does not permit the use of the email system for solicitations for another group or organization, it may lawfully prohibit solicitations for a labor union.

Based on the new standard, the Board held that the newspaper in *Register-Guard* lawfully disciplined the union president under the computer use policy for sending the two August emails from the

229. The Guard Pub. Co. d/b/a/ Register Guard, 351 N.L.R.B. No. 70, at 8-10 (Dec. 16, 2007) (S 36-CA-8743-1, 36-CA-8849-1, 36-CA-8789-1, & 36-CA-8842-1); *see* Fleming Co. v. NLRB, 349 F.3d 968 (7th Cir. 2003); Guardian Industries Corp. v. NLRB, 49 F. 3d 317 (7th Cir. 1995). As Professor Hirsch has noted, Judge Posner's recent analysis in *St. Margaret Mercy Healthcare Centers v. NLRB*, 519 F.3d 373 (7th Cir 2008), regarding discriminatory application of an anti-solicitation policy may constitute a potential conflict with the analysis applied in the earlier Seventh Circuit decisions relied upon by the Board. Jeffrey Hirsch, Is the Seventh Circuit Backing Off of Its Discriminatory Solicitation Rule?, March 12, 2008, *available at* <http://lawprofessor.typepad.com/laborprof_blog/2008/03/is-the-7th-circ.html>.

230. *Register Guard*, 351 N.L.R.B. No. 70, at 9.

231. *Id.* at 9.

232. *Id.* at 9 n.17.

union's off-site office computer to union members because there was no evidence in the record that the newspaper engaged in discrimination along Section 7 lines with respect to similar forms of organizational solicitation. The Board reasoned that although the newspaper permitted personal email, the record did not include evidence demonstrating that it permitted employees to solicit support for other groups or organizations. In a footnote, the Board conceded, however, that there was no evidence that employees in the past had ever solicited other employees for another organization.[233]

Notably absent from the Board's discrimination analysis was the fact that the union president's August emails were not sent from a workplace computer. In applying its new standard, the Board did not discuss the newspaper's practices with respect to employees receiving external email solicitations from organizations other than the incumbent union.

It remains unclear whether and how the Board's new standard will be applied to mutual aid and protection cases involving unorganized employees who utilize an employer's computer system to discuss working conditions. For example, if employees are permitted to discuss weather conditions via email but are prohibited from discussing working conditions, are the weather condition emails sufficiently similar in character to constitute evidence of discrimination along Section 7 lines?

Board member Liebman noted in her recent article that the same "Board majority has chosen a very confined view of 'concerted' activity for the purpose of 'mutual aid and protection'" under Section 7.[234] The Board's narrow view of protected activity was exemplified in *Amcast Automotive of Indiana, Inc*.[235] In that case, the Board majority dismissed an unfair labor practice complaint challenging the termination of an employee who, along with another employee, had spent less than thirty minutes over a two day period conducting an internet search on a workplace computer regarding another company engaged in negotiations to purchase the employer.[236] The Board concluded that although the internet search constituted concerted activity under the NLRA, it was not protected because it was

233. *Id.* at 10 n.24.
234. Liebman, *supra* note 38, at 583.
235. 348 N.L.R.B. No. 47 (Sept. 29, 2006).
236. *Id.* at 2.

insufficiently linked to working conditions.[237] Based on such a confined view of concerted activity, it may be very difficult under the *Register-Guard* standard to establish unlawful discrimination in mutual aid and protection cases.

One of the many Board decisions that were not cited or distinguished in *Register-Guard* is *Timekeeping Systems, Inc.*[238] In that decision, the NLRB concluded that an employee's responsive email to the employer and co-workers regarding a proposed change in a term and condition of employment constituted concerted protected activity under the NLRA.

In *Timekeeping Systems Inc.,* the chief executive officer of a small Ohio company, Barry Markwitz, sent an email to all employees with an attached memorandum setting forth proposed changes to the company policy regarding vacation schedules.[239] Under the proposal, the company would shut down during Christmas week and current paid vacation days would be adjusted accordingly. The cover email and memorandum specifically solicited input from employees regarding the proposed changes. The memorandum stated "Please give me your comments (send me e-mail or stop in to talk to me) by Tuesday, 12/5."[240]

After an employee responded with an email to chief executive officer and all other staff praising the proposed changes, another employee, Larry Leinweber, responded that he did not think the proposal was in the employees' best interest. The following day, Leinweber sent a much longer email to Markwitz and the entire staff setting forth his belief that Markwitz's justifications for the proposed policy changes were false. Based on Leinweber's second email, the other employee sent another email, indicating that based on the new information provided by Leinweber he was withdrawing his support for the employer's new policy.[241]

As the direct result of Leinweber's second lengthy email, he was fired.[242] Leinweber pursued an unfair labor practice charge and prevailed. The Board concluded that Leinweber's email to both Markwitz and the other employees was concerted activity and therefore protected by the NLRA, because the Board viewed it as an

237. *Id.* at 3-4.
238. 323 N.L.R.B. 244 (1997).
239. *Id.* at 245-46.
240. *Id.* at 246.
241. *Id.*
242. *Id.* at 247.

attempt to gain support among co-workers for his opposition to the proposed changes in the vacation policy. Therefore, the termination was unlawful retaliation for activity protected by the statute.[243]

The reverberations of *Register-Guard* will be felt primarily in non-union workplaces like Timekeeping and particularly when employees are seeking to organize into a union under the NLRA. This article next examines Board case law prior to *Register-Guard* relating to the use of email in the context of Board supervised elections.

In *Lockheed Martin Skunk Works*, the Board rejected exceptions to an election based on the disparity between the amount of anti-union email and pro-union email permitted on the employer's computer system.[244] In *Register-Guard*, the majority cited this type of disparity as constituting the epitome of unlawful discrimination without referring to its decision in *Lockheed Martin Skunk Works*.[245] In *Lockheed Martin Skunk Works*, however, the Board ruled that the disparity between anti-union and pro-union emails on the employer's computer system was an insufficient basis to set aside an election. The Board concluded the union itself was responsible for the disparity based on its preference for traditional hard copy campaign materials. In support of that conclusion, the Board majority cited to the fact that the union sent only one mass email after the employer had granted the union the opportunity to send three.[246]

In *Trustees of Columbia University*, a union seeking to represent a crew of maritime employees adopted a far more pro-active stance relating to the use the employer's computer system to reach employees during a representation election campaign.[247] During the pre-election hearing, the union requested that the NLRB direct the employer to provide a list of employee workplace email addresses as part of its requirement to provide names and home addresses of employees pursuant *Excelsior Underwear, Inc.*[248] The purpose of the

243. *Id.* at 247-51; *see also* Electronic Data Systems Corp., 331 N.L.R.B. 343 (2000); *cf.* Wash. Adventist Hosp., 291 N.L.R.B. 95 (1998) (finding discharged employee was not engaged in protected concerted activity when his e-mail critical of management was for his own purposes and was inappropriately disruptive of the hospital's mission of patient care, because he chose to use a procedure that ceased all other computer-facilitated communications at a peak usage time in order to have his message receive the immediate attention of all hospital personnel who used the workplace computers).

244. 331 N.L.R.B. 852, 854 (2000).

245. The Guard Pub. Co. d/b/a/ Register Guard, 351 N.L.R.B. No. 70, at 9 (Dec. 16, 2007).

246. *Lockheed Martin Skunk Works*, 331 N.L.R.B. at 854-55.

247. 350 N.L.R.B. No. 54 (2007).

248. *Id.* at 1; *see* Excelsior Underwear, Inc., 156 N.L.R.B. 1236 (1966).

Excelsior list is to ensure that both the employer and union have the opportunity to provide employees with information to assist the employees in making an educated decision regarding union representation.[249] In this case, the employees were going to be at sea during the course of the campaign and would not be able to receive mail at home. While at sea, they would be using the employer's email system to send and receive personal email.[250] After the union lost the election, it filed objections to the election on the ground that the employer had failed to provide the requested workplace email addresses.[251]

In denying the union's objections to the election in *Trustees of Columbia University*, the Board noted that there was no existing precedent that would require an employer to provide a list of email addresses as part of its duty to comply with *Excelsior*.[252] In addition, the majority found that based on the union's experience in representing maritime employees, along with the knowledge that it gained in seeking to organize this vessel, it should not have agreed to an election schedule that would have included the period when the ship would be seaward.[253]

It remains to be seen whether the Board's current approach to computer use policies and practices will be upheld in court or sustained administratively and legislatively in the next few years. On the administrative level, there remain a number of additional unanswered legal issues stemming from *Register-Guard* that will have to be resolved by the Board and the courts in future cases:

1) whether an employer can apply a computer use anti-solicitation policy to employee owned electronic communication devices while on break inside an employer's premises or vehicle;

2) whether an employer can prohibit union solicitations when employees receive other organization solicitations on personal hotmail or yahoo accounts accessed at the workplace during breaks;

3) whether the use of monitoring software targeted at non-work related email can constitute unlawful surveillance under the NLRA;[254]

249. Mod Interiors, 324 N.L.R.B. 164 (1997).

250. *Trs. of Columbia Univ.*, 350 N.L.R.B. No. 54, at 1.

251. *Id.* at 2.

252. *Id.* at 2-3.

253. *Id.* at 3.

254. The applicable standard for unlawful surveillance applied by the current Board was recently restated in *Sprain Brook Manor Nursing Home, LLC*, 351 N.L.R.B. No. 75 (2007):

> Although an employer may observe open union activity on or near its property,

4) whether an employer can prohibit employees from reading union-related email or accessing union-related websites while permitting such activities relating to other organizations;

5) whether an employer can lawfully require employees to take affirmative steps to be removed from a union listserv while permitting employees to receive emails from other listservs; and

6) the impact of potential future state laws regulating employer computer use policies.

The current legal challenge to the Board's decision in *Register-Guard* will result in the further development of the law with respect to workplace computer use policies and practices under the NLRA. Applying a keen strategic sense, the newspaper company filed a petition for review to the Board's order in the Court of Appeals for the District of Columbia[255] less than two weeks after the Board's decision, thereby avoiding the decision being reviewed by the Ninth Circuit, an appellate body that has been particularly active in the area of employee workplace computer use law.[256]

The D.C. Circuit may have to determine a number of fundamental legal issues stemming from the Board's decision including: 1) whether the Board properly applied Supreme Court precedent when it balanced the employer's property interest, rather than its managerial interest, in finding the newspaper's computer use anti-solicitation policy lawful; 2) if the employer's property interest is implicated, does the Board have the constitutional or statutory authority to create a nation-wide workplace property doctrine; 3) if not, should the federal court or Oregon's highest court determine state property law issues involving computer use; and 4) whether the Board set forth a sufficient rationale for overruling its earlier

> "an employer may not do something 'out of the ordinary' to give employees the impression that it is engaging in surveillance of their protected activities."

Id. at 2 (citing London Steel, Inc., 340 N.L.R.B. 307, 313 (2003). If this standard is applied in future email cases under the NLRA, the Board may have to determine whether union-related email on an employer's computer constitutes open union activity and whether it is "out of the ordinary" for the employer to monitor the subject matter of employee email thereby creating the impression of surveillance of protected Section 7 activities.

255. *Guard Publishing Co v. NLRB*, Court of Appeals Docket No. 07-1528 (D.C. Cir. Dec. 26, 2007). The Board cross-petitioned for enforcement and the Eugene Newspaper Guild has intervened. Consistent with a May 2, 2008 scheduling order, the consolidated cases will be ready for argument in the D.C. Circuit in September 2008.

256. *See*, *e.g.*, U.S. v. Heckenkamp, 482 F.3d 1142, 1145 (9th Cir. 2007); U.S. v. Greiner, 235 Fed. Appx. 541 (9th Cir. 2007); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); *see also* Neil A. Lewis, *Rebels in Black Robes Recoil At Surveillance of Computers*, N.Y. TIMES, Aug. 8, 2001, *available at* <http://query.nytimes.com/gst/fullpage.html?res=9C02E1DA163FF93BA3575BC0A9679C8B63&scp=1&sq=&st=nyt>.

precedent in discrimination claims.

Finally, *Register-Guard* may spur efforts in Congress, in conjunction with other current efforts to amend the NLRA, to enact legislation to provide greater employee rights with respect to the use of workplace computers for Section 7 activities.

VI. CONCLUSION: A TIME TO BRING INTEGRITY TO THE ELECTRONIC WORKPLACE

In his examination of the concept of integrity, Yale Law Professor Stephen L. Carter identified three core elements that lead to integrity: a) distinguishing between right and wrong through discernment; b) acting on what has been discerned even at a personal cost; and c) stating openly that you are acting based upon your discernment.[257]

There has not been a great deal of integrity in responding to the extraordinary electronic transformation of the American workplace. Very few employers, unions and employees spend time considering what is "right" and what is "wrong" when it comes to email and internet use in the workplace. If any form of examination takes place, it is usually focused on self-interest and perceived, arguable, or actual legal rights.

Email is frequently justified as a means of improving workplace communications and productivity. However, there is infrequent consideration of the negative complications associated with overuse of email: expansion of the contours of the workday and workplace; inadvertent miscommunication; wide distribution to unanticipated recipients; and potential addiction. Examining workplace email habits and the negative impact such habits can have on interpersonal relationships does not appear to be a high priority.

During a panel discussion at a New York bar association meeting a number of years ago, an employment attorney for a large computer company stridently advocated against the concept that employees should be permitted to use workplace computers for personal use. Nevertheless, in response to a question, the company's attorney freely admitted that he used his own workplace computer for personal purposes. In many ways, the inherent contradiction in the attorney's comments is emblematic of the confused state of expectations in the electronic workplace.

257. STEPHEN L. CARTER, INTEGRITY 7 (1995).

As demonstrated above, employers have many practical and legal incentives to promulgate and enforce computer use policies. Nevertheless, the workplace reality is that such policies are breached on at least a daily basis, if not more often. Both line employees and supervisors justify such work rule violations based on their own subjective needs. Few are willing to recognize or admit that their electronic workplace conduct may be inappropriate, but will be quick to criticize others for the same activities.

With the growing decentralization of the workplace along with the expansion of large private commercial malls and office complex parks, unions and activists are embracing email and the internet as a contemporary necessity to communicate with employees at workplaces.[258] In utilizing or demanding to utilize employer email systems, however, some unions and activists do not sufficiently analyze the numerous practical problems and costs connected with such use.

In many workplaces, union-related communications between employees need to remain clandestine in order to be effective. This is particularly true in unorganized settings. Nevertheless, the concept of a covert email communication on an employer's computer system is an oxymoron. Union-related email, like all email, can be easily forwarded. Union-related email can be forwarded by an unsympathetic employee to the employer's human resources department.

Moreover, a union's use of unsolicited workplace email during an initial organizing campaign can backfire by alienating or frightening employees who may fear potential adverse action based on the employer's policies and practices. Employers have the right under the ECPA to monitor email traffic on their computer systems along with emails automatically stored on their servers. To compound these potential adverse costs, new ediscovery rules and regulatory requirements can result in unanticipated third party disclosure of cyber-based organizing campaign tactics.

Based on the holding in *Register-Guard*, as well as cases enforcing employer email and surveillance policies, there is an increased vulnerability for employees who may be deemed electronically supportive of an organizing campaign by reading and/or responding to union electronic solicitation. Without necessary and

258. Hirsch, *supra* note 184.

appropriate precautions, union-related email and unguarded internet postings can lead to inadvertent or intentional employer knowledge of protected activities with related risk of terminations and other adverse actions resulting from that knowledge. The ability to prove and thereby remedy such discrimination at the NLRB is substantially diminished by the remote nature of the employer's computer-based surveillance. As noted *infra*, it remains to be seen how the standards for unlawful employer surveillance will be applied to electronic monitoring of union-related activities on workplace computers.

Many employer policies explicitly permit intermittent personal use. As a practical matter, permitting such intermittent personal use places both employers and employees in a quandary. For employers, permitting personal use can lead to a decline in productivity, complaints, possible litigation, and the necessity of imposing a vigilant monitoring program. Although the *Register-Guard* decision has the effect of empowering employers to permit non-work related computer use without opening the door to a statutory requirement to permit union related email, the decision leaves open the sometimes difficult task of determining whether the content of a particular email may be deemed similar to Section 7 communications to form the basis for unlawful discrimination. If the Board applies the *Register-Guard* rationale to mutual aid and protection cases, employers may have to engage in more extreme forms of email monitoring of intermittent use to avoid future claims of discrimination. At the same time, denying intermittent use is impractical because it can cause demoralization and may render it difficult for employers to recruit younger qualified employees who may expect broad computer access.

Many employees remain under the illusion that the content of their workplace emails and internet use are private. Although employers may have reserved the right to access and monitor, the incivility attached to an employer, or an attorney involved in litigation regarding the employer, reading the content of an electronic communication intended to be private is rarely the subject of discussion.

One possible means of establishing an integrity-based solution regarding employee email use is through technological segregation. The establishment of a policy permitting employees to utilize encryption regarding the content of email intended to be private may provide a means for balancing the needs of both an employer and employee. Under such a policy, a specific time period could be

defined when non-work related email is permissible. The use of encryption would constitute notice from the employee to the employer that the email is not job-related. In exchange for this notice, the policy would insure that the employer would not access the content of the email except under extreme or exigent circumstances and with notice to the employee. For employers, an encryption program would provide an easy means both to keep track of the amount of time spent by employees on email unrelated to work and to retain the right to engage in limited monitoring.

At present, employers retain wide legal rights and discretion in imposing and applying computer use policies. To bring integrity to the law of the electronic workplace, there needs be a societal discussion about changing the current state of the law to meet both the needs of employers and the expectations of employees. Obviously, such a dialogue aimed at establishing a balanced approach cannot take place in an atmosphere where various opposing interests in our society maintain impractical absolutist perspectives. Similarly, reliance on Fourth Amendment precedent stemming from child pornography prosecutions or Nineteenth century concepts of property law do not provide a meaningful framework for a reasoned societal discussion about the electronic workplace.

Despite the ubiquitous nature of email, in the twenty-two years since the enactment of the ECPA, Congress has not amended the law to alter the provisions relating to the workplace. Nor has there been a meaningful congressional debate about the state of applicable labor and employment law in the computer age. In contrast, both Congress and state legislatures have been active in establishing prohibitions against spam and other fraudulent and deceptive email practices.[259] There needs to be a similar substantive examination of both the federal and state laws regarding email and internet use in the workplace.

One area of reexamination should be on the subject of placing a prohibition or limitations on an employer's remote monitoring of personal computers that are attached or integrated into a network system. In general, privacy protections are strongest in one's home under the Fourth Amendment, but the Fourth Amendment is inapplicable to private employers. Under the consent provisions of the ECPA, however, an employer can lawfully impose an obligation

259. Theodore A. Olsen, *The Dangers of E-Mail Recruiting: One Peron's "Sales Pitch" Is Another Person's "Spam,"* 23 LAB. LAW. 163, 165-77 (2007).

on employees to grant the employer the ability to remotely monitor activities on a personal computer or a PDA integrated with th**e** employer's computer.

Based on the rapid changes in the structure of the workplace and the workday, there needs to be consideration of legislation aimed at ending the current imbalance in the law granting employers the power to monitor employees based on union-related and other lawful computer activities whether or not the employee is even using a the workplace computer.[260] In addition to the NLRA, there are many state laws that limit the ability of employers to take adverse action against employees for their outside or leisure activities. Placing express statutory limitations on the scope of employer electronic surveillance of such activities would enhance the substantive rights granted by those statutes.

As part of any discussion aimed at reexamining American labor law in the context of the electronic workplace, there needs to be careful consideration of the legitimate managerial and legal interests of employers, the collective and individual rights granted employees under the NLRA and other laws, as well as other interests including the desire for what Justice Brandeis deemed "the right to be let alone – the most comprehensive of rights and the right most valued by civilized men."[261]

The continued development of the electronic workplace has great potential for enhancing economic prosperity. At the same time, until practical and legal measures are instituted aimed at balancing the respective interests in the workplace, employees utilizing workplace computers to engage in lawful activities may have to remain honest while their personal and organizational email and internet activities continue to live outside the law.

260. Randall Stross, *How to Lose Your Job on Your Own Time*, N.Y. TIMES, Dec. 30, 2007, § 3, at 3.

261. Olmstead v. U.S., 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).