ELECTRONIC PRIVACY AND EMPLOYEE SPEECH

PAULINE T. KIM*

INTRODUCTION

The concept of "privacy" has been invoked to protect a variety of distinct interests in the workplace, such as employees' interests in maintaining their bodily integrity, avoiding intrusion on physical spaces, protecting against the seizure of personal items, preventing disclosure of personal information and ensuring individual autonomy.[1] Employees have asserted the right to withhold certain types of sensitive information, or to avoid intrusive scrutiny into private matters by their employers. Employers claim an interest in knowing more about their employees and how they are spending their time in order to avoid liability and ensure productivity. The conflict between these competing interests has only sharpened with advancing technology that has made it easier and cheaper for employers to monitor and collect information about their employees.

Although technological change raises many different types of privacy issues in the workplace,[2] this Essay focuses on a narrower set of interests—

* Charles Nagel Professor of Law, Washington University School of Law. An earlier version of this paper was presented as the Kenneth M. Piper lecture at the Chicago-Kent College of Law in April 2011. Special thanks to my colleagues Marion Crain and Neil Richards for conversations about these issues over the years and for very helpful comments on this paper. Thanks also to Lauren Abbott, James Ayden and William Osberghaus for research assistance.

1. *See,e.g.*, MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW (3rd ed. 2009) (cataloging variety of employee interests under the concept of "privacy"). As many commentators have observed, the concept of "privacy" is a capacious one, often invoked in a variety of seemingly unrelated situations. *See, e.g.*, DANIEL J. SOLOVE, UNDERSTANDING PRIVACY (2008).

2. For example, advances in genetics mean that increasingly detailed information about an individual's current health conditions and future medical risks can be gleaned from her genetic material, raising questions about whether or when employers should be allowed to collect and use that information. *See* Pauline T. Kim, *Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace*, 96 NW. U. L. REV. 1497 (2002). Congress responded to those challenges by passing the Genetic Information Nondiscrimination Act of 2008 (GINA), Pub. L. No. 110-233, 122 Stat. 881 (codified as amended in scattered sections of Title 26, 29, and 42 of the U.S. Code). Even if laws such as GINA prohibit employers from requesting certain types of sensitive information, there is a risk that employees may come to feel pressure to self-disclose detailed personal information in order to avoid negative inferences. *See* Scott R. Peppet, *Unraveling Privacy: The Personal Prospectus and the Threat of a Full Disclosure Future*, 105 NW. U. L. REV. 1153 (2011).

Although these and other types of privacy issues may also be affected by the developments discussed in this Essay, it focuses on employees' claims to electronic privacy because it is in this area that the impact of the evolving workplace and changing technology is greatest, and that the connection with protected employee speech interests is most significant.

what I call electronic privacy—and its relationship to employee speech. By "electronic privacy" I refer to employees' asserted interest in using various forms of electronic media—email, cell phones, social networking sites, and the internet—to communicate or to receive information free from employer scrutiny. As the use of electronic devices has proliferated, employees' electronic communications have increasingly come under the scrutiny of their employers, even when those communications are about purely personal matters unrelated to work and even when those communications occur off duty. Employers have retrieved and read highly personal communications among intimates sent over work-provided equipment.[3] They have disciplined or fired workers because of comments they posted on Facebook, or in private chat groups, even when the communications occurred off duty using the employees' home computers.[4] In other cases, employers have seized personal passwords or used forensic techniques to access email exchanged on employees' personal email accounts.[5]

As these and other incidents suggest, the norms surrounding whether or when employees can expect privacy in their communications are highly uncertain. The traditional approach of protecting purely personal matters, while allowing employer scrutiny of work-related activities is proving unworkable. Changes in the organization of work and changes in technology are increasingly blurring the boundary between professional and private life.[6] At the same time, technological advances are making it easier for employers to capture ever more detailed and comprehensive information

3. *See,* City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

4. NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (12–31), Jan. 24, 2012 (updating earlier report by describing additional cases concerning employees' use of social media and employers' social medial policies and rules); NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (11–74), Aug. 18, 2011 (describing recent claims of interference with protected rights based on employees' use of social media and Board responses). *See also* Melanie Trottman, *Workers Claim Right to Rant on Facebook*, WALL ST. J., Dec. 2, 2011, at B1 (explaining that more than 100 charges have been filed with the NLRB by employees alleging that they were terminated because of their communications on social media sites).

5. *See, e.g.*, Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002); Pietrylo v. Hillstone Rest. Group, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009); Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006); Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914, 926 (W.D. Wis. 2002); Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010).

6. *See, e.g.*, Patricia Sanchez Abril, Avner Levin & Alissa Del Riego, *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee*, 49 AM. BUS. L. J. 63, 64 (2012); Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461 (2012); Robert Sprague, *Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship*, 50 U. LOUISVILLE L. REV. 1 (2011), *available at* SSRN: http://ssrn.com/abstract=1773049; Robert Sprague, *Orwell was an Optimist: The Evolution of Privacy in the United States and Its De-evolution for American Employees*, 42 J. MARSHALL L. REV. 83 (2008).

about their employees' communications and activities on and off duty.[7] Current privacy law doctrine is ill-equipped to address these developments and, as a result, many commentators have argued that employee privacy is insufficiently protected in the electronic workplace.[8]

The extent to which the law *should* intervene in the employment relationship to protect employee privacy is highly contested. However, advocates on both sides of the debate have largely overlooked a significant related development—namely, the extent to which the law protects certain socially valuable forms of employee speech. Although the law does not generally guarantee free speech for employees in the workplace, it does carve out special areas of protection. Section 7 of the National Labor Relations Act, for example, protects workers' rights to speak collectively, guaranteeing the right to engage in concerted activity for the purpose of mutual aid or protection.[9] In addition, as the law has stepped in to regulate the workplace in various ways, it has also extended protection to employees who speak up to enforce those laws. For example, Title VII not only forbids employment discrimination, it also prohibits employers from retaliating against an employee who complains about discrimination.[10] Other legal developments reflect the belief that employees have a critical role to play in exposing public corruption and corporate wrong-doing. Courts and legislatures have increasingly extended protections to whistleblowers who report illegal or unethical conduct by their employers,[11] most recently in an effort to deter corporate wrongdoing that has undermined confidence in the financial system.[12]

7. *See, e.g.*, Dennis R. Nolan, *Privacy and Profitability in the Technological Workplace*, 24 J. OF LAB. RES. 207 (2003).

8. *See, e.g.*, Abril, et al., *supra* note 6, at 95; William A. Herbert. *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 EMP. RTS. AND EMP. POL'Y J. 49 (2008); Nolan, *supra* note 7; Sprague, *supra* note 6.

9. 29 U.S.C. § 157 (2006).

10. 42 U.S.C. § 2000e-3(a) (2006).

11. As state courts began to recognize the common law claim of wrongful discharge in violation of public policy, some extended it to protect employees fired for whistleblowing activities, particularly when public health or safety was involved. *See, e.g.*, White v. General Motors Corp., 908 F.2d 669, 671 (10th Cir. 1990); Garibaldi v. Lucky Food Stores, 726 F.2d 1367, 1375 (9th Cir. 1984); Sheets v. Teddy's Frosted Foods, 427A.2d 385, 389 (Conn. 1980); Boyle v. Vista Eyewear, 700 S.W.2d 859, 878 (Mo. Ct. App. 1985). In other states, the legislature stepped in to protect certain types of employees for certain types of whistleblowing speech. For a comprehensive overview of statutory whistleblower protections, see DANIEL P. WESTMAN & NANCY M. MODESITT, WHISTLEBLOWING: THE LAW OF RETALIATORY DISCHARGE (2d ed. 2004 & Supp. 2009).

12. Congress extended whistleblower protections to some private sector employees in the Sarbanes-Oxley Act of 2002, 18 U.S.C. § 1514A(a) (2006) and further expanded these protections in the Dodd-Frank Act of 2010. *See* Tammy Marzigliano & Cara E. Greene, *The Dodd-Frank Act's Whistleblower Provisions: The Act's Best Hope for Exposing Financial Wrongdoing*, 8 WORKPLACE L. REP. 1507 (2010) (explaining that whistleblower provisions of Dodd-Frank Act attempt to address the short-

These two developments—weak protection for employee's electronic privacy and increased protection for some socially valued forms of employee speech—are at odds because privacy and speech are closely connected. Although the law has often assumed that privacy and speech rights exist in tension with one another,[13] scholars have recently pointed out that these values are in many ways consistent, even mutually reinforcing.[14] They argue that some forms of privacy protection *promote* speech values by granting individuals space to explore and test new ideas, and to associate with like-minded others—activities that are often precursors to speech that is valuable in the public sphere.[15] In the context of the workplace, these insights suggest that socially valued forms of speech may be less likely to be produced without some privacy for employees to explore ideas and communicate with others. Ironically, then, the law is simultaneously expecting more from employee speech and protecting employee privacy less, even though some measure of privacy protection may be necessary to support speech.

This Essay proceeds as follows: Part I discusses how protection of employee privacy under current law rests on a distinction between personal and work-related matters, and explores the ways in which changes in the organization of work and changes in technology are blurring that boundary. Part II briefly surveys the limitations of existing law in protecting employee privacy given these developments. In Part III, I turn to a consideration of employee speech interests, exploring how the law currently recognizes and protects certain socially valued forms of employee speech—namely, collective speech, and speech necessary to enforce workplace regulation and to report and deter corporate wrong-doing. The connection between these protected forms of employee speech and employees' interest in privacy is explored in Part IV. Drawing on theories about the importance of privacy in fostering speech and participation in public discourse, I argue that some

comings of the whistleblower protections of the Sarbanes-Oxley Act and to broaden the application of those protections).

13. In a number of cases, the Supreme Court has rejected privacy claims based on the First Amendment rights of the speaker to publish arguably private information. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 527–30 (2001) (holding that disclosures by media of illegally intercepted communications on matters of public concern are protected by First Amendment); Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989); Smith v. Daily Mail Publ'g, 443 U.S. 97, 103–04 (1979); Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494–95 (1975); Time, Inc. v. Hill, 385 U.S. 374, 396–97 (1967). *Cf.* Cohen v. Cowles Media, Co., 501 U.S. 663, 670 (1991) (holding that First Amendment does not bar promissory estoppel claim against newspaper for revealing identity of a source promised confidentiality).

14. *See, e.g.*, Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999); Sean M. Scott, *The Hidden First Amendment Values of Privacy*, 71 WASH. L. REV. 683 (1996).

15. *See, e.g.*, Richards, *supra* note 14, at 403–04.

measure of workplace privacy is necessary to encourage socially valued forms of employee speech. The last Part concludes.

I. BLURRING BOUNDARIES

A. Distinguishing the Personal and the Professional

Although the relevant doctrine for analyzing employee claims of invasion of privacy by their employers depends upon the type of intrusion and the type of workplace,[16] as a general matter, the law roughly tries to distinguish personal from work-related matters. Public employees receive some protection for personal privacy from the Constitution, particularly the Fourth Amendment guarantee against unreasonable searches and seizures.[17] This inquiry has been framed in terms of whether an employee has a "reasonable expectation of privacy" in the matter intruded upon. The leading case, *O'Connor v. Ortega*,[18] considered the claims of a public employee that his Fourth Amendment rights were violated when his employer searched his office, desk and file cabinets. Although the Supreme Court concluded that the Fourth Amendment restrains government employers, it held that its prohibitions apply only if the employer's actions "infringe[] 'an expectation of privacy that society is prepared to consider reasonable.'"[19] According to a plurality of the Court, the goal is to distinguish "the workplace context"—that is, "those areas and items that are related to work and are generally within the employer's control,"[20]—from personal matters not part of that context—for example, the contents of closed luggage or a

16. In addition to the constitutional and common law doctrines discussed in the text, a variety of state and federal statutes protect against specific types of privacy invasions and many of these turn on the type of workplace as well as the type of intrusion. For a comprehensive list of statutes regulating privacy interests in employment, *see* FINKIN, *supra* note 1, at 615–971. These statutes vary considerably in the extent to which they protect employee privacy, and in many instances, the interests protected are quite narrow. *See, e.g.*, CONN. GEN. STAT. ANN. § 31-40s (West 2011) (prohibiting discrimination against employees who smoke or use tobacco outside the workplace and off duty). Nevertheless, they reflect legislative judgments about which matters are sufficiently personal to the employee that they should not be subject to employer scrutiny.

17. O'Connor v. Ortega, 480 U.S. 709 (1987) (holding that the Fourth Amendment constrains government employers). Some lower federal courts have also found the constitutional interest "in avoiding disclosure of personal matters" that derives from the Fourteenth Amendment, *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977), to apply in the employment setting. *See, e.g.*, Denius v. Dunlap, 209 F.3d 944 (7th Cir. 2000); Fraternal Order of Police v. City of Philadelphia, 812 F.2d 105 (3d Cir. 1987). The Supreme Court recently rejected such a privacy claim brought by employees of a government contractor. NASA v. Nelson, 131 S. Ct. 746 (2011). In doing so, it "assume[d], without deciding" that such a privacy right is protected by the Constitution, but concluded that the background check challenged by the plaintiffs did not violate that right. *Id.* at 751.

18. 480 U.S. 709 (1987).

19. *Id.* at 715.

20. *Id.* at 715.

purse brought to work by an employee.[21] The "reasonable expectation of privacy" test was thus intended to delineate legitimate employee claims of privacy by distinguishing the personal from the work-related.

Determining that a public employee has a "reasonable expectation of privacy" in a matter intruded upon "is only to begin the inquiry."[22] The plurality in *O'Connor* found that determining the reasonableness of a workplace search under the Fourth Amendment requires "balanc[ing] the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace."[23] Given the "realities of the workplace," the Court concluded that a workplace search did not require a warrant and probable cause to satisfy the Fourth Amendment. Rather, workplace searches "should be judged by the standard of reasonableness under all the circumstances," taking into account whether the intrusion was "justified at its inception" *and* was "reasonably related in scope" to the initial justification.[24]

Employees in the private sector generally cannot rely on constitutional rights to protect against employer intrusion.[25] Instead, these employees have invoked common law privacy torts to redress perceived violations of their privacy rights.[26] The common law tort most relevant to the employ-

21. *Id.* at 716. Justice Scalia agreed that the Fourth Amendment applies to searches and seizures by government employers, but disagreed with the plurality's open-ended, contextual inquiry for determining whether or not a reasonable expectation of privacy exists in the workplace. *Id.* at 729–30 (Scalia, J., concurring). He would have held that government employees' offices and their contents are covered by the Fourth Amendment, but that the employment relationship is significant for determining whether a given search is "reasonable." *Id.* at 731.

22. *Id*. at 719 (quoting New Jersey v. T.L.O., 469 U.S. 325, 337 (1985)).

23. *Id.* at 719–20.

24. *Id*. at 725–26 (quoting *T.L.O.*, 469 U.S. at 342).

25. Although private sector employees generally cannot rely on constitutional provisions as a source of privacy protections, courts in a few states have allowed them to invoke state constitutional provisions. The California Supreme Court, for example, has held that the state's constitutional guarantee of individual privacy directly applies to both public and private actors—including private employers. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633 (Cal. 1994). In Alaska, the constitutional right to privacy applies only to state action; however, the Alaska Supreme Court looked to the constitutional privacy guarantee, along with other sources of law, to conclude that public policy protects certain spheres of employee conduct from employer intrusion even in the private sector. Luedtke v. Nabors Alaska Drilling, Inc., 768 P.2d 1123 (Alaska 1989).

26. In a unionized workplace, employees may have additional protections, depending upon the terms of the collective bargaining agreement. Such agreements generally restrict employers' right to discipline or discharge employees without just cause. Because a just cause standard requires the employer to have reasons connected to the work or the workplace for its actions, *see* Roger I. Abrams & Dennis R. Nolan, *Toward a Theory of "Just Cause" in Employee Discipline Cases*, 1985 DUKE L. J. 594, 611–12 (1985), it protects employees' privacy indirectly to the extent that it limits the employer's ability to take disciplinary action based on personal information or activities that are not job related. In addition, employers may be required to bargain with a union before initiating privacy-intrusive practices such as workplace monitoring of employees. *See* Colgate-Palmolive Co. and Local 15, International

ment setting establishes liability for an intentional intrusion "upon the solitude or seclusion of another or his private affairs or concerns" that is "highly offensive to a reasonable person."[27] Although cases decided under the Constitution are not binding precedent, many courts have borrowed language from those cases, asking whether the plaintiff had a "legitimate expectation of privacy" as part of its analysis of the invasion of privacy tort claim. For example, in *K-Mart Corporation v. Trotti*, the Court of Appeals of Texas concluded that an employee who placed a personal lock on a locker at her worksite had "demonstrated a legitimate expectation to a right of privacy in both the locker itself and those personal effects within it."[28] Conversely, in *O'Bryan v. KTIV Television*, the Northern District of Iowa concluded that an employee lacked a "reasonable expectation of privacy" that his desk and office area would not be searched for work-related documents.[29]

As in the constitutional cases, this inquiry serves roughly to separate personal matters from areas of legitimate employer concern. Even at the workplace, the law limits searches of personal effects[30] and shields employees from observation in traditionally private spaces such as a restroom or dressing room.[31] Similarly, the common law tort protects employees' privacy in traditionally secluded off duty locations such as a home[32] or hotel room.[33] On the other hand, the more closely the matter intruded upon is connected to work or the workplace, the less likely an actionable invasion of privacy will be found. As examples, courts have found no invasion

Chem. Workers Union., 323 N.L.R.B. 515 (1997). On the other hand, the union grievance process tends to focus on job security, rather than dignitary harms caused by invasions of privacy. *See* Pauline T. Kim, *Collective and Individual Approaches to Protecting Employee Privacy: The Experience With Workplace Drug Testing*, 66 LA. L. REV. 1009, 1019–22, 1029 (2006).

27. Restatement (Second) of Torts § 652B (1977). Although the common law tort offers some protection of employee privacy interests, its application in the workplace context is complicated by the fact that most private sector employees are employed at will, making it difficult for them to object to perceived invasions of privacy without risking discharge. *See* Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L. J. 671 (1996).

28. 677 S.W.2d 632, 638 (Ct. App. Tex.1984).

29. 868 F. Supp. 1146, 1159 (N.D. Iowa 1994).

30. *See, e.g.*, *K-Mart*, 677 S.W.2d at 632 (remanding for consideration of plaintiff's claim that her employer invaded her privacy when it opened her locker and searched her purse).

31. *See, e.g.*, Johnson v. Allen, 613 S.E.2d 657 (Ga. App. 2005) (rejecting summary judgment for employer on invasion of privacy claim alleging installation and monitoring of video camera in women's restroom); Kjerstad v. Ravellette Publ'n, Inc., 517 N.W.2d 419, 424 (S.D. 1994) (upholding jury verdict for plaintiffs on invasion of privacy claim based on employer's surreptitious observation of employees in bathroom).

32. *See, e.g.*, Wal-Mart Stores v. Lee, 74 S.W.3d 634, 648–49 (Ark. 2002) (upholding jury verdict for employee for invasion of privacy based on employer's search of his home for allegedly stolen merchandise).

33. *See, e.g.*, Sowards v. Norbar, Inc., 605 N.E.2d 468, 474–75 (Ohio Ct. App. 1992) (affirming jury finding that employer invaded employee's right to privacy by searching motel room).

of privacy when employers have searched for work-related documents in an employee's office and desk[34] or for contraband in an employee's car parked on the employer's premises.[35] Thus, even though framed in terms of a "highly offensive intrusion," the common law privacy tort, like privacy protections under the Constitution, purports to distinguish personal from work-related matters.

Scholars have long criticized constitutional and common law doctrines as insufficiently protective of employee privacy.[36] Some have criticized the "reasonable expectation of privacy" test to the extent that it looks to employer policies and practices, rather than existing social norms to determine "reasonableness."[37] Such an approach permits employers to destroy any expectations of privacy simply by announcing privacy-invading practices in advance, and regularly carrying them out.[38] The common law privacy tort similarly turns on business practices, and courts have relied on the existence of a business justification to reduce an employee's expectation of privacy or render the intrusion inoffensive. Professor Matthew Finkin asserts that this analytical structure "reduces the idea of a common law protective of employee privacy to an irrelevance insofar as systematically invasive action is taken in the name of what management perceives as a greater business good."[39] Whether or not the law adequately protects traditional concerns like bodily or spatial privacy, it has proven quite anemic when confronted with employees' claims to privacy in their electronic communications, as discussed in Part II, *infra*.

B. Changes in the Organization of Work

Recent developments in the organization of work have contributed to a blurring of the boundary between personal and professional identities. Of course, work and private life have never been entirely distinct. Over time and across workplaces, there has been great variation in the extent to which personal and work lives overlapped or were rigidly compartmentalized.

34. *O'Bryan*, 868 F. Supp. at1146 (granting summary judgment for employer on employee's invasion of privacy claim based on a search of his desk and office area).

35. Terrell v. Rowsey, 647 N.E.2d 662, 667 (Ind. Ct. App. 1995) (finding no wrongful invasion of privacy when employer searched employee's car on suspicion he was drinking beer during a work break).

36. *See, e.g.*, Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI.-KENT L. REV. 221 (1996) [hereinafter Finkin, *Employee Privacy*]; Kim, *supra* note 27; Don Mayer, *Workplace Privacy and the Fourth Amendment: An End to Reasonable Expectations?*, 29 AM. BUS. L.J. 625 (1992).

37. *See,e.g.*, Mayer, *supra* note 36, at 643–45.

38. *See* Finkin, *Employee Privacy*, *supra* note 36, at 226.

39. *Id.* at 240.

Under traditional common law rules, for example, the master-servant relationship entailed not merely an economic exchange, but a personal relationship with obligations and duties as well.[40] Often, the work relationship was also a domestic one, with the servant residing with the master.[41] In the mid-twentieth century, however, the modern organization of work clearly separated home and paid work. The protection of employee privacy was one means of policing that boundary.[42]

In recent decades, changes in the organization of work have once again blurred that boundary. These changes have received considerable attention—firms are abandoning the internal labor market model, lifetime jobs are rare, employees change jobs frequently and employers no longer encourage expectations of job security.[43] The breakdown of career employment means that employer and employee interests are no longer as clearly aligned over the long term. Employers that no longer hold out the prospect of lifetime employment cannot rely on traditional policies, such as the promise of pensions and retiree health care benefits to align their workers' long term interests with their own.[44]

Unwilling to promise long term job security, firms now encourage employees to develop affective ties to the workplace to induce employee loyalty.[45] When sociologist Arlie Hochschild began an in-depth study of the challenges faced by working parents, she "assumed that home was 'home' and work was 'work.'"[46] What she discovered instead was that for some employees, these worlds are becoming reversed. Particularly for working parents, home may be experienced as a place of obligation, stress and conflict, while work can be a site of affirmation, positive social interactions and strong emotional ties. Employers often deliberately cultivate these feelings, referring to the company as "family," encouraging social bonds among employees and inculcating firm values—all intended to foster emotional attachment and increased loyalty to the firm. Similarly, Marion Crain has documented employer efforts to ensure worker loyalty by inducing

40. *See* JAMES B. ATLESON, VALUES AND ASSUMPTIONS IN AMERICAN LABOR LAW 11–14 (1983) (depicting the household model of master-servant law, with defined expectations and obligations).

41. Jay M. Feinman, *The Development of the Employment at Will Rule*, 20 AM. J. LEGAL HIST. 118, 123 (1976) (describing the master servant relation as personal, often familial).

42. *See, e.g.*, PHILIP SELZNICK, LAW, SOCIETY, AND INDUSTRIAL JUSTICE 197–200 (1969).

43. *See, e.g.*, PETER CAPPELLI, THE NEW DEAL AT WORK: MANAGING THE MARKET-DRIVEN WORKFORCE (1999); KATHERINE V.W. STONE, FROM WIDGETS TO DIGITS: EMPLOYMENT REGULATIONS FOR THE CHANGING WORKPLACE (2004).

44. Marion Crain, *Managing Identity: Buying Into the Brand at Work*, 95 IOWA L. REV. 1179, 1192–95 (2010).

45. *Id.* at 1197–98.

46. ARLIE RUSSELL HOCHSCHILD, THE TIME BIND: WHEN WORK BECOMES HOME AND HOME BECOMES WORK (1997).

employees to identify with the company brand. As she writes, such efforts "aim[] to induce employees to view their employment as a personal relationship akin to a family tie, imbuing the economic transaction with emotional significance."[47]

The changing demographics of the labor force have further contributed to blurring the boundary between home and work. The traditional family model with clearly delineated roles of breadwinner and homemaker permitted a clean separation of work and home life. Men were free to focus on market work, while women performed care work in spaces physically separate from the paid workplace. In recent years, the influx of women, particularly women with children, into the workplace has disrupted this traditional model. Strict compartmentalization of work and home is no longer possible for the increasing number of dual-earner and single-parent families. Today, both men and women have multiple, significant roles—worker, partner, parent—putting pressure on employers to accommodate workers' family obligations through benefits such as flex time, on-site daycare, and telecommuting. While these types of policies may help employees balance work and family obligations, a side effect is that work and home are more difficult to separate, with home life and personal matters inevitably seeping into the workplace, while work activities often extend into the home. As a result, the boundary between home and work has become increasingly unstable and difficult to police.

C. Changes in Technology

The advent of the electronic workplace is also making it more difficult to separate work and home. Even before the rise of electronic communications, the line was not always a clear one. Dissenting in *O'Connor v. Ortega* nearly a quarter century ago, Justice Blackmun noted that long working hours meant that "the workplace has become another home for most working Americans."[48] Inevitably, employees might sometimes need to make personal calls or attend to personal business during breaks at work. "As a result," he argued, "the tidy distinctions . . . between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality."[49] Justice Blackman thus rejected the plurality's suggestion that an employee could protect personal

47. Crain, *supra* note 44, at 1179.
48. 480 U.S. 709, 739 (1987) (Blackmun, J., dissenting).
49. *Id.*

belongings "by simply leaving them at home" as insensitive to the "operational realities of the workplace."[50]

The difficulty of neatly compartmentalizing home and work has been exacerbated by technological change. In an earlier era, an employee might have used an office telephone to make a personal call during a break. Although phone calls could be recorded, phone systems in most workplaces were not routinely configured to constantly record conversations. Workplace norms generally permitted limited private use of an employer's phone system, and some employers provided separate phone lines for employees' personal use.[51] In addition, the law restricted the employer's ability to capture purely personal phone calls.[52] Today, an employee might use a work computer during a break to check a website for information regarding a medical condition or send an email to a spouse or lover. Information about these online activities is automatically stored and can be systematically tracked or retrieved and reviewed long after the fact.

Given the ubiquity of electronic communications in both business and social life, it is unrealistic to expect that employees will never use employer-provided systems to communicate about personal matters.[53] In order to keep personal life entirely out of the workplace, an employee would have to consciously segregate any non-work related information, engaging in constant self-monitoring of how, when and with whom she communicates. If it were necessary to engage in the occasional bit of personal business during a break or lunch hour, the employee would not only need to maintain a personal email account, she would also need to bring a personal smartphone or computer to work—one that did not access the internet through her employer's server. She would need to take care that her personal and work calendars, contacts and other electronically stored data

50. *Id.* at 740.

51. *See, e.g.*, Watkins v. L. M. Berry & Co., 704 F.2d 577, 579 (11th Cir. 1983) (describing employer policy of permitting personal calls on company phones); Jandak v. Vill. of Brookfield, 520 F. Supp. 815, 824–25 (N.D. Ill. 1981) (describing workplace with 10 phone lines, nine of which were continuously taped and one of which was unmonitored and provided expressly for personal use).

52. *See* Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (affirming award of damages under Title III of Omnibus Crime Control and Safe Streets Act of 1968 to employee whose personal phone calls were surreptitiously recorded by employer); *Watkins*, 704 F.2d at 583 (interpreting Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to permit interception of a personal call to determine whether it was a business or personal call, but not to learn its contents).

53. In *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), a police officer alleged his Fourth Amendment rights were violated when his employer reviewed transcripts of messages sent on his work pager. Although the pagers were intended to coordinate the activities of SWAT team members, Quon had sent numerous private messages, many of which were sent to intimates and were sexually explicit in nature. The facts in *Quon* are notable for the sheer number of personal texts sent on work time (nearly 400 in a one month period) and their highly personal nature; however, occasional employee use of employer-provided equipment for personal communications is a much broader phenomenon.

were stored separately and accessed on separate devices. Even with such assiduous efforts, the employee is unlikely to succeed entirely in preventing personal matters from seeping into the workplace. A friend or family member might send communications containing personal information to an employee at work without her consent, and an employer may be able to infer personal information simply by knowing to whom an employee is related and with whom she associates.[54]

Advances in technology have also allowed work to extend far beyond the workplace. In an effort to increase flexibility and efficiency, employers provide smartphones, laptop computers and pagers, so that employees can work at home or while travelling. These devices permit work to intrude into previously private spaces, and into times traditionally considered beyond the bounds of the workday, further blurring the boundaries of the work environment. The co-mingling of work and private life in time and space makes it more difficult for employees to determine when their activities might be subject to employer scrutiny and control. For example, in a recent case, an employee used an employer provided laptop to review and send several emails to her attorney regarding a possible discrimination claim against the employer.[55] She did so off-premises during nonworking hours using a personal, password-protected Yahoo account, believing that her communications would thereby remain confidential. Nevertheless, the employer was able to recover copies of the emails from the computer's hard drive after she had returned it.

Even off duty activities that take place completely outside the work environment may have repercussions at work. With the growth of information technologies, more and more individuals are active participants in blogs, online fora and social media sites, increasing the likelihood that their employers will become aware of their off duty communications and activities. Even when employees use their own computers or personal smartphones to access these sites, their employers may learn of their online activities. News stories have reported numerous instances of employees

54. For example, because many diseases have a genetic basis, genetic information about an individual may be revealed simply by knowing about the health condition of a close blood relative. Mark MacCarthy discusses other types of "privacy externalities"—situations in which information revealed by others about themselves can indirectly reveal information about another individual who has not chosen to reveal that information. Mark MacCarthy, *New Directions in Privacy, available at* http://works.bepress.com/mark_maccarthy/2 (2010). For example, as knowledge of networks grows, researchers can often infer health and behavioral characteristics about an individual simply by knowing about that person's associates.

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

terminated because of their blog posts,[56] and members of Facebook groups, such as "Have You Been Fired Because of Facebook?" share stories about losing their jobs because of their communications on social media. In recent months, the National Labor Relations Board has received over a hundred complaints from employees terminated or disciplined because of their use of social media—in most cases, while off duty.[57]

While employers have always had an interest in monitoring their employees' activities, technological change has increased both the incentives and means to do so. In addition to concerns about productivity and abuse of property that traditionally motivated employer surveillance, employers now also fear that employee misuse of electronic communications will increase their liability risks—for example, by giving rise to charges of racial or sexual harassment, or subjecting the employer to claims of fraud, defamation or copyright infringement. Employee mishandling of electronic files could also result in improper disclosure of customers' private information or other security breaches, or risk the disclosure of trade secrets or other valuable business information, either intentionally or inadvertently. And when an individual is identifiable as an employee, even her off duty activities, when amplified by the internet, have the potential to cause harm to a firm's public image.[58]

At the same time, technological advances are making it easier and cheaper for employers to monitor their employees' electronic activities, and employers are increasingly engaging in such monitoring. A recent survey of over 300 firms found that 43% of the respondents monitored their employees' email, 66% monitor website connections and 45% track computer

56. *See, e.g.*, Stephanie Armour, *Warning: your clever little blog could get you fired*, USA TODAY (June 15, 2005, 10:24 PM), http://www.usatoday.com/money/workplace/2005-06-14-worker-blogs-usat_x.htm; *Fired for Blogging*, CBSNEWS (Feb. 11, 2009, 7:33 PM), http://www.cbsnews.com/stories/2005/03/07/tech/main678554.shtml.

57. *See* Melanie Trottman, *Workers Claim Right to Rant on Facebook*, WALL ST. J., Dec. 2, 2011, at B1 (explaining that more than 100 charges have been filed with the NLRB by employees alleging that they were terminated because of their communications on social media sites); NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (12–31), Jan. 24, 2012 (updating earlier report by describing additional cases concerning employees' use of social media and employers' social medial policies and rules); NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (11–74), Aug. 18, 2011 (describing recent claims of interference with protected rights based on employees' use of social media and Board responses).

58. A notable example is the video produced by several Domino's Pizza employees as a joke, in which they purported to prepare food for customers in a highly unsanitary manner. Their attempt at humor went awry when the video went viral on Youtube, harming Domino's reputation and resulting in their termination. *See* Stephanie Clifford, *Video Prank at Domino's Taints Brand*, N. Y. TIMES, April 15, 2009, at B1.

use by monitoring time spent, content or keystrokes entered.[59] Although the survey focused on workplace monitoring, anecdotal reports suggest that at least some employers are seeking to monitor their employees' online activities off the job as well. Some have reportedly required current or prospective employees to provide their usernames and passwords for Facebook or private chat groups.[60] In addition, software is now available that employers can use to automatically monitor their employees' activities on social networking sites such as Facebook, Twitter, and LinkedIn.[61]

II. THE LIMITATIONS OF PRIVACY LAW

The current law of privacy is not well equipped to address these developments in the workplace. The Electronic Communications Privacy Act ("ECPA"),[62] which prohibits the interception of electronic communications and unauthorized access to stored communications, would appear to limit employers' ability to access and monitor private employee communications, and it has on occasion provided redress to employees for employer intrusions into their off duty activities.[63] The prohibitions contained in the ECPA, however, are subject to a number of exceptions—for example, when there is consent to the interception,[64] or when the communication is accessed by the provider of the electronic communications service.[65] Be-

59. American Management Association & The ePolicy Institute, *2007 Electronic Monitoring & Surveillance Survey* (Feb. 28, 2008), http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/.

60. *See, e.g.*, Abril, et al., *supra* note 6, at 102 (noting that some survey respondents reported being required to give employers access to their online social media profiles); Alexis Madrigal, *Should Employers Be Allowed to Ask for Your Facebook Login?*, THE ATLANTIC (Feb. 19, 2011, 10:54 PM), http://www.theatlantic.com/technology/archive/2011/02/should-employers-be-allowed-to-ask-for-your-facebook-login/71480/; Declan McCullagh, *Want a Job? Hand Over Your E-Mail Login*, CBSNEWS (June 19, 2009, 1:02 PM), http://www.cbsnews.com/stories/2009/06/18/national/main5096450.shtml.

61. Joshua Brustein, *Keeping a Closer Eye on Employees' Social Networking*, N.Y. TIMES (Mar. 26, 2010, 6:51 PM), http://bits.blogs.nytimes.com/2010/03/26/keeping-a-closer-eye-on-workers-social-networking/.

62. 18 U.S.C. § 2510 (2006). The EPCA has two parts that are potentially relevant to the employment relationship. Title I, sometimes referred to as the Wiretap Act, prohibits the interception of electronic communications. Title II contains the Stored Communications Act (SCA), which creates civil liability for intentional access without authorization of "a facility through which an electronic communication service is provided" or which "intentionally exceeds an authorization to access that facility." 18 U.S.C. § 2701(a) (2006).

63. *See, e.g.*, Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002) (reversing summary judgment on SCA claim for employer who accessed employee's password protected website, given dispute whether it obtained access through an authorized user); Pietrylo v. Hillstone Rest. Group, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (refusing to set aside jury verdict finding that employer violated the SCA when it accessed plaintiffs' private chat group on MySpace); Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914, 926 (W.D. Wis. 2002) (denying summary judgment on SCA claim to employer who accessed plaintiff's web-based Hotmail account).

64. 18 U.S.C. § 2511(2)(c) (2006).

65. 18 U.S.C. § 2701(c)(1) (2006).

cause employees may be deemed to have consented to surveillance, and employers are often the providers of electronic communications systems such as email, the Act's protections have been found inapplicable in a number of workplace cases.[66] Although the ECPA could be interpreted in ways more protective of employee privacy,[67] under current interpretations it provides rather weak protection against employer scrutiny of employees' electronic communications.[68]

Given the uncertain protections of the ECPA, employees have also asserted privacy rights under constitutional and common law doctrines. As discussed in Part I. A., *supra*, the analysis under either framework begins with the threshold question whether an employee has a reasonable expectation of privacy. This test has been criticized on a number of grounds,[69] but it is particularly unhelpful in analyzing new technologies. In the Fourth Amendment context, courts look to such factors as "the intention of the Framers" and "societal understanding" to determine whether an expectation of privacy is reasonable.[70] These inquiries offer little help, however, when considering new technologies for which no historical consensus or established societal understanding exists. Precisely because their role in society and the norms governing their use are contested and evolving, no existing "societal understanding" can determine which expectations of privacy are fundamental enough to warrant protection.

In the absence of established societal understandings, many courts considering employees' claims of electronic privacy have resorted to mechanical forms of reasoning. Thus, some have concluded that the employer's ownership of the computer system or the fact that it is technologically possible for a message to be intercepted negates any reasonable expectation

66. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107 (3d Cir. 2003) (finding no violation of Title II of ECPA because employer was provider of the service); Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329 (N.D. Cal. Aug. 27, 2009) (finding ECPA exception applies where employee had impliedly consented to monitoring of his work email); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996) (same).

67. *See, e.g.*, Levinson, *supra* note 6.

68. *See* Ariana R. Levinson, *Workplace Privacy and Monitoring: The Quest for Balanced Interests*, 59 CLEV. ST. L. REV. 377 (2011). A number of states have enacted statutory protections analogous to the federal ECPA and in some cases, these statutes have narrower exceptions. Nevertheless, these state laws have generally not provided any significant protection in the employment context.

69. *See, e.g.*, SOLOVE, *supra* note 1, at 72–73 (discussing the difficulties in determining how reasonable expectations of privacy are to be determined); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974) (arguing that government can destroy 'reasonable expectation of privacy' merely by announcing that it will conduct comprehensive surveillance); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (1979) (asserting that "reasonable expectation of privacy" test is circular because expectations will depend upon the legal rule).

70. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

of privacy.[71] Property ownership and technological feasibility, however, are not decisive in determining whether an expectation of privacy is reasonable.[72] As Professors Bellia and Freiwald have argued, the "reasonable expectation of privacy" test should entail "*normative* rather than merely positive analysis."[73] In other words, the role of courts should be to "ask what society is *entitled to believe*," not merely whether a given form of communication is potentially vulnerable to interception.[74] When the Supreme Court in *Katz v. United States*[75] held that individuals have a reasonable expectation of privacy in their telephone conversations, the public was well aware of the possibility of wiretapping. Nonetheless, the Court protected these conversations because of "the vital role that the public telephone has come to play in private communication."[76]

Thus, courts *could* work to discern when new forms of monitoring implicate fundamental interests that warrant recognition and protection; however, for the most part they have declined to do so in the employment context. For example, the Supreme Court in *City of Ontario v. Quon*[77] recently confronted whether a public employee had a reasonable expectation of privacy in personal texts sent on an employer provided pager, but declined to decide the question because of uncertainty about "how workplace norms, and the law's treatment of them, will evolve" given "[r]apid chang-

71. *See, e.g.*, Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (rejecting employee claim of privacy in files stored on laptop computer in part because the laptop was owned by employer); *Bohach*, 932 F. Supp. at 1234 (finding expectation of privacy not objective reasonable given that recording and storing of pager messages are "an integral part of the technology"); Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (finding employee did not have reasonable expectation of privacy in messages sent over company owned e-mail system); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999) (noting that email messages were stored on a company-owned computer and were accessible when transmitted in rejecting employee claim of privacy in email).

72. *See, e.g.*, *O'Connor*, 480 U.S. at 740 n.7 (Blackmun, J., dissenting) ("This Court . . . has made it clear that privacy interests protected by the Fourth Amendment do not turn on ownership of particular premises), (citing Rakas v. Illinois, 439 U.S. 128, 143 (1978); U. S. v. Warshak, 631 F.3d 266, 286–87 (6th Cir. 2010) ("The mere *ability* of a third-party intermediary to access the content of a communication cannot be sufficient to extinguish a reasonable expectation of privacy.") (emphasis in original); Schowergerdt v. General Dynamics, 823 F.2d 1328, 1233 ("Fourth Amendment privacy interests do not . . . turn on property interests."). *Cf.* Watkins v. L. M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (stating that "knowledge of the *capability* of monitoring alone cannot be considered implied consent" that would permit interception of telephone conversations under federal wiretapping statute). Moreover, under the common law privacy tort, employees have long been protected against unreasonable searches of their personal belongings or surveillance in traditionally private places, such as bathrooms and locker rooms, even when on employer property. *See* cases cited *supra* notes 30–35.

73. *See* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U.CHI. L. F. 121, 137 (2008).

74. *Id.*; *see also* Mayer, *supra* note 36.

75. 389 U.S. 347 (1967).

76. *Id.* at 352.

77. 130 S.Ct. 2619 (2010).

es in the dynamics of communications and information transmission."[78] In refusing to decide the issue, the Supreme Court failed to recognize that law is itself constitutive of what expectations of privacy are "legitimate."[79] By finding that certain areas are worthy of protection, the law validates and reinforces claims of privacy; by declining to do so, the law negates those claims, further diminishing expectations of privacy.

The Sixth Circuit's recent decision in *United States v. Warshak*[80] acknowledged this constitutive role of law. It addressed the question whether individuals have a reasonable expectation of privacy in the contents of their email stored with or received through an internet service provider, thereby triggering Fourth Amendment protections.[81] Arguing that the Fourth Amendment "must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish," the court found that email requires "strong protection" given that it "plays an indispensable part in the Information Age."[82] Similarly, the concurring Justices in *United States v. Jones* argued that Fourth Amendment protections should turn on the underlying interests at stake rather than the mechanical aspects of a search. When considering whether attaching a GPS device to a vehicle constitutes a search, Justice Alito pointed out that the significance of the device lay not in its attachment to the vehicle, but its *use* to track the defendant's movements over a long period of time.[83] Justice Sotomayor likewise emphasized that the device "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[84]

The approaches taken by the *Warshak* court and Justices Sotomayor and Alito in *Jones* suggest that existing law *could* be interpreted in ways

78. *Id.* at 2629–30. Rather than risk articulating an overly broad holding concerning the existence and extent of employee privacy expectations, the Court chose to decide the case on alternative grounds. The Court decided that even assuming that Quon had a reasonable expectation of privacy in his text messages, the search was reasonable because it was justified by a legitimate employer purpose. *Id.*

79. Established social norms now treat postal mail and telephone conversations as private in part because the law at an earlier time extended protection to these forms of communication, thereby reinforcing emerging norms. *See, e.g.*, Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 562–68 (2007) (describing the development of laws and norms enforcing the confidentiality of postal mail); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 141–42 (2007) (same).

80. 631 F.3d 266 (6th Cir. 2010).

81. *Id.* Thus, it found that to the extent that the SCA permits government searches of stored emails without a warrant, it is unconstitutional. *Id.* at 288.

82. *Id.* at 285–86. The *Warshak* court commented that "as some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise." *Id.* at 285.

83. United States v. Jones, 132 S.Ct. 945, 961 (2012) (Alito, J., concurring).

84. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

more protective of employees' electronic privacy. Some courts have found electronic communications protected under existing law, particularly in cases involving employer monitoring of private email accounts or off duty fora such as chat groups.[85] Others have distinguished between an employer's legitimate interests in knowing whether an employee is using electronic communications for personal matters or improper purposes and its lack of need to access the *contents* of those communications.[86]

However, protection of employee privacy is complicated by the contractual nature of the employment relationship. Many cases have concluded that employees lack any expectation of privacy if they have been given notice that monitoring or review of electronic communications will occur.[87] Consent-based arguments should have less force when employees are given only generic notice and the employer engages in novel forms of monitoring and surveillance. Many employees are relatively unsophisticated users of technology and simply may not realize its potential for tracking and storing information about their activities.[88] Moreover, employers sometimes send

85. *See, e.g.*, Konop v. Hawaiian Airlines, 302 F.3d 868 (9th Cir. 2002); Stengart v. Loving Care Agency, 990 A.2d 650 (N.J. 2010); Pietrylo v. Hillstone Rest. Group, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009); Fischer v. Mt. Olive Lutheran Church, 207 F. Supp. 2d 914, 926 (W.D. Wis. 2002); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

86. *See, e.g.*, Stengart v. Loving Care Agency, 990 A.2d 650, 665 (N.J. 2010) (asserting that "employers have no need or basis to read the specific *contents* of personal, privileged, attorney-client communications in order to enforce [legitimate] corporate policies"). *See also* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 909 (9th Cir. 2008) (noting that there were "a host of simple ways" the employer could have met its legitimate business needs without intruding on plaintiffs' Fourth Amendment rights by reading a transcript of his personal text messages), *rev'd* City of Ontario v. Quon, 130 S. Ct. 2619 (2010). *Cf.* Watkins v. L. M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983) (finding that employer is permitted to intercept a personal call to determine whether it was a business or personal call, but not to learn its contents).

87. *See, e.g.*, Muick v. Glenayre Elecs., 280 F.3d 741 (7th Cir. 2002) (holding that employer's announcement that it could inspect laptops it furnished destroyed any reasonable expectation of privacy); Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *5 (N.D. Cal. Aug. 27, 2009) (finding that advance notice that a company monitors computer use diminishes employee's expectation of privacy); Thygeson v. U.S. Bancorp, No. CV-03-467-ST., 2004 WL 2066746 (D. Or. Sept. 15, 2004)(holding employee had no expectation of privacy because he was warned that office computer could be monitored); Kelleher v. City of Reading, No. CIV.A.01-3386, (E.D. Pa. May 29, 2002) (finding no reasonable expectation of privacy where employer's policy informed employees that email was not private); Bohach v. City of Reno, 932 F. Supp. 1232, 1235 (D. Nev. 1996) (finding a diminished expectation of privacy where users were notified that their messages would be logged). *Cf.* Curto v. Medical World Communications, Inc., No. 03CV6327 (DRH) (MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (finding extent to which employer actually enforced its computer usage policy a relevant factor in evaluating employee's expectation of privacy in computer use).

88. Employees often know enough to use computers or other electronic devices to accomplish work-related tasks, but understand little about how those devices actually operate and the extent to which they can collect and store information. For example, in *Stengart v. Loving Care Agency*, 990 A.2d 650 (N.J. 2010), the employee communicated with her attorney via email using an employer-provided laptop computer. She believed, erroneously, that by using a personal, password-protected account, she was ensuring the confidentiality of her communications. After her employment terminated,

conflicting messages, maintaining an official policy against personal use of electronic systems while tolerating or even subtly encouraging such use.[89] Nevertheless, because the employment relationship is a contractual one, employee privacy rights are vulnerable to the claim that the employee has consented to any intrusion.

In addition to asking whether an expectation of privacy is reasonable, the law also weighs the employer's interest in the matter intruded upon. If work and home are neatly separated, it is relatively simple to delineate areas of legitimate employer concern, distinct from purely personal concerns of the employee. However, as discussed *supra*, technological developments have heightened concerns about employee misuse of technology, increasing employers' interests in monitoring employee communications and activities at work. At the same time, the power of the internet has raised fears that employees' off duty communications—postings on blogs or Facebook—might harm the employer's interests or reputation. And so employers are increasingly claiming an interest in knowing what employees do on their own time as well. Thus, as the boundary between work and personal life becomes more porous, the areas of employers' legitimate concern are expanding, reaching employee activities, spaces, and communications previously considered private.

The combination of these factors—the unsettled norms surrounding new forms of electronic communication, the contractual nature of the employment relationship, and the increasing difficulty of disentangling work and personal interests—means that current law only weakly protects employees' electronic communications from employer scrutiny.[90]

her former employer used forensic techniques to recover the contents of her email communications with her attorney, which had been permanently stored on her hard drive. Similarly, in *Curto v. Medical World Communications, Inc.*, No. 03CV6327 (DRH)(MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006), the employee believed that she had protected the privacy of her personal communications by deleting all of her personal files and emails before returning a laptop she used to work at home to her employer. The employer was nevertheless able to recover those files and emails later with the assistance of forensic consultants. Gaia Bernstein argues that the concealed nature of internet monitoring "dilutes the perception of a threat" and makes individuals less likely to take steps to protect their privacy. Gaia Bernstein, *When New Technologies are Still New: Windows of Opportunity for Privacy Protection*, 51 VILL. L. REV. 921, 936 (2006). A similar dynamic may exist for employees who receive only a generic warning that their computer usage is subject to monitoring.

89. In *Quon*, for example, the City of Ontario asserted that text messages were included in its policy that computer messages were not private. 130 S. Ct. 2619 (2010). Quon argued, however, that he had been assured by a supervisor that his messages would not be audited as long as he paid any excess usage fees. *Id. See also* Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387 (E.D.N.Y. May 15, 2006) (finding that lack of enforcement of employer's computer usage policy lulled employees into believing it would not be enforced).

90. While these factors make it more difficult to protect the privacy of employees' electronic communications, it is possible to imagine legal regimes that are more privacy protective while also accommodating employers' interests. For example, Israel's National Labor Court recently held that

III. SOCIALLY VALUABLE EMPLOYEE SPEECH

At the same time that employee privacy is eroding, the law increasingly seeks to encourage certain socially valuable forms of employee speech. To a large extent, employees have no legally protected right to speak freely.[91] Freedom of expression may be valued as an important aspect of individual autonomy, but the workplace is not generally regarded as an appropriate forum for unrestricted expressive activity. In managing its business, the employer has a great deal of discretion in setting work rules, and in some respects, the law may be growing less protective of employees who speak up in ways that their employer does not approve.[92] Nevertheless, several types of employee speech have consistently been recognized to have social value—a public significance beyond whatever benefit they may afford to the individual speaker—and are therefore protected by law.

The first such area is collective speech. When Congress passed the National Labor Relations Act in 1935, the core of its protections were found in Section 7, which guaranteed the rights of workers to self-organize and bargain collectively.[93] Significantly, however, the language of Section 7 extends not just to formal collective bargaining, but to employees' right

employers can limit employee use of company email systems, but must clearly inform workers in advance and, even with such a policy, they may not make use of personal content discovered in employees' email correspondence. The court further restricted the right of employers to monitor employees' personal email accounts, even if accessed through employer systems, and suggested policies that might balance employee and employer interests—such as providing separate email accounts for business and personal use, blocking access to certain sites rather than monitoring internet use, or designating times when workers could use computers for personal reasons. *See* Jenny David, *Israel National Labor Court Ruling Restricts Access of Employers to Worker E-Mails*, 37 BNA DAILY LAB. REP. A-7 (Feb. 24, 2011).

91. Scholars have argued that employee speech interests are insufficiently protected under current law. *See, e.g.*, Cynthia L. Estlund, *Free Speech and Due Process in the Workplace*, 71 IND. L.J. 101 (1995); David C. Yamada, *Voices From the Cubicle: Protecting and Encouraging Private Employee Speech in the Post-Industrial Workplace*, 19 BERKELEY J. OF EMP. & LAB. L. 1 (1998).

92. As an example, the Supreme Court's recent decision in *Garcetti v. Ceballos*, 547 U.S. 410 (2006), narrowed the speech rights of public employees by holding that statements made pursuant to an employee's official duties are not protected from employer discipline by the First Amendment. In an earlier case, *Connick v. Myers*, 461 U.S. 138 (1983), the Court had similarly narrowed the rights of public employees by excluding from First Amendment protection speech regarding personnel grievances or internal office policies. Despite rejecting the plaintiff's claim, the Court in *Garcetti* acknowledged the value of whistleblowing speech. It noted that "[e]xposing governmental inefficiency and misconduct is a matter of considerable significance," *id.* at 425, and pointed to various whistleblower protection laws as providing safeguards independent of the First Amendment. Professor Richard Moberly argues that the *Garcetti* Court recognized the importance of whistleblowing speech, but its decision reflected its understanding that whistleblower protection is a matter of statutory, not constitutional, law. Richard Moberly, *The Supreme Court's Antiretaliation Principle*, 61 CASE W. RES. L. REV. 375, 430 (2010).

93. *See* 29 U.S.C. § 157 (2006). Section 7 protects a fundamental associational right, one seen as necessary to counter the inherent inequality of bargaining power when a single employee negotiates alone with the employer. *See* NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1 (1937).

"to engage in other concerted activities for . . . mutual aid or protection."[94] Numerous court and Board decisions have interpreted this clause to extend protection to unorganized workers acting together, even when they have no intention or thought of organizing a union.[95] As Professor Charles Morris explained, "[c]oncerted conduct . . . may not necessarily be intended to achieve union organization, at least not deliberately or initially."[96] Section 7 ensures that unrepresented employees, who are often poorly informed of their rights, need not "act at their peril when they begin informal joint discussions."[97] They might not be "looking toward group action" initially, "[b]ut given the opportunity, group action—be it mild or assertive—might in time evolve from that rudimentary process."[98] Thus, even preliminary discussions among employees about wages, hours, or working conditions "must be protected, because it is from such exchanges that agreements, formal or informal, tacit or implicit, arise."[99] In other words, in order to meaningfully protect employees' rights of association and self-organization, Section 7 rights must extend to its precursors—that is, simple speech among employees about shared workplace concerns.

Recent Board cases illustrate the continuing relevance of Section 7. Today, "precursor speech" is far more likely to occur by electronic means. For example, in *Timekeeping Systems, Inc.*,[100] the Board found the employer in violation of Section 7 when it terminated an employee for circulating an email critical of a proposed change in the company's vacation policy. The Board found that the email clearly constituted "concerted activity" for "mutual aid or protection" because it was intended to inform co-workers about the effects of the proposed change and to elicit their opposition to the policy. More recently, the Board has considered the application of Section 7 to employee speech off duty on social networking sites like Facebook.[101]

94. 29 U.S.C. § 157 (2006) (emphasis added).

95. *See, e.g.*, NLRB v. Wash. Aluminum Co., 370 U.S. 9 (1962); NLRB v. Phx. Mutual Life Ins. Co., 167 F.2d 983 (7th Cir.), *cert. denied*, 335 U.S. 845 (1948); NLRB v. Guernsey-Muskigum Electric Coop., Inc., 285 F.2d 8 (6th Cir. 1960).

96. Charles J. Morris, *NLRB Protection in the Nonunion Workplace: A Glimpse at a General Theory of Section 7 Conduct*, 137 U. PA. L. REV. 1673, 1701 (1989).

97. *Id.*

98. *Id.*

99. *Id.* at 1704.

100. 323 N.L.R.B. 244 (1997).

101. NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (12–31), Jan. 24, 2012 (updating earlier report by describing additional cases concerning employees' use of social media and employers' social medial policies and rules); NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (11–74), Aug. 18, 2011 (describing recent claims of interference with protected rights based on employees' use of social media and Board responses). *See also* Melanie Trottman, *Workers Claim Right to Rant on Facebook*, WALL ST. J., Dec. 2, 2011, at B1 (explaining that more than 100 charges have

In recent months, it has filed charges against employers for disciplining or terminating employees who exchanged comments about shared workplace concerns such as late paychecks,[102] or unfair treatment by supervisors.[103] At the same time, it has declined to pursue other charges on the grounds that the employees' posted complaints about their employer were merely individual gripes, rather than looking to group activity.[104] Although the law as applied to electronic communications is still developing, the Board's pursuit of charges involving employee use of social media demonstrates its continuing concern with protecting collective employee speech, even as that speech moves online.

In addition to collective speech, the law recognizes the social value of individual employee speech in numerous other contexts. In particular, as legislatures have stepped in to regulate the workplace in various ways, they have also created causes of action to protect individuals from retaliation for asserting their rights under those statutes. For example, Congress has not only forbidden discrimination in employment on the basis of protected characteristics such as race, sex, or age; it also prohibits employers from retaliating against an employee who complains about such discrimination.[105] Similarly, laws that establish minimum wage and overtime entitlements or require compliance with health and safety standards also protect employees from retaliation when they speak up to assert their rights to pay, or to a safe workplace.[106] These statutory schemes establish regulatory standards for the workplace, but rely primarily on aggrieved individuals to enforce their rights either through private lawsuits or by triggering agency action through their complaints. By including these anti-retaliation provisions, Congress recognized that effective enforcement of its policies depends upon employees having the freedom to speak up about violations. Such speech about potential regulatory violations serves not only the individual employee's private interest, but also society's interests in seeing its

been filed with the NLRB by employees alleging that they were terminated because of their communications on social media sites).

102. Bay Sys Tech., 357 N.L.R.B. 28 (2011).

103. *American Medical Response of Conn., Inc.*, NLRB No. 34-CA-12576 (complaint issued on Oct. 27, 2010). The case was settled before the hearing. Michelle Amber, *Connecticut Company Settles ULP Charges Prior to ALJ Hearing in Facebook Firing Case*, 25 BNA DAILY LAB. REP. A-2 (Feb. 7, 2011).

104. NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (12–31), Jan. 24, 2012 (explaining why several of the social media cases described did not result in the Board filing charges against the employer); NAT'L LABOR RELATIONS BD., REPORT OF THE ACTING GENERAL COUNSEL CONCERNING SOCIAL MEDIA CASES (11–74), Aug. 18, 2011 (same).

105. 42 U.S.C. § 2000e-3(a) (2006).

106. 29 U.S.C. § 660(c) (2006); 29 U.S.C. § 215(a)(3) (2006).

policies enforced and in learning about the efficacy of existing regulation.[107]

The Supreme Court has recognized the importance of these anti-retaliation provisions in achieving legislative goals.[108] Noting that the purpose of Title VII's anti-retaliation provision is to "[m]aintain[] unfettered access to statutory remedial mechanisms,"[109] it explained that "Title VII depends for its enforcement upon the cooperation of employees who are willing to file complaints and act as witnesses."[110] The anti-retaliation provision "helps ensure the cooperation upon which accomplishment of the Act's primary objective depends."[111] The Court has similarly described the function of the anti-retaliation provision found in the Fair Labor Standards Act. In order to enforce FLSA's wage and hour standards, Congress chose to rely "not upon 'continuing detailed federal supervision or inspection of payrolls,' but upon 'information and complaints received from employees seeking to vindicate rights claimed to have been denied.'"[112] Recognizing the crucial role played by employee speech in enforcing statutory workplace regulations, the Court has consistently interpreted these anti-retaliation provisions liberally.[113]

107. *See* Estlund, *supra* note 91, at 111 ("[P]rivate employees may provide information to the public about how private firms operate with regard to working conditions, product safety, environmental practices, and other matters in which the society has a well-established regulatory interest.").

108. *See* Richard Moberly, *The Supreme Court's Antiretaliation Principle*, 61 CASE W. RES. L. REV. 375, 378 (2010) (arguing that Court's underlying rationale in retaliation cases "focuses on the notion that protecting employees from retaliation will enhance the enforcement of the nation's laws"). Moberly asserts that the Court recognizes that antiretaliation protections are "a law-enforcement tool that benefits society, rather than simply [ ] extra protection for employees provided at a cost to employers." *Id*. at 380.

109. Burlington-Northern & Santa Fe Ry. Co. v. White, 548 U.S. 53, 64 (2006) (quoting Robinson v. Shell Oil Co., 519 U.S. 337, 346 (1997)).

110. *Burlington-Northern*, 548 U.S. at 67.

111. *Id.*

112. Kasten v. Saint-Gobain Performance Plastics Corp., 131 S. Ct. 1325 (2011) (quoting Mitchell v. Robert DeMario Jewelry, Inc., 361 U.S. 288, 292 (1960).

113. *See, e.g.*, *Burlington-Northern*, 548 U.S. at 68 (holding that Title VII's prohibitions are not limited to actions that affect the terms, conditions or status of employment, but extend to any retaliatory action that a reasonable employee would find "materially adverse"); *Robinson*, 519 U.S. at 341 (holding that Title VII's protection against retaliation applied to former employees, even though the literal statutory language mentions only "employees"); Crawford v. Metro. Gov't of Nashville & Davidson Cnty., Tenn., 555 U.S. 271, 273 (2009) (holding that prohibition on retaliation for "opposing" any unlawful practice protects employee who did not initiate a complaint, but reported sexually harassing conduct by a co-worker during the employers' internal investigation); Thompson v. N. Am. Stainless, 131 S.Ct. 863, 870 (concluding that employee fired because his fiancée filed a sex discrimination complaint against their employer is protected by Title VII antiretaliation provision) (2011); *Kasten*, 131 S.Ct. at 1329 (holding that antiretaliation provision in FLSA protects oral as well as written complaints); Gomez-Perez v. Potter, 553 U.S. 474, 477 (2008) (holding that a federal employee may assert a claim for retaliation under the federal-sector provision of the Age Discrimination in Employment Act).

Not only does the law encourage employee speech to enforce workplace regulations, it also recognizes that employees have a critical role to play in exposing other forms of employer wrong-doing that violate established societal rules or norms. Initially, state courts created legal protection for whistleblowers by extending the common law tort of wrongful discharge to employees who were fired because they objected to or reported illegal or unethical activities by their employers.[114] As recognition spread that employees could play an important role in exposing wrong-doing and corruption, a variety of state and federal statutes sought to protect whistleblowers from retaliation.[115] Many of these statutes, however, are quite narrow in coverage, limiting protection to certain types of workers or certain types of reports.[116]

In the Sarbanes-Oxley Act of 2002,[117] Congress responded to this uneven patchwork of protections by creating broader whistleblower protections for employees of publicly traded companies. The collapse of Enron and other corporate failures the previous year had heightened concern over financial misconduct, while illustrating the difficulty that outside monitors faced in detecting fraud when they had only limited information about the complex inner workings of a firm. Many thought that corporate wrong-doing could be more easily detected if those with inside information—employees—were encouraged to report problems. Thus, Sarbanes-Oxley included a number of provisions intended to encourage whistleblowing, such as prohibiting retaliation against employees who report corporate fraud,[118] and requiring corporations to create channels for employees to report misconduct internally.[119]

114. *See, e.g.*, Adler v. Am. Standard Corp., 538 F. Supp.572, 580 (D.Md. 1982); Sheets v. Teddy's Frosted Foods, 427 A.2d 385, 389 (Conn. 1980); Harless v. First Nat'l Bank, 246 S.E.2d 270, 276 (W.Va. 1978).

115. For comprehensive listings of whistleblower laws, see WESTMAN & MODESITT, *supra* note 11; Elletta S. Callahan & Terry M. Dworkin, *The State of State Whistleblower Protection*, 38 AM. BUS. L.J. 99 (2000).

116. *See* Callahan & Dworkin, *supra* note 115, at 104–05.

117. Sarbanes-Oxley Act of 2002, Pub.L. 107-204, 116 Stat. 745 (codified as amended at 15 U.S.C. §§ 7201–7266).

118. As reported by Professor Richard Moberly, cases brought under Sarbanes-Oxley's antiretaliation provisions have been spectacularly unsuccessful. *See* Richard E. Moberly, *Unfulfilled Expectations: An Empirical Analysis of Why Sarbanes-Oxley Whistleblowers Rarely Win*, 49 WM. & MARY L. REV. 65 (2007) [hereinafter Moberly, *Unfulfilled Expectations*].

119. *See* Richard E. Moberly, *Sarbanes-Oxley's Structural Model To Encourage Corporate Whistleblowers*, 2006 BYU L. REV. 1107 (2006) [hereinafter Moberly, *Structural Model*]. Sarbanes-Oxley also places obligations on certain highly placed corporate actors to respond to suspected wrong-doing, obligations which Elizabeth Tippett has argued amounts to a form of compelled whistleblowing. Elizabeth C. Tippett, *The Promise of Compelled Whistleblowing: What the Corporate Governance Provisions of Sarbanes Oxley Mean for Employment Law*, 11 EMP. RTS. & EMP. POL'Y J. 1, 13–15 (2007).

In the wake of the financial crisis of 2008, Congress acted again to increase incentives for employees to report corporate wrong-doing. The Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010[120] strengthens the protections provided to whistleblowers under Sarbanes-Oxley by expanding coverage of its anti-retaliation provisions and addressing some of its perceived shortcomings. In addition, Dodd-Frank creates a "bounty" system that financially rewards whistleblowers who provide certain types of information regarding violations of commodities or securities law. Although Dodd-Frank's whistleblower provisions—particularly the bounty provisions—are controversial, the underlying assumption of the legislation is clear: corporate wrong-doing is more likely to be detected if employees are encouraged to speak up and report violations.

The law, then, clearly recognizes the social value of certain types of employee speech, particularly speech that is critical of the employer. Section 7 of the NLRA protects collective speech because it is essential to employees' rights of association and self-organization. A wide variety of statutes regulating the workplace also protect employee speech from retaliation as a means of enforcing those policies. And a growing body of whistleblower protections reflects the belief that employee speech plays an important role in preventing or revealing corporate wrong-doing. Employee speech may be valuable for other reasons as well. Some have argued for broad employee speech protections because of the importance of self-expression, or because of the benefits—both intrinsic and instrumental—of employee voice and participation in workplace governance.[121] These values are less consistently protected by current doctrine, but to the extent that one believes that they are worthy of protection, they, too, will be affected by diminished employee privacy as explored in the next section.

IV. THE CONNECTION BETWEEN SPEECH AND PRIVACY

When considering speech in the public arena, courts and scholars have often viewed First Amendment values to be in tension with privacy rights.[122] The focus on press freedoms in First Amendment case law em-

120. Dodd–Frank Wall Street Reform and Consumer Protection Act, Pub.L. 111-203, H.R. 4173 (2010) (codified as amended at 12 U.S.C. §§ 5301–5641).

121. *See* Estlund, *supra* note 91, at 106–09 (arguing for the intrinsic value of employee speech for individual autonomy and its intrinsic and instrumental value in fostering informed self-governance in the workplace).

122. *See, e.g.*, cases cited *supra* note 13; Peter B. Edelman, *Free Press v. Privacy: Haunted by the Ghost of Justice Black*, 68 TEX. L. REV. 1195, 1196 (1990); Harry Kalven, Jr. *Privacy in Tort Law: Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROBS. 326, 327 (1966); Neil M. Richards, *The Limits of Tort Privacy*, 9 J. TELECOMM. & HIGH TECH. L. 357, 365–71 (2011); Diane L. Zimmer-

phasizes the occasions in which the two interests conflict—for example, when the subject of a news story asserts a tort claim against a media defendant for emotional injury caused by the disclosure of private facts.[123] By contrast, in the workplace, scholars have recognized that speech and privacy interests are sometimes inter-related.[124] Both speech and privacy, it is asserted, are fundamental dignitary interests—areas in which employees ought to be allowed to exercise autonomy absent some clear business interest on the part of the employer. At times these claims overlap, for example, when an employee objects that an adverse personnel action was based on the contents of her email or her online activities off duty. Her claim might be framed in terms of an invasion of privacy—an unwarranted intrusion on matters that should be protected from employer scrutiny. Alternatively, her complaint might be cast in terms of speech rights, asserting unlawful retaliation because of the contents of her speech.

However, these interests do not merely overlap on occasion, for the connection between privacy and speech goes deeper. As Professor Neil Richards asserts, some degree of privacy is essential to free speech. He writes, "In order to speak, it is necessary to have something to say, and the development of ideas and beliefs often takes place best in solitary contemplation or collaboration with a few trusted confidants. To function effectively, these processes require a measure of . . . 'intellectual privacy'."[125] Privacy theorists have pointed out that awareness that one is observed has a "deep effect" on the subject,[126] often chilling potential speech. When assessing the effects of wiretapping phone lines, a Presidential commission once noted that "[f]ear or suspicion that one's speech is being monitored . . . can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas."[127] Similarly, Justice Sotomayor recently observed that awareness that one is being observed "chills associational and expressive freedoms."[128]

man, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 293 (1983).

123. *See, e.g.*, Doe v. Star Telegram, 864 S.W.2d 790, 792 (Tex. App. 1992), *rev'd on other grounds*, 915 S.W.2d 471 (Tex. 1995).

124. *See, e.g.*, FINKIN, *supra* note 1, at 488–531 (discussing employee interests in association and expression as aspects of privacy); Yamada, *supra* note 91, at 45 (suggesting that electronic surveillance should be considered both a privacy and free-speech issue).

125. Richards, *supra* note 14, at 389.

126. *Id.* at 403.

127. PRESIDENT'S COMM'N ON LAW ENFORCEMENT AND ADMIN. OF JUSTICE, THE CHALLENGE OF CRIME IN A FREE SOCIETY 202 (1967).

128. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). *See also* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 62 VAND. L. REV. 1609, 1651 (1999) ("when

Surveillance not only inhibits individuals from expressing their ideas, it also tends to warp the way in which those ideas are formed. As Julie Cohen writes:

> "the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior. Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream, . . . [resulting in] a blunting and blurring of rough edges and sharp lines."[129]

Pervasive monitoring thus tends to discourage the exploration of unconventional or dissenting views. This monitoring might take the form of observing an individual's intellectual activities—books read, websites visited, and the like—or of capturing his communications with others. Richards argues that both types of intrusion threaten intellectual privacy by chilling the exploration of new ideas.[130] Private communications, in particular, are critical in allowing the individual to gather information, ask questions and test out tentative conclusions free from public scrutiny.[131] In the absence of some zone of privacy for exploration and testing of new ideas, speech is less likely to serve its function of challenging existing orthodoxies or advancing new perspectives.

Richards, Cohen, and other theorists like them are concerned with participation in the public sphere—the kinds of speech central to truth-seeking and democratic self-governance. One might object that the workplace is different—it is a site for productive labor, not self-expression. And although many have advanced a vision of democratic self-governance in the workplace, that ideal has not been consistently embraced.[132] However, one need not accept the goal of a democratic workplace to recognize that employee speech *does* play an important role. As seen in Part III above, collective speech, speech that enforces workplace regulation and speech that deters wrong-doing are highly valued and explicitly protected by law. And to that extent, observations about the necessity of privacy to make speech rights meaningful are applicable in the workplace as well.

widespread and secret surveillance becomes the norm, the act of speaking or listening takes on a different social meaning").

129. Cohen, *supra* note 14, at 1426.

130. Richards identifies four areas in which intellectual privacy is protected and nurtured. Richards, *supra* note 14, at 408–25. I focus on the last two of these as most relevant to the workplace.

131. *Id.* at 421–25.

132. Cynthia Estlund, a strong proponent of increased employee voice in the workplace, acknowledges that "the ideal of workplace democracy is at best contested." Estlund, *supra* note 91, at 108.

Significantly, the kinds of speech valued in the workplace are oppositional.[133] When workers join together to speak collectively, it is because they are dissatisfied with some term or condition of their employment and wish to change it. When an employee objects to sexual harassment by a supervisor, or reports a failure to pay overtime to the Department of Labor, she is criticizing her employer's lack of compliance with the law. And when a whistleblower raises questions about the legality of his employer's business practices, he may be speaking against the prevailing ethos of the firm.

Employers generally do not like it when employees speak up in these ways, which is precisely why the law steps in to protect these speakers from retaliation. However, simply forbidding retaliation is not enough to ensure that socially valued speech is actually produced.[134] The employer need not actually retaliate: employees' fear of retaliation may be enough to discourage oppositional speech. Anti-retaliation remedies can be invoked only after the employee has suffered discharge or discipline, and offer, at best, the possibility of an uncertain remedy after a long delay. Moreover, as Estlund points out, much of this speech has the characteristics of a "public good": it may produce benefits far beyond the individual speaker, but she alone bears the costs of speaking.[135] Given the difficulties of pursing a retaliation claim, she argues, "all but the most intrepid employees will be deterred, or 'chilled' from speaking out in ways that might provoke the employer's displeasure."[136]

To put the point more directly, speaking out at the workplace in the ways that the law encourages is hard. Not only is there no guarantee of protection against retaliation at the outset, but the employee also will be highly uncertain about the effect of her speech. For example, an employee may wish to join with others to address a workplace concern, but prior to speaking, she is unlikely to know if they share her concerns. Workplace regulations can be complex, and so the employee considering complaining about her treatment at work may not be sure that she has a valid claim. A

133. As Estlund points out, employers dislike the types of private employee speech protected by law precisely because they "bring[] information to the public or spread[] ideas among the workforce that may threaten the employer's chosen way of doing business." *Id*. at 133.

134. *See id.* at 132–35 (explaining why employers will retaliate and employees fail to speak, even when retaliation if prohibited); Moberly, *Unfulfilled Expectations*, *supra* note 118, at 153 (concluding that Sarbanes-Oxley fails to protect employee whistleblowers as originally intended); Moberly, *Structural Model*, *supra* note 119, at 1126–31 (explaining why anti-retaliation provisions alone are insufficient to overcome barriers to whistleblowing); Tippett, *supra* note 119, at 16–24 (explaining why antiretaliation provisions are both overbroad and fail to adequately encourage whistleblowing).

135. Estlund, *supra* note 91, at 111.

136. *Id.* at 135.

potential whistleblower faces a similar dilemma. She may suspect that her employer is engaged in financial wrong-doing, but be uncertain whether what she has observed actually constitutes a violation of law.[137]

In each of these situations, anti-retaliation provisions protect the employee *after* she speaks out. However, a different kind of protection—protection from monitoring and surveillance—may be necessary *before* the employee speaks. Employees may need some space to seek information, to explore ideas and discuss concerns with others before they are ready to speak in the ways that the law most values. In order to take concerted action, employees may first need to coordinate their efforts by speaking privately amongst themselves. However, awareness that their employer is monitoring their communications will likely chill those conversations.[138] If employees are unable to communicate about shared workplace concerns without employer scrutiny, collective speech is unlikely ever to emerge. Similarly, the employee who contemplates asserting her statutory rights may need to talk to other employees or seek additional information from a public agency or attorney. For example, she may not even realize that she is being paid less or treated differently without talking to co-workers.[139] The process of consultation—in the form of private communications—may be an important first step before an employee asserts rights legally granted her at work.

Some measure of privacy is likely necessary to encourage the whistleblower as well. The obstacles to whistleblowing are well-documented in the literature. Not only does the potential whistleblower risk employment retaliation and the material losses that accompany it, she may also face social ostracism by her peers and public disapproval for her "disloyalty."[140]

137. The Sarbanes-Oxley Act protects employees who provide information regarding conduct "which the employee reasonably believes constitutes a violation" of certain laws listed in the statute. Although the statute only requires a "reasonable belief," this provision has been interpreted to require the employee to show the conduct specifically relates to securities fraud, or one of the other specific causes of action. *See, e.g.*, Day v. Staples, Inc., 555 F.3d 42 (2009).

138. *See, e.g.*, Carl Botan, *Communication Work and Electronic Surveillance: A Model for Predicting Panoptic Effects*, 63 COMM. MONOGRAPHS 293, 309 (1996) (reporting survey results suggesting that workplace surveillance is inimical to communications among co-workers).

139. *See, e.g.*, Ledbetter v. Goodyear Tire & Rubber Co., 550 U.S. 618 (2007). Many employers have policies forbidding employees from discussing how much they are paid, even though they are illegal. *See, e.g.*, Radisson Plaza Minneapolis, 307 N.L.R.B. 94 (1992); Heck's, Inc., 293 N.L.R.B. 1111,1113 (1989).

140. *See, e.g.*, Miriam A. Cherry, *Whistling in the Dark? Corporate Fraud, Whistleblowers, and the Implications of the Sarbanes-Oxley Act for Employment Law*, 79 WASH. L. REV. 1029 (2004); Yuval Feldman & Orly Lobel, *The Incentives Matrix: The Comparative Effectiveness of Rewards, Liabilities, Duties, and Protections for Reporting Illegality*, 88 TEX. L. REV. 1151 (2010); Geoffrey Christopher Rapp, *Beyond Protection: Invigorating Incentives for Sarbanes-Oxley Corporate and Securities Fraud Whistleblowers*, 87 B.U. L. REV. 91 (2007).

The whistleblower must overcome psychological barriers as well. She may experience the cognitive dissonance of questioning the activities and motives of colleagues and superiors in an organization to which she devotes her professional energies. As Professor Geoffrey Rapp explains, whistleblowing causes psychological pain because "it requires deviation from a group." The whistleblower must "accuse members of her professional and, oftentimes, social group of wrongdoing—something that can undermine the employee's own identity with the group."[141] Like the dissident speaker in the public sphere, the potential whistleblower may require a measure of intellectual privacy in order to overcome these psychological barriers to dissenting.

Just as in public discourse, then, valuable workplace speech does not often arise spontaneously and fully formed. Employees may need to communicate privately with others—to explore ideas and options, to consider what they believe—before they are certain what they want to say or even realize that they have something to say. They may need to ask questions and seek information before they feel confident speaking out, particularly when that speech is critical or runs contrary to the prevailing norms of the organization. Protecting and encouraging socially valuable speech at work thus requires protecting the precursors to speech, such as the ability to gather information and to communicate with others privately.

One might argue that protecting employee privacy is unnecessary because the employee can avoid scrutiny simply by undertaking her intellectual exploration or private communications at home. However, as discussed in Part I, *supra*, the line between home and work is growing more difficult to maintain. Employers increasingly assert an interest in their employees' electronic communications off duty, and have sometimes used technological tools to monitor them. In other instances, employers have used their managerial authority over workers to discover these communications, by, for example, requesting or requiring the disclosure of personal passwords. In order for life away from work to be a haven for nurturing speech, greater protections may be needed to restrict employers' ability to scrutinize their employees' off duty activities.

Even if employees' off duty activities are protected, the importance of privacy in nurturing valuable speech argues for some, albeit reduced, privacy protections in the workplace. The types of activities that are precursors to valuable employee speech are not necessarily undertaken self-consciously. If a worker suspects she is being discriminated against, she

141. Rapp, *supra* note 140, at 123.

may seek out legal advice off duty, carefully segregating these communications from channels that could be observed by the employer. Sometimes, however, the employee's movement toward speaking out might evolve unexpectedly, as when an exchange with a co-worker suggests a disparity in pay, or an off-hand complaint reveals shared concerns about working conditions. These types of communications are most likely to occur at work; however, constant monitoring and surveillance of employee activities can have an inhibitory effect. Thus, as in the public sphere, protecting and encouraging valuable employee speech requires that the potential speaker be afforded some "breathing space."[142]

The deep connection between privacy and speech suggests that more is at stake in protecting employee's privacy than avoiding subjective hurt feelings. Some courts have rejected the wrongful discharge claims of employees asserting privacy rights. They have reasoned that privacy rights are "private" by definition and cannot be the basis for a "public" policy exception limiting an employer's power to fire at will.[143] As I have argued elsewhere, this semantic argument misapprehends the nature of privacy, which reflects fundamental normative practices of a community.[144] The connection between privacy and speech highlighted here suggests another *public* dimension to employee privacy. Because employee privacy plays a crucial role in nurturing socially valued employee speech, protecting that privacy also promotes the broader public values advanced by that speech.

CONCLUSION

Observing the contemporary workplace, one can discern two distinct trends. On the one hand, changes in the organization of work and changes in technology appear to be eroding employees' privacy—particularly their ability to gather information or communicate through electronic media free from employer scrutiny. On the other hand, certain types of employee speech have been recognized as socially valuable and subject to increased legal protection and encouragement. These two trends are in tension because employees' privacy and speech interests are not wholly independent of one another. Rather, as in the public sphere, protecting socially valuable speech may require providing some measure of privacy in order to encour-

142. *See* NAACP v. Button, 371 U.S. 415, 433 (1963) ("First Amendment freedoms need breathing space to survive.").

143. *See, e.g.*, Luck v. Southern Pac. Transp. Co., 267 Cal. Rptr. 618, 635 (Cal. Ct. App. 1990) (claiming that the "right to privacy is, by its very name, a private right, not a public one" and therefore could not be the basis for a public-policy exception to the at-will rule).

144. *See*, Kim, *supra* note 27, at 724–29.

age the potential speaker, particularly the one who might raise a critical or dissenting voice.

Noticing this connection between employee privacy and speech does not solve the difficult challenges of balancing employees' privacy and employers' managerial interests. It does, however, suggest that these two interests are not the only ones at stake. Diminished employee privacy has an impact beyond the affected individual, because it undermines the law's efforts to protect and encourage socially valuable forms of speech. Recognizing this fact may affect how the competing interests are weighed. If employee privacy is viewed as protecting only the subjective hurt feelings of the employee, it is too easily outweighed by an employer's asserted business interests. By contrast, understanding the role that privacy plays in fostering valuable employee speech adds some heft to the privacy side of the balance.