Electronic Privacy and Employee Speech

Pauline T. Kim*

I. 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—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, 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.

* 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 very helpful comments on this paper.

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. 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 26, 29, 42 U.S.C.). 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 (forthcoming NW. L. REV. 2011).

Although these and other types of privacy issues may also be affected by the developments that I discuss 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.
Employers have retrieved and read highly personal communications among intimates sent over work-provided equipment. 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. In other cases, employers have seized personal passwords or used forensic techniques to access email exchanged on employees’ personal email accounts.

As these and other incident 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. At the same time, technological advances are making it easier for employers to capture ever more detailed and comprehensive information about their employees’ communications and activities on and off-duty. 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.

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

---

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

4 Office of the General Counsel, NLRB, Report of the General Counsel, Jan. 24, 2012 (updating earlier report by describing additional cases concerning employees’ use of social media and employers’ social medial policies and rules); Office of the General Counsel, NLRB, Report of General Counsel, 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).


8 See, e.g., William A. Herbert. The Electronic Workplace: To Live Outside the Law You Must Be Honest, 12 EMPLOYEE RIGHTS AND EMPLOYMENT POLICY JOURNAL 49 (2008); Nolan, supra note --; Sprague, supra note --.
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 attempt to deter corporate wrongdoing that has undermined confidence in the financial system.12

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 interests 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

---

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., Sheets v. Teddy’s Frosted Foods, Inc., 427A.2d 385 (Conn. 1980); White v. General Motors Corp., 908 F.2d 669 (10th Cir. 1990); Boyle v. Vista Eyewear, Inc., 700 S.W.2d 859 (Mo. App. 1985); Garemba v. Lucky Food Stores, Inc., 726 F.2d 1367 (9th Cir. 1984). 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).
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. In the context of the workplace, these insights suggest that socially valued forms of speech may be less likely to be produced without some measure of 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 II 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 III briefly surveys the limitations of existing law in protecting employee privacy given these developments. In Part IV, I turn to a consideration of employee speech interests, arguing that 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 the protected forms of employee speech and employees’ interest in privacy is explored in Part V. Drawing on theories about the importance of privacy in fostering speech and participation in public discourse, I argue that some measure of workplace privacy is also necessary to encourage socially valued forms of employee speech. Part VI concludes.

II. 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, 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. This inquiry has

15 See, e.g., Richards, supra note ----, at 403-04.

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 MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 615-971 (3d ed. 2009). 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. § 31-40s (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. Philadelphia, 812 F.2d 105 (3d Cir. 1987). The Supreme Court recently rejected such a privacy claim
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 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 brought by employees of a government contractor. National Aeronautics and Space Administration 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.


19 *Id.* at 715.

20 *Id.* at 715.

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. 480 U.S. at 729-30 (J. Scalia, 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.


23 *Id.* at 719-20.

to redress perceived violations of their privacy rights. The common law tort most relevant to the employment 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.” 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 of a right of privacy in both the locker itself and those personal effects within it.” Conversely, in *O'Bryan v. KTIV Television*, the court concluded that an employee lacked a “reasonable expectation of privacy” that his desk and office area would not be searched for work-related documents.

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 protects employees’ personal effects and shields them from observation in traditionally private spaces such as a restroom or dressing room. Similarly, the common law tort protects employees’ privacy in

---

26 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. National Collegiate Athletic Assn*, 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 a 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).

27 Restatement (Second) of Torts § 652B (1977).


30 *See*, e.g., *K-Mart Corp. v. Trotti*, 677 S.W.2d 632 (Ct. App. Tex. 1984) (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., *Kjerstad v. Ravellette Publications, Inc.*, 517 N.W.2d 419 (S.D. 1994) (upholding jury verdict for plaintiffs on invasion of privacy claim based on employer’s surreptitious observation of employees in bathroom).
traditionally secluded off-duty locations such as a home or hotel room. 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 of privacy when employers have searched for work-related documents in an employee’s office and desk or for contraband in an employee’s car parked on the employer’s premises. 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 been critical of the level of legal protection afforded employee privacy under constitutional and common law doctrines. Some have criticized application of a “reasonable expectation of privacy” test that looks first to employer policies and practices, rather than existing social norms. Such an approach permits employers to destroy any employee expectations of privacy simply by announcing privacy-invading practices in advance, and regularly carrying them out. 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.” Regardless of the merits or deficiencies of existing law when applied to 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 III, infra.

__________________________


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


37 See, e.g., Mayer, supra note --, at 643-45.

38 See Finkin, supra note ---, at 226.

39 Finkin, supra note ---, at 240.
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. 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.\textsuperscript{40} Often, the work relationship was also a domestic one, with the servant residing with the master.\textsuperscript{41} In the mid-twentieth century, however, the modern organization of work clearly separated home and paid work, and the protection of employee privacy was one means of policing that boundary.\textsuperscript{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.\textsuperscript{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.\textsuperscript{44}

Unwilling to promise long term job security, firms now encourage employees to develop affective ties to the workplace to induce employee loyalty.\textsuperscript{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.’”\textsuperscript{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

\textsuperscript{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).

\textsuperscript{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).


\textsuperscript{44} Marion Crain, Managing Identity: Buying Into the Brand at Work, 95 IOWA L. REV. 1179, 1192-95 (2010).

\textsuperscript{45} Id. at 1197-98.

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 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.”

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.” 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.” And thus, Justice Blackmun rejected the plurality’s suggestion that an employee could protect personal belongings “by simply leaving them at home” as insensitive to the “operational realities of the workplace.”

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 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

47 Crain, supra note ---, at 1179.
48 480 U.S. at 739 (J. Blackmun, dissenting).
49 Id.
50 Id. at 740.
separate phone lines for employees’ personal use. In addition, the law restricted the employer’s ability to capture purely personal phone calls. Today, an employee might use a work computer during a break to check a website for information regarding a medical condition or send a quick 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.

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. 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 terminated because of their blog posts, and members of

---

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. Village 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 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 The Supreme Court recently confronted such a situation in City of Ontario v. Quon, 130 S. Ct. 2619 (2010), in which 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, employee use of employer-provided equipment for personal communications is a much broader phenomenon.

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

While employers have always had an interest in monitoring their employees’ activities, technological change has increased both their 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 their off-duty activities, when amplified by the internet, have the potential to cause harm to a firm’s public image.

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 use by monitoring time spent, content or keystrokes entered. 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. A few employers have reportedly required current or prospective employees to provide their usernames and passwords for Facebook or private chat groups. In addition, software is now available that employers can use


56 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); Office of the General Counsel, NLRB, Report of the General Counsel, Jan. 24, 2012 (updating earlier report by describing additional cases concerning employees’ use of social media and employers’ social medial policies and rules); Office of the General Counsel, NLRB, Report of General Counsel, Aug. 18, 2011 (describing recent claims of interference with protected rights based on employees’ use of social media and Board responses).

57 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.


59 See, e.g., Alexis Madrigal, Should Employers Be Allowed to Ask for Your Facebook Login?, The Atlantic, available at: http://www.theatlantic.com/technology/archive/2011/02/should-employers-be-allowed-to-ask-for-your-
to automatically monitor their employees’ activities on social networking sites such as Facebook, Twitter and LinkedIn.  

III. 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, 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. The prohibitions contained in the ECPA, however, are subject to a number of exceptions—for example, when there is consent to the interception, or when the communication is accessed by the provider of the electronic communications service. Because 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. Although the ECPA could be interpreted in ways more protective of employee privacy, under current interpretations it provides rather weak protection against employer scrutiny of employees’ electronic communications.

---


61 18 U.S.C. §§ 2510 et seq. The ECPA 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).


64 18 U.S.C. § 2701(c)(1).


66 See, e.g., Levinson, supra note ---.

67 See Ariana R. Levinson, Workplace Privacy and Monitoring: The Quest for Balanced Interests, 59 CLEVELAND ST. L. REV. --- (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.
Given the uncertain protections of the ECPA, employees have also asserted privacy rights under constitutional and common law doctrines. As discussed in Part II. 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, 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. 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 an established societal understanding, many courts considering employees’ claims of 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 of privacy. Property ownership and technological feasibility, however, are not decisive in determining whether an expectation of privacy is reasonable. As Professors Bellia and Freiwald have argued, the “reasonable expectation of privacy” test should entail “normative rather than merely positive analysis.” 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. When the Supreme Court in Katz v. United States held that

\[\text{References omitted for brevity.}\]

68 See, e.g., O’Connor v. Ortega, 480 U.S. 709, 715.

69 See, e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Penn. 1996) (finding employee did not have reasonable expectation of privacy in messages sent over company owned e-mail system); McLaren v. Microsoft Corp., 1999 WL 339015 (Ct. App. Tex. 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); Muick v. Glenayre Electronics, 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 v. City of Reno, 932 F.Supp. 1232, 1234 (D. Nev. 1996) (finding expectation of privacy not objective reasonable given that recording and storing of pager messages are “an integral part of the technology”).

70 See, e.g., O’Connor v. Ortega, 480 U.S. 709, 740 n. 7 (1987) (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); Schwergerdt v. General Dynamics Corp., 823 F.2d 1328, 1233 (“Fourth Amendment privacy interests do not . . . turn on property interests”). 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 in note --, supra.

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

72 Id.; see also Mayer, supra note --. 
individuals have a reasonable expectation 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.”

Thus, courts could work to discern when new forms of monitoring implicate fundamental interests that warrant recognition and protection; however, they have for the most part declined to do so in the employment context. For example, the Supreme Court in City of Ontario v. Quon 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 “rapid changes in the dynamics of communications and information transmission.” In refusing to decide the issue, the Supreme Court failed to recognize that law is itself constitutive of what expectations of privacy are “legitimate.” 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, acknowledged this constitutive role of law. It found that 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. 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.” 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

---

74 Id. at 352.
75 130 S.Ct. 2619 (2010).
76 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.
77 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).
78 631 F.3d 266 (2010).
79 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.
80 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.
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. 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.”

The approaches taken by the Warshak court and Justices Sotomayor and Alito in Jones suggest that existing law could be interpreted in ways 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. 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. There is reason to be particularly skeptical of consent-based arguments when it comes to 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. Moreover, employers sometimes send

---


84 See, e.g., Sporer v. UAL Corp., 2009 WL 2761329, *5 (N.D. Cal. 2009)(finding that advance notice that a company monitors computer use diminishes employee’s expectation of privacy); 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); Muick v. Glanayre Electronics, 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); Thygeson v. U.S. Bancorp, 2004 WL 2066746 (D. Or. 2004)(holding employee had no expectation of privacy because he was warned that office computer could be monitored); Kelleher v. City of Reading, 2002 WL 1067442 (E.D. Pa. 2002)(finding no reasonable expectation of privacy where employer’s policy informed employees that email was not private). Cf. Curto v. Medical World Communications, Inc., 2006 WL 1318387 (E.D. N.Y. 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).

85 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 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, 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., 2006 WL 1318387 (E.D.N.Y. 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,
conflicting messages, maintaining an official policy against personal use of electronic systems while tolerating or even subtly encouraging such use.  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 employer’s 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 employees’ privacy in their electronic communications are only weakly protected from employer scrutiny.

IV. Socially Valued 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 rights to speak freely. Freedom of expression may be valued as a form of individual autonomy for the employee, but the workplace is generally not regarded as an appropriate forum for unrestricted expressive activity. In managing the 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.

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.

86 In Quon, for example, the City of Ontario asserted that text messages were included in its policy that computer messages were not private. 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.

87 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 EMPL. & L. LAW 1 (1998).

88 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,
Nevertheless, several types of employee speech have consistently been recognized to have social value—a public significance beyond whatever value they may hold for 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. Significantly, however, the language of section 7 extends not just to formal collective bargaining, but to employees’ right “to engage in concerted activity for . . . mutual aid or protection.” 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. As Professor Charles Morris explained, “[c]oncerted conduct . . . may not necessarily be intended to achieve union organization, at least not deliberately or initially.” 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.” They might not be “looking toward group action” initially, “but given the opportunity, group action—be it mild or assertive—might in time evolve from that rudimentary process.” 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.” In other words, in order to meaningfully protect employees’ rights of association and self-organization, section 7 rights must extent 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, 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 WESTERN RES. L. REV. 375, 430 (2010).

89 29 U.S.C. § 157. 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).


93 Id.

94 Id.

95 Id. at 1704.
In , 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. 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, or unfair treatment by supervisors. 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. 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. 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. 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

---

96 323 N.L.R.B. 244 (1997).
97 Office of the General Counsel, NLRB, Report of the General Counsel, Jan. 24, 2012 (updating earlier report by describing additional cases concerning employees’ use of social media and employers’ social media policies and rules); Office of the General Counsel, NLRB, Report of General Counsel, 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).
98 Bay Sys Technologies, LLC, NLRB, No. 5-CA-36314 (Decision and Order filed Aug. 2, 2011).
100 See Office of the General Counsel, NLRB, supra note ---- (explaining why several of the social media cases described did not result in the Board filing charges against the employer).
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 policies enforced and in learning about the efficacy of existing regulation.103

The Supreme Court has recognized the importance of these anti-retaliation provisions in achieving legislative goals. Noting that the purpose of Title VII’s anti-retaliation provision is to “[m]aintain[] unfettered access to statutory remedial mechanisms,”104 it explained that “Title VII depends for its enforcement upon the cooperation of employees who are willing to file complaints and act as witnesses.”105 The antiretaliation provision “helps ensure the cooperation upon which accomplishment of the Act’s primary objective depends.”106 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.’”107 Recognizing the crucial role played by employee speech in enforcing statutory workplace regulations, the Court has consistently interpreted these anti-retaliation provisions liberally.108

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

103 See Estlund, supra note ---, 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”).


105 Burlington-Northern, at 67.

106 Id.


108 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 --- (holding that Title VII’s protection against retaliation applied to former employees, even though the literal statutory language mentions only “employees”); Crawford v. Nashville, 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. North American Stainless, 131 S.Ct. 863, 870 (concluding that employee fired because his fiancee 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).
employees who were fired because they objected to or reported illegal or unethical activities by their employers. 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. Many of these statutes, however, are quite narrow in coverage, limiting protection to certain types of workers or certain types of reports.

In the Sarbanes-Oxley Act of 2002, Congress attempted to respond to this uneven patchwork of protections by creating broader whistleblower protections for employees of publicly traded companies. The collapse of Enron and other corporate failure 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 employee whistleblowing, such as prohibiting retaliation for speaking up about corporate fraud, and requiring corporations to create channels for employees to report misconduct internally.

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 strengthens the protections provided to whistleblowers under Sarbanes-Oxley by expanding coverage of its antiretaliation provisions and addressing some of its perceived shortcomings. In addition, Dodd-Frank creates a “bounty” system which 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

---


111 See, Callahan & Dworkin, supra note ----, at ----.

112 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 WILLIAM & MARY L. REV. 65 (2007).

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 wrongdoing. 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. 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.

V. 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. The focus on press freedoms in First Amendment case law emphasizes the occasions in which the two interests conflict—for example, when the subject of a news story asserts a tort claim for emotional injury caused by the disclosure of private facts against a media defendant. By contrast, in the workplace, scholars have recognized that speech and privacy interests are sometimes inter-related. 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 which 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.” Privacy theorists have pointed out that awareness that

---

114 See Estlund, supra note ---, 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).


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

118 Richards, supra note ---, at 389.
one is observed has a “deep effect” on the subject,\footnote{Id. at 403.} 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.”\footnote{President’s Comm’n on Law Enforcement and Admin. of Justice, The Challenge of Crime in a Free Society 202 (1967).} Similarly, Justice Sotomayor recently observed that awareness that one is being observed “chills associational and expressive freedoms.”\footnote{United States v. Jones, No. 10-1259, slip op. at 3 (Jan. 23, 2012) (Sotomayor, J., concurring).}

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.”\footnote{Cohen, supra note --, at 1426.} 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.\footnote{Richards identifies four areas in which intellectual privacy is protected and nurtured. Richards, supra note --, at 408-25. I focus on the last two of these as most relevant to the workplace.} Private communications, in particular, are critical in allowing the individual to gather information, ask questions and test out tentative conclusions free from public scrutiny.\footnote{Id. at 421-25.} 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.\footnote{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 ---, at 108.} 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 IV 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.
Significantly, the kinds of speech valued in the workplace are oppositional. 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 is 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. Anti-retaliation remedies are invoked only after the employee has been discharged or disciplined, 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. Given the difficulties of pursuing 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.”

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 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.

---

126 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.
127 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 ——, at 513 (concluding that Sarbanes-Oxley fails to protect employee whistleblowers as originally intended); Moberly, Structural Model, supra note ——, at 1126-31 (explaining why anti-retaliation provisions alone are insufficient to overcome barriers to whistleblowing).
128 Estlund, supra note ——, at 111.
129 Id. at 135.
130 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).
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, 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. 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.\footnote{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).} 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.”\footnote{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.”\footnote{Rapp, supra note ---, at 123.} 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 II, supra, the line between home and work is not always a clear one. Employers have increasingly asserted an interest in employee’s 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 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.”

VI. 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 encourage 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 adds some heft to the privacy side of the balance.

134 See NAACP v. Button, 371 U.S. 415, 433 (“First Amendment freedoms need breathing space to survive”).