J. INDIVIDUAL EMPLOYMENT RIGHTS, Vol. 5(3) 235-249, 1996-97

ELECTRONIC MAIL PRIVACY IN THE WORKPLACE: E-MAIL SHOWS NEED FOR LEGISLATIVE ACTION, BUT OPPORTUNITY MAY HAVE BEEN MISSED

DAVID M. SNYDER
Widener University School of Law
Harrisburg, Pennsylvania

ABSTRACT

One of the most rapidly evolving areas of employment law is privacy. Technological innovation in the workplace continually challenges our conceptions of privacy. E-mail is the latest tool to exceed the grasp of existing privacy law. The common law's inability to adapt to e-mail exemplifies the need for legislative action to protect employee privacy. This article explores possible legislative solutions and attempts to identify procedures that reflect the core values of those solutions.

One of the most rapidly evolving areas of employment law is privacy [1]. The right to privacy in general is a young concept, "discovered" in 1890 by Samuel Warren and Supreme Court Justice-to-be Louis Brandeis [1, 2]. The authors of *The Right to Privacy* were alarmed by the "modern enterprise and invention" of turn-of-the-century technology, particularly the rapid dissemination of information via the burgeoning field of mass communication [2]. The "instantaneous photographs and newspaper enterprise" threatened not only to "proclaim [ ] from the housetops" what was "whispered in closets" and ruin reputations, but also, Brandeis and Warren feared, to invade the "spiritual" value of the "inviolate personality" [2, p. 205]. Thus, invasion of privacy would cause damage beyond reputation to affect "the estimate of [one's] self and upon his feelings" [2, p. 197].

Since then, legal scholars have struggled to categorize the bundle of interests contained within the "inviolate personality." Dean Prosser reduced the privacy

doi: 10.2190/410E-V5CW-9DAC-5HJK
http://baywood.com

right to distinct causes of action protecting interests in reputation, intangible property, and freedom from emotional distress [3]. Conversely, scholars argued that tort cases involving privacy were "of one piece" and involved a single tort, an injury to individuality and dignity [4]. As early as thirty years ago, conceptualizing individual dignity and autonomy as a separate interest was considered essential to developing "new legal remedies" in response to the use of "modern technology," including "electronic storage of personal data" by "large-scale corporate enterprise" [4, p. 1006]. Today, many scholars still compile comprehensive "laundry lists" of the interests we intend to protect with a legal right of privacy [5]. Regardless of the conceptual source, the interests in protecting a private sphere in our lives remain paramount, and fear of intrusion on that sphere is still prompted by technological developments.

Electronic monitoring in the workplace entails both the informational and dignitary conceptions of privacy. In the employment context, privacy interests deserving protection are both informational privacy, or control of the use and distribution of employee information by the employer, and behavioral privacy, or the employee's personal autonomy to engage "in activities free from employer regulation . . . at and outside the workplace" [1, p. 10]. As technology makes monitoring more prevalent, both of these interests come more under the notice and control of the employer. As one present-day employment privacy lawyer has commented: "The question is whether you get inured to the lack of privacy or whether it makes privacy all that more important. It may be like the environment: the more we destroy our environment, the more precious the remainder of that environment becomes" [6].

TYPES OF MONITORING AND PRIVACY

The realm of electronic monitoring encompasses three general categories: telephone call accounting and service observation, video surveillance, and computer-based monitoring [7]. First, telephonic monitoring involves telephone call accounting, or recording the length, time, and destination of employee phone calls, and telephone service observation, where managers of industries where telephone skills are an "integral part of the employee's work" like long-distance operators, telemarketers, airline and travel clerks, may review the substance and content of the employees' performance [7]. Second, employers use video surveillance to detect theft or violation of workplace rules, or to observe work skills and habits in manufacturing or other "assembly line" type jobs [7]. Finally, computer-based monitoring includes not only recording the rate and number of repetitive tasks such as keystrokes, but auditing activities and "overwriting passwords" to view contents of files and, as discussed below, e-mail [7].

Electronic monitoring is used by employers to monitor the activities of their employees "continuously and secretly" [7]. A widely cited survey by *MacWorld* magazine showed a pervasive use of electronic monitoring in the workplace [8].

Surveying three hundred companies, representing a total of almost one million workers, the survey found that over 30 percent of business with 1000 employees or more routinely engaged in monitoring via computer [8]. Even among smaller businesses, who have less money for sophisticated computer systems, almost 22 percent admitted to computer monitoring [8]. As computer monitoring equipment becomes more affordable, it seems likely that its increased availability for small business will result in its increased use.

With the increased use of electronic monitoring has come a correlative increase in the stress-related disorders among workers. Monitored workers are more likely to suffer from stress-related ailments such as neck, back, and shoulder problems than those who were not monitored [9]. Psychologically, electronically monitored workers were almost 20 percent more likely to complain of depression, fatigue, and anxiety than nonmonitored workers [10]. In fact, studies have shown that discontinuing secret monitoring of telephone operators resulted in improved quality of service, decreased customer complaints, and fewer employee grievances [7]. Further, recent changes in many industries from the old adversarial labor-management system to one of employee participation and labor-management cooperation are viewed as "essential" to the success of American business in the "global marketplace" [7]. As a result of these changes, management consultants have concluded "monitoring that creates feelings of surveillance and stress is antithetical to the new cultures of management that our society is moving toward" [9]. Thus, electronic monitoring does touch on the "inviolate personality" to harm "the estimate of [one's] self" [2, p. 19]. However, should employees have to suffer physical and mental anguish before the law steps in to protect them?

The core values of privacy are reflected in the common-law "procedures" surrounding its attempted deprivation, and enforced in the tort law that has developed. Common-law actions for invasion of privacy, while not uniform, generally involve several factors: 1) whether the intrusion was intentional, 2) the location and private nature of the activity involved, 3) whether the intrusion is highly offensive to the reasonable person, and 4) whether the infringer had a legitimate business purpose for warranting the intrusion [11], and the search is reasonably calculated to further that purpose [9, p. 4]. Electronic monitoring presents unique concerns for issues in workplace privacy that complicate the application of the traditional common-law invasion-of-privacy analysis. These complications arise for several reasons: 1) the information derived by the employer is obtained "somewhat voluntarily" because it is usually through the employee's use of the employer's property, 2) because the employer's property is used, the employer has the right to prevent the abuse of that property, 3) the method of obtaining the information is not highly intrusive on the physical person of the employee, as in a drug test or strip search, and 4) employees have a general idea of the technological possibility that their computer can be monitored [12]. Thus, the common law reflects an agreement on *how* we should treat employees

when privacy is to be deprived, but not *when* an actual deprivation of privacy occurs.

In applying the common-law analysis to the workplace, the most troublesome requirement for a plaintiff to meet, and where "consensus" on privacy values breaks down, is that the employer's action must be considered "highly offensive to a reasonable person" [7, p. 1268]. This becomes even more difficult in cases of electronic monitoring in the workplace for several reasons. First, in the light of the "public nature of the workplace" [9, p. 143], it is considerably difficult to establish that a typical office work environment is an atmosphere where one expects privacy [9]. Second, the employee must show not just the existence of the monitoring but that a reasonable person would find it "highly objectionable" [7, p. 1267]. Typically, these "offensive" situations have involved employer monitoring of bathrooms and locker rooms, not files and conversations [7]. Finally, even if the employer's intrusion causes great distress to the plaintiff, some courts further require that the employer actually publish the information obtained via the monitoring to a third party before any right of privacy is breached [7, p. 1267]. Again, the difficulty of applying this factor to the workplace atmosphere reflects the ongoing lack of consensus over what "privacy" actually is.

One exception to that lack of consensus on definitions of privacy may exist under state constitutions. While ten states have constitutions that recognize privacy rights [11, pp. 174-175], only California has extended its constitutional amendment on privacy to nongovernment employers [13]. The ballot initiative on which the amendment was voted itself discussed the concern that advances in technology would result in a greater threat to privacy rights [13]. Using the ballot initiative as "legislative history," the courts extended the right of privacy to protect private employees against encroachments by private employers [12, pp. 330-331]. Employers were required to show a "compelling interest," such as safety, prior to drug testing [12, p. 330]. Because citizens of the state themselves determined that the privacy interests to be protected were "fundamental," the courts were able to avoid the question of "highly offensive" and put the burden on the employer to find the "least burdensome alternative" to further that interest [12, pp. 330-331]. However, while state constitutions are a powerful potential source of strong privacy rights, applying those rights to private actors does not seem to be a growing trend.

CASE IN POINT: ELECTRONIC MAIL

> A fierce struggle is shaping up over the definition of privacy in cyberspace, as evidenced by . . . a handful of e-mail privacy cases, rising public concern and renewed efforts to pass federal legislation [7, p. g1].

The debate surrounding electronic mail provides an example of how new communications technologies are instantly fraught with danger of privacy

invasion and the concurrent inability of common law to keep pace with technological developments. E-mail is a message sent from one computer user to another, either both using the same computer or using different computers connected by a network [14, pp. 104-105]. E-mail differs from regular mail in three ways that make it more susceptible to privacy intrusion. First, e-mail systems exist between (or among) private parties and thus are not regulated under the aegis of the postal laws [14]. In fact, the transmission and storage of e-mail is often under the supervision of the systems operator, who is either an employee of the employer or works for the service provider of which the employer is a client or customer [14]. Second, the system operator's power to supervise the e-mail means any messages sent may be not only intercepted without the knowledge of the sender or the receiver, but may be read via the backup messages that are kept stored on disk in the event of power or system failure [14]. Third, unlike paper mail or office memoranda, e-mail allows for almost instantaneous communication, so, like a telephone call, there is a greater spontaneity of communication and words are less carefully chosen [14]. Thus, e-mail allows employers to have a greater ability to monitor employees, while employees have less notice of the intrusion.

Aside from the mechanical aspects of e-mail, privacy concerns arise because the employer and employee have different perceptions of e-mail's role in the workplace. Employees consider e-mail to be similar to a personal letter, a perception bolstered by the "personal" passwords issued by the employer necessary to gain access to the system [9, p. 141]. Also, employers often encourage their employees to use the e-mail to replace the telephone, fax, or the standard office memo in communicating with their coworkers or customers. Thus, employees develop an expectation (in the personal sense, if not the legal sense) that their e-mail messages are their own personal property [9, p. 142]. In contrast, despite encouraging their employees to become "comfortable" using e-mail to conduct daily business, employers consider e-mail to be a business tool, used on equipment owned by the employer, and therefore may be used only for business purposes [9, p. 141], negating any assumed privacy or property interest of the employee. Further, studies of employee perceptions show most people are more comfortable with an employer's right to read written material and oppose the employer's listening in on a telephone conversation [11, p. 118]. However, these expectations run contrary to the law, which generally permits telephone monitoring but grants greater protection to mail [11].

In short, e-mail inhabits an area of communication that is a shadowy zone between paper mail and a telephone call. Like a telephone call, it can be intercepted during its transmission [5, p. 469]. Like a letter, it is a message that remains fixed for a period of time; conversely, unlike a letter, it can be "unsealed" and opened secretly and without notice to the sender before or after it is read [5, p. 469]. Again, because e-mail messages in the workplace are stored in encoded plain text files, they can be intercepted and read by third-party service providers,

computer technicians, corporate managers [6], system managers and operators, or "anyone with a working knowledge of and access to the corporate network" [14]. This leads to the most offensive possibility of privacy invasion, where corporate executives, at their whim, ask a systems operator to deliver an employees' e-mail files [11, p. 140]. Aside from any information the employer might legitimately need, the employee's personal feelings about a supervisor or particular employer policies may be intercepted [5, p. 469]. As a result, "gossip, which may have at one time been communicated at the water cooler, may be read by an employee's supervisor and result in termination" [6, p. g1].

E-MAIL CASES TO DATE

Although one author views state law as the best avenue to protect private employees who use e-mail [15], to date no state courts have held a reasonable expectation of privacy exists in the employee's use of the employer's e-mail system [16]. However, the few cases filed have confirmed the fears discussed earlier. The most notorious three challenges to employer intrusion into e-mail privacy brought before a state court were filed in California under that state's wiretap statute. The first was *Shoars v. Epson America, Inc.* [16]. Shoars, an e-mail administrator for Epsom America, Inc. discovered a supervisor was reading all employee e-mail that originated from outside the company [16]. She had been previously instructed to inform all employees that e-mail would be private [16]. When she complained to her superiors via the company e-mail system, her supervisor intercepted the message and terminated her for gross insubordination [16]. Soon after, in *Flanagan v. Epson Am., Inc.*, the monitored employees brought a class action suit against Epson for the invasion [17]. Both cases were dismissed for failure to state a claim because the court held the employees had no expectation of privacy in their e-mail messages, and even if they did, the California wiretap statute did not apply to e-mail [17]. To date, both cases have been appealed but no decision has been rendered. More recently, in *Bourke v. Nissan Motor Corp.*, under the same wiretap law, the California court again rejected the privacy claim of two Nissan employees who claimed they were wrongfully terminated after their employer read their personal e-mail messages sent to clients on the company system [18]. These cases reflect at least one state court's struggle with recognizing threats to privacy that exist in new e-mail technology, despite an existing state statute that forbid other types of electronic interception [18].

Despite the plaintiffs' lack of success in the above cases, their publicity piqued employers' interests in avoiding possible liability for invasion of privacy. Many employers developed e-mail policies based on the assumption they have the right to read e-mail as long as they tell their employees about the policy [19]. At the same time, employees were alerted to the possible pitfalls of monitoring via cautionary articles on e-mail "etiquette" [20] and vigilance against sending e-mail messages "that you wouldn't post on the bulletin board" [21, p. 51]. However, in

the absence of a recognized legal right against the privacy invasion, those policies provide little if any protection to the employee from employer abuse. As a result, many looked to Congress to implement a national standard for e-mail privacy.

LEGISLATIVE EFFORTS TO DATE

The first significant attempt by Congress to protect employees from electronic monitoring was the Electronic Communications Privacy Act of 1986 (ECPA), which amended Title III of the Omnibus Crime Control and Safe Streets Act [22]. Prior to 1986, Title III prohibited the monitoring of wire communications and oral communications unless one of the communicating parties has given consent [6]. However, "wire communications" required that the method of communication to be protected involve some form of human voice transmission [6]. The ECPA, a response to communications technology developments, was expected to cover new technologies and to expand the scope of Title III to include three broad new areas: 1) interception of electronic communications, 2) stored electronic communications between computers or between a computer and a human, and 3) private communication systems such as an intracompany network [23]. These definitions are expansive enough to encompass e-mail or any transfer of data over a phone line connecting two computers [23]. In short, the EPCA protects electronic communication from monitoring by anyone except the sender or the receiver of the message [14, pp. 132-133].

However, it is not clear that Congress intended to protect individual private employees from invasion of privacy by their own employers [23, pp. 925-926]. Thus, the ECPA probably provides little protection for the employee against the employer reading his/her e-mail. This is because there are major exceptions to the prohibition against consensual monitoring of electronic communications. First, the ECPA does not cover electronic monitoring performed on noninterstate systems. Like most federal laws, the scope of the ECPA is limited to "electronic communications" that "affect interstate or foreign commerce" [11, p. 152]. To the extent the EPCA protects some intracompany electronic communication, it does so only for systems that involve wire communication, which, as stated earlier, means human voice communication [11]. Thus, absent some type of contact with an interstate system, such as through subscription to an e-mail service, it is unlikely the EPCA would protect intracompany e-mail communications by employees [11]. However, even if an employer uses an interstate e-mail system, the other two exceptions might render monitoring of e-mail outside the protection of the ECPA.

The second exception to interception of electronic communications exists where one of the parties to the communication in question gives his/her consent to the monitoring [11]. While the courts have not yet addressed the issue of consent of monitoring of stored communications [24], they have addressed the issue of consent to interception of communications via telephone [23, pp. 942-943]. Here,

most courts have focused their analysis on whether characteristics of the employer-employee relationship have given rise to the employee's implied consent based on surrounding circumstances [11]. Consent to monitoring cannot be implied merely from the employee's knowledge of the employer's ability to monitor communications [11]. However, where the employee consents to an employer's policy that permits unintended monitoring of personal phone calls for a limited period of time until the personal nature of the call is determined, the court may find implied consent to the monitoring [11]. In an e-mail context, a written policy might similarly create an atmosphere of implied consent [11]. However, if an employer promulgated a policy that e-mail messages would be monitored to prevent transfer of trade secrets, it might limit the employee's implied consent to monitoring for that purpose [23, pp. 934-935]. Thus, if the employer monitored an employee for reasons beyond the scope of that policy, otherwise permissible monitoring might intrude upon a reasonable expectation of privacy created by the employer. For example, in *Deal v. Spears*, a federal district court held that, under the ECPA, telling and employee they "might" be monitored does not equal implied consent to a specific instance of monitoring [25]. The *Deal* court indicated that a "reasonable expectation" exists that an employee would not consent to admit certain private information on a phone they believed to be tapped [25]. Thus, by using an objective/reasonable test by looking into the plaintiff's "probable belief" [5, fn. 65-67], the *Deal* court seemed to be searching for an objective standard for consent that afforded greater protection to the employee than an earlier case, which required the employer only to show that the employee has "manifest[ed] acquiescence . . . of otherwise protected rights" [5, fn. 65-67]. The court probably recognized the inconsistency of implying consent to monitoring from employees who do not know they are actually being monitored [5, p. 452]. Thus, under the ECPA, courts may find an objective expectation of privacy in the specific terms of the employer's e-mail policy, rather than the employee's actual actions. Therefore, the ECPA might offer a clearer protection of e-mail privacy than the common law.

The third exception to the ECPA, which arguably gives the employer the broadest discretion to intercept e-mail is the "business-use" exception [11, p. 155]. The ECPA allows monitoring of electronic communication if it is necessary for the "rendition" of the employer's service or for the "protection of the rights or property of the provider of that service" [11, p. 155]. While this has not yet been applied by the courts to e-mail, cases involving phone-extension monitoring have liberally construed the business-use exception. Business purposes ranging from suspected theft and divulging of trade secrets to abuse of phone privileges and improving public relations have been upheld as legitimate [11]. However, courts have found employers liable for privacy intrusions [5, p. 456], even when a legitimate business purpose existed, if the scope of the intrusion and the nature of the monitoring is beyond that necessary to further the otherwise valid business purpose [11], and the plaintiff's transmission was clearly for a personal purpose

[5, p. 455]. Thus, e-mail might be able to be monitored consistent with the ECPA if the employer only intercepted the employee's e-mail messages relevant to the proposed purpose [5, p. 456].

The business-use exemption leads to the aspect of e-mail most susceptible to employer abuse: stored messages. A recent case indicates that the distinction between stored and intercepted e-mail messages is the electronic status of the message, and not whether it was read by the receiver [24]. There are two types of stored messages: those stored temporarily while the message is transmitted and those stored permanently by the system provider [23, pp. 929-930]. E-mail system providers are exempt from the prohibitions on access to stored messages [23, pp. 929-930]. However, these exemptions for storage are limited to messages stored for backup purposes only [23]. It might be argued that this exemption results in veritable carte blanche for an employer with an in-house e-mail system to review and disclose e-mail communications stored on a wholly company-owned system [23, p. 933; 1, §7.14A, 1995, p. 173]. However, just as an employer who reads e-mail in violation of his/her own policy may fall outside of the consent exception, an employer who accesses stored e-mail messages for reasons other than system-maintenance use of backup files might violate a reasonable expectation of privacy held by the employee [23, p. 933].

Thus, it is possible that as the courts moved toward a standard of a "reasonable expectation of privacy" in interpreting the ECPA, a uniform standard for all electronic communications including e-mail might develop. Again, cases under the ECPA that address the same issues of notice, implied consent, and legitimate purpose while avoiding determinations of "highly offensive" seem to reflect the core values embodied in the concept of "privacy." However, the failure to expressly protect employees whose employers have in-house e-mail systems still leaves gaps through which an employer could read employee e-mail. Also, as reflected in the California cases discussed above, existing state wiretap statutes to date have failed to fill the gap.

THE MISSED OPPORTUNITY: THE PRIVACY FOR CONSUMERS AND WORKER'S ACT

A much-anticipated attempt to fill the gap left by the ECPA and state law was the Privacy for Consumers and Worker's Act (PCWA) [26]. Many had predicted success for the bill during the beginning of the Clinton Administration [5, p. 473]. However, the Democrat-sponsored bill is probably dead due to the sweeping Republican Congressional victories of November 1994. Further, the main sponsor of the PCWA, Senator Paul Simon (D-Illinois), has since announced that he is not running for re-election [27]. Senator Simon had been introducing the PCWA for several years [5, p. 473], and much of the press on e-mail privacy since 1990 has revolved around debates over merits of the PCWA. Those debates serve as an

instructive review of the competing interests in electronic monitoring in general and e-mail in particular.

The substance of the PWCA protected employees from "electronic monitoring," which included all data collection, storage, and analysis via any technological device by transfer of sound, data, images, or writing [27]. This definition excluded any monitoring done for the purposes of wiretapping, electronic transfer of payroll, insurance, or related information [27]. The scope of the act allowed it to regulate any individual or business entity employing any number of workers [27]. It would require the employer to give general notice to present employees and prospective employees that the employer engages in workplace monitoring [27].

The PCWA addressed the concerns surrounding the informed consent decisions discussed here and avoided the issue of whether the intrusion is "highly offensive." The PCWA was envisioned by its supporters as a workplace "right-to-know" policy that protected employees by arming them with information [2, §6123]. Recognizing the benefits that monitoring brings to the employer, the PCWA set a framework for permissible use of electronic monitoring. First, an employer could randomly monitor new employees without any advance notice of the specific surveillance during the first sixty days on the job [26]. To monitor other employees, however, the employer would be required to provide individualized notice not more than seventy-two hours prior to actual monitoring [26]. Even after giving the employees notice, the employer was limited to two hours per week of random monitoring [26]. Finally, an employee would have the right to review the information collected by the employer, and the employer would be required to explain how the information would be collected, how personal data would be used, and the method used to determine how production standards and work performance would be furthered by electronic monitoring [26]. Thus, within this framework, an employer would be able to use the latest technology to improve its business, while following procedures that would respect the employees' privacy via informed notice and consent.

In recognition of the employer's important interest in protecting its property, the PCWA made exceptions to the notice requirement. Unannounced electronic monitoring was allowed if the employer had reasonable suspicion that the employee had engaged in illegal, tortious, or willful gross misconduct, and that action had resulted in significant adverse economic loss to the employer or injury to other workers [26]. Unannounced monitoring was also permitted to protect against employees' workers' compensation abuse [26]. However, the employer was also required to document "with particularity" the conduct to be monitored and the basis for the reasonable suspicion, sign the documentation, and retain it for a certain period of time [26]. The employee would be able to review this statement if any disciplinary or termination proceedings were instigated by the employer based on the monitoring results [26].

Employers strongly opposed the PCWA, arguing that it gutted the benefits of electronic monitoring. The rigid requirements of the frequency and duration of monitoring were thought to eschew the flexibility needed to adapt specific types of monitoring to different industries [11]. Also, opponents charged that requiring specific notice to employees of when they would be monitored would hinder the effectiveness of monitoring techniques to accurately assess employee performance [11]. If employees knew when they were being monitored, it was noted, they would be on their "best behavior," both in work performance and honesty, only when monitoring occurred [11, p. 168]. Thus, employers feared losing electronic monitoring as a powerful tool for enhancing production, quality, and efficiency [11].

Employers also criticized the "reasonable suspicion" requirement for unannounced monitoring of employees engaged in wrongful action. Opponents pointed out that conduct that was neither criminal or tortious could still adversely affect the interest of the employer and other employees [28]. For example, employers would be unable to monitor employee conduct that might expose employers to tort liability. In addition, forbidding surreptitious monitoring without reasonable suspicion in the face of increasing computer crime, and the ever-evolving sophistication of those who commit it, would leave employers helpless to protect themselves [28] from theft of "trade secrets and other intangible property interests" [7, p. 1261].

Finally, opponents argued that the PWCA was simply bad law because its implementation would result in a conflict with developing law of the ECPA [28; 11, pp. 29-37]. The PWCA's protection of electronic *monitoring* did not encompass the *interception* of electronic communications protected by the ECPA [11]. As a result, if e-mail is covered by the ECPA, the ECPA exceptions for prior consent and business use discussed above might allow an employer to access and read e-mail as long as the employer's e-mail was part of an interstate system, while the PCWA would forbid the use of the obtained information [11]. Thus, because Congress had already spoken on the issue of electronic monitoring with the ECPA, passing a statute that undercut that developing law would leave employers with "no clear direction" for compliance [28]. Therefore, the gap left by the ECPA would be incompletely filled by an overlapping and contradictory policy [29].

RECOMMENDATIONS

While the apparent demise of the PCWA renders advocacy for its passage moot, the core provisions of the act reflect the essential concerns that surround the law of privacy in general and e-mail in particular. First, the PCWA's requirements of informed notice via explanation of the uses and rationales of electronic monitoring are at the core of respect for employee privacy. Informing employees would obviate the stress created by feelings of surveillance. Also, employees educated in

the methods used to evaluate them would not only understand their industry better, but might develop trust in management through educated participation in decisions to improve their performance and the company's productivity. Particularly since employees are encouraged to use e-mail in all aspects of business communication, employees should be comfortable with e-mail as the natural extension of their communication skills. Finally, recognizing the employee's right to informed consent preserves the dignity of the individual without requiring a finding of "highly offensive" intrusion before protection is warranted.

The PCWA's opponents were probably correct to oppose the legislating of specific days and hours when monitoring could to take place. Different standards of monitoring must exist for different industries based on the skills to be tested and the sensitivity or security concerns of the business. One commentator has suggested leaving the definition of reasonableness to the courts [11]. Courts could then compare the reasonableness of the monitoring to the legitimate business purpose on an industry-by-industry basis and determine a reasonable fit between that purpose and the scope of the monitoring [11]. Further, to remain competitive, employers must be able to safeguard their trade secrets and intellectual property from theft via e-mail and should be able to monitor employees unannounced if they have reasonable suspicion of employee misdeeds. Requiring employers to document their suspicions with particularity would deter the over-curious employer from monitoring without good cause and, contrary to the opponents of the PCWA, adds no additional burden to the employer. In reality, even if documentation of particularity were not *required* under a PCWA-type law, savvy employers would document any such monitoring to protect themselves from possible liability. Also, the employee's right to review any monitoring results would protect the employee from wrongful or retaliatory discharges.

Finally, a legislative mandate of procedures governing electronic monitoring would relieve courts from deciding the difficult question of whether the intrusion or the dissemination of the information is "highly offensive." As argued above, the state courts have been slow to adapt the common law privacy tort to e-mail privacy, or recognize e-mail privacy under their wiretap statutes. It is no small influence that the legal profession is notoriously slow to adapt and implement new technology. As a result, many attorneys and judges framing and deciding these issues have never used a word processor, much less e-mail, the Internet, or other technologies prevalent in the workplace. The time is ripe for legislative action to show the way.

CONCLUSION

Ours is a society that celebrates the value of individual rights and personal autonomy over the potentially oppressive, authoritarian power of the government. In contrast, however, we tolerate arbitrary treatment and significant intrusions into our lives by large, powerful, private organizations, whose actions would be clearly

condemned if done by a governmental actor. We tolerate this treatment regardless of the similarity of the indignity imposed by the intrusion, and regardless of the similarity of the power the employer may hold over our lives [30].

As the scholarly literature indicates, and as most of us agree, there is a significant part of our lives and our personality which should remain beyond the scope of intrusion by our employers absent a very good reason for the intrusion. However, it is equally true that we disagree on exactly what we intend to protect, or what we should protect, under the umbrella concept of "privacy." Thus, legislating a definition of privacy, or leaving the definition to individual judges on a case-by-case basis, seems an insufficient solution to protect this nebulous but widely recognized interest. The reasonable middle ground might be a uniform statutory standard of procedures that an employer must follow prior to, and while engaging in, electronic monitoring. This statute should encompass prior notice to the employee, documentation of a legitimate business purpose, monitoring and use of information reasonably related to that purpose, and informing the employee of the possible uses of the information obtained. The PCWA, while flawed, seemed a step in the right direction toward establishing a strong policy of protecting the employee's privacy while allowing the employer to ensure the quality, profitability, and efficiency of its business.

* * *

David M. Snyder, Esq., is currently serving as Law Clerk to Hon. Lorraine C. Parker, New Jersey Superior Court, Sussex County.

ENDNOTES

1. K. H. Decker, Employee Privacy Law and Practice, §1.2 (1987), p. 10.
2. S. D. Warren and L. D. Brandeis, *The Right to Privacy*, Harv. L. Rev. 193 (1890), pp. 195, 196-197, 205, 968.
3. W. L. Prosser, *Privacy*, 48 Cal.L.Rev. 383 (1960).
4. E. J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U.L.Rev. 962 (1964), p. 1006. A detailed comparison of the various privacy theorists can be found at [5].
5. D. N. King, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S.Cal.L.Rev. 441, 442-446 (1994).
6. M. Ewell, Watch What Your Computer Messages Say, The Boss May Be Listening: Privacy Laws are Mostly on the Employer's Side, *Philadelphia Inquirer*, p. g1, May 3, 1994.
7. J. A. Flanagan, *Restricting Electronic Monitoring in the Private Workplace*, 43 Duke L.J. 1256 (1994), p. 1258.
8. C. Piller, Bosses with X-Ray Eyes, *MacWorld*, pp. 118, 120, July 1993.
9. S. N. Baxi and A. A. Nickel, *Big Brother or Better Business: Striking a Balance in the Workplace*, 4-Fall Kan. J.L. & Pub. Pol'y, 137 (1994).

10. C. Hanson, Working Smart—Watch What You Say: The Boss Could be Listening, *Chicago Tribune*, p. 9, September 26, 1993.
11. L. T. Lee, *Watch Your E-mail! Employee E-mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop."* 28 J. Marshall L. Rev., 139, Fall 1994.
12. H. F. Heredia, *Is There Privacy in the Workplace?: Guaranteeing a Broader Right to Privacy under California Law*, 22 S.W.U.L.R. 307 (1992-93), pp. 330-331.
13. Heredia [12], citing *Semore v. Poole* 266 Cal. Rptr. 280 (Ct. App. 1990); see also *Luck v. Southern Pacific Transportation Co.* 267 Cal. Rptr. 618 (Ct. App. 1990), cert. denied, 111 S.Ct. 344 (1990); and *Soroka v. Hudson Corp.*, 1 Cal. Rptr 2d 77 (Ct. App. 1991), rev. granted, 4 Cal. Rptr. 2d 180 (1992), at fn. 234. A detailed treatment of California's state right to privacy under these cases is found at [12]. Also, the New Jersey Supreme Court has found a limited extension of state constitutional right to privacy to private employers in random drug testing cases based on public policy. *Hennesey v. Coast Eagle Point Oil Co.*, 129 N.J. 81, 609 A.2d 11 (1992).
14. D. Loundy, *E-Law: Legal Issues Affecting Computer Information Systems and System Operator Liability*, 12 Computer/L.J. 101 (December 1993), pp. 131-133.
15. S. Winters, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 High Tech L.J. 197 (1993).
16. Lee [11] Westlaw p. 166, fn. 162, citing *Shoars*, No. SWC 112749, slip op. (D.C. Cal. 1990).
17. Lee [11] Westlaw p. 166, fn. 162, citing *Flanagan*, No. BC 007036, slip op. (D.C. Cal. 1990).
18. Winters [15], p. 223, citing *Bourke*, No. YC 003979, slip op. (D.C. Cal. 1993).
19. L. Wilson, Addressing E-mail Rights, *Informationweek*, p. 54, February 15, 1993.
20. A. Kuebelbeck, Getting the Message: E-Mail is fast and efficient. But it isn't always private—and that can mean big trouble for users. *Los Angeles Times*, Part E, p. 1, Wednesday, September 4, 1991.
21. L. Alderman, Safeguard Your Secrets from Your Nosy Boss, *Money*, p. 51, December 1994.
22. *See generally* The Omnibus Crime Control and Safe Streets Act of 1968, as amended. ECPA codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1988), Baumhart [23].
23. J. T. Baumhart, *The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?* 8 Lab. Law. 923 (Fall 1992).
24. In applying the ECPA to governmental actors, seizure of a computer that contained stored private e-mail messages that were later read by law enforcement officers was an impermissible reading of stored messages, but did not constitute an "intercept," although the stored messages had not yet been read by the intended recipients. *Steve Jackson Games, Inc. v. U.S. Secret Service* 36 F.3d 457 (5th Cir. 1994).
25. Lee [11] Westlaw p. 154, fn. 79, citing *Deal v. Spears*, 980 F.2d 1153 (8th Cir. 1992).
26. S.984 103d Cong., 1st Sess. (1993) 139 Cong. Rec. S6121-02, at S6122 (introduced by Sen. Paul Simon, D-Ill.).
27. L. Sweet, Why Simon Won't Run: Senator Cites Meanness and Rigors of Politics, *Chicago Sun-Times*, p. 1, Tuesday, November 15, 1994.

28. The PCWA's companion bill of the same title in the House of Representatives was H.R. 1900, 103d Cong., 1st session (1993) 139 Cong. Rec. E1077-02 (introduced by Rep. Pat Williams, D-Mo.). The minority views opposing the 1992 version of this bill give a comprehensive summary of employer's objections at H.R. 1218, 102 H. Rpt. 1024 (1992).
29. It can be argued that further confusion in this area of the law is undesirable, for at least one federal court has lamented the "infamous" lack of clarity of the ECPA. See *Steve Jackson Games* [24].
30. I was first introduced to the idea of "shadow government," describing the pervasive, government-like power and effect of wholly private entities on our daily lives, in relation to the health insurance industry by Professor Gregory Gelfand at Widener University School of Law's Fall 1994 Health Law class. Similarly, the power of the modern private employer over the employee's daily life is well stated by Professor Kurt Decker:

> In entering the employment relationship, the employee must often relinquish considerable autonomy. Most employees do not bargain for their employment position. They adhere to the employer's unilateral terms. If they do not follow these employment terms, they may not be employed.
>
> If employed by a large employer, the employee must conform to the employer's expectations, rules, and procedures that define specific rights and responsibilities. Many employees are wholly dependent upon their employers for their economic well-being.
>
> Based on the anticipated continuance of this relationship, the employee creates various social and financial commitments. These may include marriage, children, home, automobile, and so forth. This establishes a social or financial reliance in others that is also dependant upon the employee's relationship with the employer [1, §1.6, p. 13].

Direct reprint requests to:

David M. Snyder
1404 Sunny Slope Road
Bridgewater, NJ 08807