June 2015

Carpe Diem: Privacy Protection in Employment Act

Ariana R. Levinson

CARPE DIEM:
PRIVACY PROTECTION IN EMPLOYMENT ACT

*Ariana R. Levinson**

"Just over the horizon are more technology breakthroughs and refinements that we cannot even envision today. Unless we begin now to define privacy—and in particular workplace privacy—as a value worth protecting, these new technologies will be upon us before we are ready for them. Weighing these issues will allow us to be the masters of the technology, instead of its slaves."[1]

"Privacy protection in the United States has often been criticized, but critics have too infrequently suggested specific proposals for reform."[2]

Scholars generally agree that the law in the United States fails to adequately protect employees from technological monitoring by their employers. And groups as diverse as the ACLU and a coalition of multi-national businesses are calling for legislation to address privacy concerns stemming from the rise of new technologies. Yet, few, if any, academic articles have proposed an actual draft of legislation designed to protect employees from technological monitoring by their employers. If recent calls for privacy protection to address emerging technologies are to succeed, blueprints for legislation must be provided. This article, thus, contributes to the call for reform by proposing a federal statute to

---

* Assistant Professor, University of Louisville, Louis D. Brandeis School of Law; J.D., University of Michigan Law School. The author thanks Forrest Kuhn and Rexéna Napier for valuable research assistance. She also thanks Bill Herbert for taking the time to comment on an earlier draft of the manuscript. All views are solely those of the author, as are all errors.

1. 139 CONG. REC. S 6121 (1993) (Senator Paul Simon introducing the Privacy for Consumers and Workers Act).

2. Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357, 358 (2006).

protect employees' privacy from technological monitoring by their employers.

The article surveys potential sources of law and legislation that, while inadequate on their own to protect employees' privacy, serve as a foundation for the proposed legislation. While each of these sources has been reviewed by scholars in the past, consideration of all as a potential source upon which to model legislation is a notable strength underlying the proposed statute. The basic framework of the proposed statute is to provide protection based on the degree of intrusiveness of the privacy invasion. The framework provides baseline protection for on-duty actions, intermediate protection for on-duty communications and use of employer communications technology, and the greatest protection for off-duty behavior. Other notable features of the proposal include the comprehensive nature of the proposal, in comparison to most prior scholarly proposals; the flexibility the statute provides to employers to engage in necessary monitoring; provisions designed to foster employee involvement in implementing and enforcing workplace technological monitoring policies; and the involvement of a government agency, the Department of Labor, in educating interested parties about employee privacy issues and in enforcing the statute. While passage of legislation protecting employees' privacy from employer technological monitoring may face an uphill battle, it is possible and should be done.

I. INTRODUCTION

A group of security officers used their locker area to store personal belongings and to change. Their employer installed a video camera that recorded the area for at least several weeks.[3] Another employee received personal electronic mail ("e-mail") through a company e-mail system and then stored the e-mails in a folder that was password protected with a password known only to him. His employer accessed the messages.[4] Yet another employer used a "powerful camera lens" to observe, through an open window, an employee while he was inside his home.[5]

What these employees have in common is that their employers technologically monitored them, invading their privacy, yet their lawsuits were dismissed.[6] Indeed, scholars generally agree that the law in the United States fails to adequately protect private sector employees from technological monitoring by their employers.[7]

This article proposes a solution: federal legislation intended to permit private sector employers to monitor their employees when necessary but to also provide their employees adequate privacy protection.[8] Section II reviews the nature and extent of the problem of technological monitoring of employees by their employers.

Section III surveys the laws and proposed legislation that serve as a foundation for the Proposed Act and articulates the strengths and

3. Thompson v. Johnson County Cmty. Coll., 930 F. Supp. 501, 503-04 (D. Kan 1996) (discussed in Alexandra Fiore & Matthew Weinick, *Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change*, 25 HOFSTRA LAB. & EMP. L.J. 525, 526 (2008)).

4. McClaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 Tex. App. LEXIS 4103, at *2 (May 28, 1999).

5. Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 383 (Mich. App. 1989) (discussed in Clyde W. Summers, *Individualism, Collectivism and Autonomy in American Labor Law*, 5 EMPLOYEE RTS. & EMP. POL'Y J. 453, 469 (2001)).

6. *Thompson*, 930 F. Supp. at 506-08 (reasoning that silent video does not violate the Electronic Communications Privacy Act and that the employees had no reasonable expectation of privacy in the area and dismissing the pendant state claims); *McClaren*, 1999 Tex. App. LEXIS 4103, at *12 (reasoning that the plaintiff had no reasonable expectation of privacy in the e-mail messages); *Saldana*, 443 N.W.2d at 384 (reasoning that the employee's "privacy was subject to the legitimate interests of his employer.").

7. *See infra* note 18 and accompanying text.

8. *See infra* note 531 and accompanying text for reasons the Proposed Act is limited to the private sector.

weaknesses of the various approaches in comparison to that of the Proposed Act. It reviews several disparate but relevant sources, arbitration decisions, federal legislation that failed to pass, state legislation, and the privacy framework in use in the European Union. While each of these sources has been reviewed by scholars in the past, consideration of all as a potential source upon which to model legislation is a notable strength underlying the Proposed Act.

Section IV illustrates how the Proposed Act flows from but is different than the prior work of scholars addressing the issue. Many scholars either endorse the approach of one of the several sources considered in drafting the Proposed Act or propose legislation that is less comprehensive than the Proposed Act, either because it is limited to protection of one type of activity, such as blogging, or from one means of monitoring, such as a global positioning system ("GPS").[9] Some scholars do, however, propose more comprehensive protections similar to the Proposed Act.[10] The Proposed Act, however, aims to provide employers more flexibility to monitor than these prior proposals.[11] The Proposed Act does so, in part, by providing employers with an array of safe-harbor policies that they can elect to implement in compliance with the Proposed Act.[12]

Perhaps most significantly, few, if any, academic articles have proposed an actual draft of legislation designed to protect employees from technological monitoring by their employers. Yet if recent calls for privacy protection to address emerging technologies are to succeed, blueprints for legislation must be provided. Thus, Section V is a draft of the Proposed Act.

The basic framework of the Proposed Act is to provide legal protections based upon the degree of intrusiveness of the employer's surveillance because of the type of employee behavior being monitored rather than based upon the particular employee activity being monitored, means of monitoring, or seniority of the employee.[13] The framework provides baseline protection for on-duty actions, intermediate protection for on-duty communications and use of employer communications technology, and the greatest protection for off-duty behavior.[14] The

9. *See infra* notes 379-380 and accompanying text.

10. *See infra* note 382 and accompanying text.

11. *See infra* Part V.

12. *See infra* Part V.

13. *See infra* notes 62-64 and accompanying text discussing the Privacy for Consumers and Workers Act's different levels of protections based on the seniority level of the employees.

14. *See* Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J. L. & PUB. POL'Y 609, 609-10 (2009). This article uses the term "actions" to exclude

rationale is that monitoring of on-duty actions is invasive to the degree that it captures behavior much more systematically and continually than direct observation. However, it tends to capture predominately work-related conduct even given the overlap between private life and work. Thus, employees have the lowest level of privacy interest in on-duty actions while employers have the greatest need to monitor on-duty actions.[15] Monitoring of on-duty communications and use of employers' communications technology[16] is generally more invasive because personal non-work related thoughts and associations are more likely to be monitored. Employers have a need to monitor their communications technology and employees' on-duty communications, but employees also have a relatively high privacy interest because of the likelihood that thoughts or associations that they desire to keep private will be monitored. Most invasive is monitoring of employee behavior while off duty. [17] Off-duty behavior tends to be largely unrelated to work, and employees have a high privacy interest in their off-duty behavior.

Section VI discusses the decisions underlying the drafting of the Proposed Act. Notable features of the Proposed Act, in addition to the basic framework, include provisions designed to foster employee involvement in implementing and enforcing workplace technological monitoring policies and the involvement of a government agency, the United States Department of Labor ("DOL"), in educating interested parties about employee privacy issues and in enforcing the Proposed Act. Section VII concludes by exhorting that while passage of legislation protecting employees' privacy from employer technological monitoring may face an uphill battle, it is possible and should be done.

"communications and use of employer communications technology" and the term "behavior" to include "actions" and "communications and use of employer communications technology."

15. One note states that video is arguably the most intrusive means of monitoring. Fiore & Weinick, *supra* note 3, at 557. However, video in the workplace generally captures largely work-related conduct. The potential severe intrusiveness of viewing bodily functions or parts is easily reduced by barring video in places most likely to be used for changing, which the Proposed Act does.

16. All monitoring of employees' use of employer-issued computers, including visiting websites and e-mailing, is addressed alongside monitoring of communications. While monitoring website use may be less likely than monitoring of e-mail to reveal personal behavior, the risk of such revelation is significant enough to include all monitoring of computer use under one set of requirements. Moreover, employers and employees are more likely to understand one unified policy governing computer use. Levinson, *supra* note 14, at 657.

17. Robert Sprague, *Orwell Was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83, 91 (2008) (discussing how "as more workers bring their work into their home and private lives, 'workplace' restrictions will erode the one last bastion of privacy—one's home. Thus, the concern is no longer limited to 'workplace privacy' but employee privacy.").

II. THE PROBLEM: LACK OF PROTECTION FROM EMPLOYER TECHNOLOGICAL MONITORING

The lack of adequate protections for employees' right to privacy from employer technological monitoring has been well documented by numerous scholars.[18]

---

18. MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW, 346 (2d ed. 2003); Marc A. Sherman, *Webmail at Work: The Case for Protection Against Employer Monitoring*, 23 TOURO L. REV. 647, 664 (2007) ("The law generally allows employers to monitor workers' private communications . . . ."); Colette Cuijpers, *ICT and Employer-Employee Power Dynamics: A Comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning of Employees*, 25 J. MARSHALL J. COMPUTER & INFO. L. 37, 52 (2007) ("The foregoing statements lead to the overall conclusion that in general, U.S. employees have no right to privacy with regard to their use of Internet and e-mail in the workplace."); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 293 (2002) ("This Article begins by establishing the failure of statutory law or common law in the United States to guarantee a right of electronic privacy in the workplace."); Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 399 (2000) ("There are several putative sources of the legal protection of workers from electronic surveillance and monitoring in the workplace; on close investigation, however, these sources provide little protection."); Summers, *supra* note 5, at 475; S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 838 (1998) ("A great deal of scholarly energy has been devoted to pointing out the inadequacies of the existing protections for employee privacy in the private sector, and it would be unproductive to attempt to catalog all of these efforts."); William R. Corbett, *The Need for a Revitalized Common Law of the Workplace*, 69 BROOK. L. REV. 91, 103 (2003) ("[E]lectronic monitoring is an area where technology has outstripped the law, leaving employees largely unprotected."); Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DEPAUL L. REV. 739, 739 (1992) ("[T]he law supplies employees with precious little protection from the assault on workplace privacy"); *see also* Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 HOFSTRA LAB. & EMP. L.J. 395, 403 (2008) ("In the employment context, employers have generally been found to invade the privacy of employees only in the most extreme circumstances, such as prying—in detail—about an employee's sex life."); Sprague, *supra* note 17, at 134 ("Unless the courts abandon the approach that any potential disclosure eliminates the right to privacy, and rebalance the priority of employer property rights versus employee privacy rights, employees will have no right to privacy as to their employers—at work or at home."); Gaia Bernstein, *The Parodoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241, 276 (2006) ("The law has, in effect, authorized email and Internet monitoring by employers."); Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 912, (2002) (arguing that "expectation-driven nature of privacy" gives rise to a need for great "structural reform" in the area of workplace privacy); Laura Evans, Comment, *Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?*, 95 CAL. L. REV. 1115, 1116 (2007) ("Currently, U.S. employment law does not sufficiently regulate employers' collection and use of private data about employees."). *But see* James A. Sonne, *Monitoring for Quality Assurance: Employer Regulation of Off-Duty Behavior*, 43 GA. L. REV. 133, 136 (2008) (arguing that off-duty activity/lifestyle discrimination statutes are unnecessary and employees' privacy is better protected "by the market than by the law."); Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American*

Employment at will governs in the United States in all states but one.[19] Those who follow discharge cases understand what it means in concrete terms for employers to have the right to fire an employee for no reason at all. In one case, for example, an employee's laptop was stolen. He was reissued a new one. The wireless use on the new laptop was high. The employer investigated and found child pornography running on the computer. The employer, therefore, terminated the employee and criminal charges were brought against the employee. The defense attorney discovered that the pornography was invisible to the viewer, including the employee. A defect in the virus program, loaded onto the machine by the employer, caused the pornography to run in the background. Thus, the criminal charges were dropped. Was the termination rescinded? No, it remained in place–after all the employee was employed at will.[20]

While that case addresses issues of accuracy and reliability of employer technological monitoring, the cases directly addressing privacy issues are no less bleak.

In one case, an employer monitored an employee to dispute the extent of injuries claimed for workers' compensation purposes. The investigator took video of the man urinating in his yard. The court found that the monitoring did not violate the employee's right to privacy because his activity "could have been observed by any passerby."[21]

Another seminal case confirms that employees generally lack privacy protection from employer technological monitoring.[22] The employer assured the employees that their e-mail was "confidential and privileged" and would not be "intercepted and used as a grounds for

---

Values?, 72 CHI.-KENT L. REV. 271, 283 (1996) (arguing that laws governing employee privacy "strike[] the right balances between privacy and other social interests").

19. Montana requires employers to show just cause for discharge. Rafael Gely & Leonard Bierman, *Social Isolation and American Workers: Employee Blogging and Legal Reform*, 20 HARV. J.L. & TECH. 287, 315 (citing Montana Wrongful Discharge from Employment Act, Mont. Code Ann. §§ 39-2-901 to 915 (2005)). Additionally, "[t]he Virgin Islands and Puerto Rico also depart from the at-will standard." Nicole B. Porter, *The Perfect Compromise: Bridging the Gap Between At-Will Employment and Just Cause*, 87 NEB. L. REV. 62, 70 (2008).

20. Marcia L. McCormick, *Job Termination Nightmare of the Week,* June 18, 2008, http://lawprofessors.typepad.com/laborprof_blog/2008/06/job-termination.html (last visited Jan. 21, 2010).

21. I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685, 689-90 (Ala. 2000).

22. Smyth v. Pillsbury Co., 914 F. Supp. 97, 101. (E.D. Pa. 1996). *But see* Quon v. Arch Wireless Operating Co., 529 F.3d 892, 910 (2008) (review of text messages violated ECPA); Brahmana v. Lembo, No. C-09-00106 RMW, 2009 U.S. Dist. LEXIS 42800, *7-*10 (N.D. Ca. May 20, 2009) (denying motion to dismiss a claim that employer monitoring keyboard strokes to obtain private e-mail password violated the ECPA).

termination."[23] Nevertheless, when an employee sent an e-mail disparaging of management from his home computer to his supervisor, the employer intercepted the e-mail and terminated the employee. The court held that the employer had not violated the employee's right to privacy and upheld the termination.[24]

Further evidence of the lack of adequate protection for employees' privacy is found in the United States' international reputation. Europe considers the United States a country with inadequate protections for employees' privacy.[25] Thus, data transfers containing information about monitoring of employees from the European Union to the United States are prohibited unless the employer has taken precautions greater than those mandated by United States law.[26]

As for the scope of the problem, surveys suggest that the use of technology in the workplace "has been steadily increasing over the past decade."[27] And with it, employer technological monitoring has increased as well.[28] An estimated 77 percent of employers technologically monitor their employees.[29] Approximately, 14 million "are under 'continuous' surveillance . . . for their Internet access or e-mail usage."[30] Yet, one study estimates that approximately two out of every three "corporate workplaces have no policy requiring their employees to manifest consent

23. *Smyth*, 914 F. Supp. at 98.

24. *Id.* at 101.

25. William A. Herbert, *Workplace Electronic Privacy Protections Abroad: The Whole Wide World is Watching*, 19 U. FLA. J.L. & PUB. POL'Y 379, 383 (2008) ("The limits of American electronic privacy protections were highlighted almost a decade ago, when a European governmental entity concluded that the 'current [American] patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union," quoting Opinion 1/99 of the Working Party Concerning the Level of Data Protection in the United States and the Ongoing Discussions Between the European Commission and the U.S. Government, at 2 WP (1999) 15 final (Jan. 26, 1999), available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf (last visited Nov. 19, 2008)); Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 925-26 (2009) ("In 1999, the Working Party of EU Data Protection Commissioners found that U.S. privacy law did not meet the adequacy standard."); Stephen B. Moldof, *International Employee Privacy Issues Panel: Union/Employee Perspective*, 10 (May 1, 2008), available at http://www.abanet.org/labor/mw/2008/tech/pdf/LEL-Tech-Materials.pdf.

26. *See infra* note 337 and accompanying text (discussing three methods by which U.S. companies can adequately secure data).

27. Levinson, *supra* note 14, at 615.

28. Levinson, *supra* note 14, at 616-17.

29. Levinson, *supra* note 14, at 616.

30. Levinson, *supra* note 14, at 616.

to electronic monitoring or acknowledging their workplace monitoring activities."[31]

Employers have always monitored.[32] But new technology creates a monitoring different in degree if not in kind. An employee's every movement can be monitored by GPS[33] or keystroke technology in a way not possible when a limited number of humans were available to monitor. Additionally, the possibility of monitoring personal rather than only work related behavior has increased exponentially with the availability of devices to monitor computer use.[34] GPS and computer technology also have a greater potential to monitor off-duty behavior.[35]

III. PARTIAL SOLUTIONS: POTENTIAL SOURCES OF LEGISLATIVE LANGUAGE

Potential sources upon which to model legislation[36] that would adequately protect private sector employees' privacy, while permitting employers to engage in necessary technological monitoring, include the following: protections for privacy provided by arbitration in the unionized sector, previously proposed federal legislation that failed to pass, the little state legislation that is currently in force to address the problem, and the laws of other countries that more adequately protect employees' right to privacy.[37]

---

31. Levinson, *supra* note 14, at 616.

32. *See* Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263, 1265 (1993).

33. *See* New York v. Weaver, 12 N.Y.3d 433, 441 (2009) ("GPS is not a mere enhancement of human sensory capacity, it facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over, in most cases, a practically unlimited period.").

34. *See* Sonne *supra* note 18, at 146-47 (discussing blurring of working and non-working time).

35. William A. Herbert, *No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery?*, 2 I/S: J. L. & POL'Y FOR INFO. SOC'Y 409, 472 (2006) (discussing "growing portability of tracking devices that enables an employer to monitor an employee while working or not working and within the employee's own dwelling").

36. *But see* Corbett, *supra* note 18 at 96 (arguing common law should respond "to the emerging workplace problems of electronic monitoring" with legislation following later only if necessary).

37. The Electronic Communications Privacy Act ("ECPA") is the federal statute that currently governs technological monitoring. Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2510 et seq. (2002). While it provides privacy protections outside of the employment context, and even some limited protection to employees, the overwhelming majority of commentators agree that with the advent of new technology, such as the Internet and e-mail, it provides inadequate safeguards for employees from employer technological monitoring. Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 67 (2009) ("Three exceptions render the

A. The Law of the Shop

The law of the shop as reflected in the decisions of labor arbitrators who decide cases in the unionized sector serves as one good starting point for developing adequate protections for employees' right to privacy from technological monitoring. [38]

The author's recent survey of published arbitration decisions on employer technological monitoring suggests that arbitrators use twelve safeguards to protect employees' right to privacy. Use of these

---

ECPA almost meaningless in the work place."); Cuijpers, *supra* note 18, at 44 ("Even though this Act prohibits intercepting of wire, oral and electronic communications . . . and accessing stored communications, the exceptions to these prohibitions diminish their effect, making them virtually non-existent in the employment relationship."); Jill Yung, *Big Brother is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 195 (2005) (mentioning that ECPA specifically excludes tracking devices, including GPS); Leonard Court & Courtney Warmington, *The Workplace Privacy Myth: Why Electronic Monitoring is Here to Stay*, 29 OKLA. CITY U.L. REV. 15, 26 (2004) ("[T]he exceptions to the Act nearly swallow the rule, making any expectation of privacy illusory under most circumstances."); William G. Porter II & Michael C. Griffaton, *Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace*, 70 DEF. COUNS. J. 65, 66 (2003) ("In reality, however, the act provides employees little protection from monitoring of their workplace communications"); Kesan, *supra* note 18, at 299 ("In sum, the ECPA is ineffective in regulating the employer/employee relationship"); Stuart J. Kaplan, *E-mail Policies in the Public Sector Workplace: Balancing Management Responsibilities with Employee Privacy Interests*, 15 LERC MONOGRAPH SER. 103, 107 (1998) ("[T]hree broad exceptions in the ECPA would seem to allow most forms of E-mail monitoring by both private and public employers."); Lee Nolan Jacobs, Note and Comment, *Is What's Yours Really Mine?: Shmueli v. Corcoran Group and Penumbral Property Rights*, 14 J.L. & POL'Y 837, 876 (2006) ("With the continued evolution of technology, any protections afforded by the ECPA have become practically irrelevant."); Ira David, Note, *Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is It Big Brother or Just Business?*, 5 NEV. L.J. 319, 328 (2004) ("For E-mail, the protection of the Stored Communications Act has been diluted by the low standard imposed by the courts in recognizing implied authorization . . ."); Jeremy U. Blackowicz, Note, *E-mail Disclosure to Third Parties in the Private Sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80, 104 (2001) ("Commentators are practically unanimous in calling for statutory solutions in the form of both amendments and revisions to the ECPA or a new statutory scheme to give employees some form of protection."); Rothstein, *supra* note 18, at 401 ("The Electronic Communications Privacy Act of 1986 . . . has generally proven ineffective in protecting employees in the workplace from their employers' monitoring."). Mini-electronic communications privacy acts enacted by states may sometimes provide a higher level of protection than the ECPA, such as by requiring consent by both, rather than only one, parties to a communication, but state acts generally mirror the ECPA and its inapplicability to many employment-related disputes arising out of monitoring via new technology. Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 395-97 (1995). Additionally, while unlikely to provide protection for privacy from technological monitoring, traditional employment exceptions to the at-will rule of employment might be considered as potential sources of protection. *See* Scott R. Grubman, Note, *Think Twice Before You Type: Blogging Your Way to Unemployment*, 42 GA. L. REV. 615, 627-29 (2008) (discussing possibility of covenant of good faith and fair dealing, implied contractual obligation, or public policy protecting employees who are discharged for blogging).

38. Levinson, *supra* note 14, at 638.

safeguards permits employers the flexibility to monitor when necessary but protects employees from an unwarranted level of intrusion.

These safeguards are the following: 1) the right to affirmatively refuse monitoring; 2) notice of monitoring; 3) notice of the particulars of monitoring; 4) notice of infractions related to the use of new technology; 5) notice of resulting discipline for those infractions; 6) consistent enforcement of policies relating to technology; 7) confidential review of information discovered through monitoring; 8) limited collection of information through technological monitoring; 9) reasonable suspicion of an infraction before monitoring; 10) assessment of the accuracy and reliability of the information produced by the monitoring; 11) compensation for a violation of privacy; and 12) restrictions on discipline imposed based on information gathered as a result of monitoring.[39]

These safeguards are unevenly applied by arbitrators who are most often asked to determine whether discipline was for just cause.[40] Thus, the focus of many disputes is not providing protection for employee privacy, but rather on providing employees job security.[41] Nevertheless, the safeguards provide a level of protection for employees' privacy not generally found in the United States outside the unionized sector.[42] And the safeguards, thus, serve as a workable starting point for protecting employees' privacy and are the basis of many of the substantive provisions of the Proposed Act.

B. Federal Proposals

Two federal bills have previously been proposed to address the problem of inadequate protection of employees' privacy from employer technological monitoring: the Privacy for Consumers and Workers Act

39. Levinson, *supra* note 14, at 640.

40. Levinson, *supra* note 14, at 637, 638.

41. *See* Levinson, *supra* note 14, at 637.

42. *See* Marvin Hill & Emily Delacenseri, *Procrustean Beds and Draconian Choices: Lifestyle Regulations and Officious Intermeddlers-Bosses, Workers, Courts, and Labor Arbitrators*, 57 MO. L. REV. 51, 55 (1992) ("While at common law no nexus between the conduct complained of and a private-sector employee's job need be shown, it is difficult to justify according some protection from arbitrary dismissal to public-sector employees and individuals covered under collective bargaining agreements while in most cases denying any protection to common law 'at-will' employees."). *But see* Edward Hertenstein, *Electronic Monitoring in the Workplace: How Arbitrators Have Ruled*, 52-ALT. DISP. RESOL. J. 36, 44 (1997) ("Arbitration history and case law suggest that employers have great latitude in administering surveillance and monitoring [of] employees.").

("Workers Act" or "PCWA")[43] and the Notice of Electronic Monitoring Act ("Notice Act" or "NEMA").

1. Privacy for Consumers and Workers Act

The Workers Act was initially introduced in 1990.[44] The most cited version is S. 984, introduced in 1993 by Senator Paul Simon.[45] That bill "received the broadest support" in the Senate with 130 cosponsors.[46] A similar bill considered in the House, during 1992, H.R. 1218, had 168 co-sponsors.[47]

The Workers Act broadly defines "electronic monitoring" as "the collection, storage, analysis, or reporting of information concerning an employee's activities by means of a computer, electronic observation and supervision, telephone service observation, telephone call accounting, or other form of visual, auditory or computer-based technology which is conducted by any method other than direct observation by another person . . . ."[48] The definition appears to broadly encompass any type of technological monitoring, whether currently invented or not. However, it excludes "the interception of wire, electronic, or oral communications as described in chapter 119 of title 18, United States Code,"[49] the Electronic Communications Privacy Act ("ECPA"). Thus, certain types of technological monitoring, such as telephone wiretapping, would have been routinely excluded while other types of technological monitoring, such as of e-mail, would have been excluded depending upon whether or not an interception was involved. It is unclear why the Workers Act did not extend protection to monitoring of these types.[50]

---

43. The act is typically referred to as the PCWA, but in an effort to avoid acronyms and ease the reader's understanding, the author is using a shortened title instead.

44. Lee Nolan Jacobs, *supra* note 37, at 861 (citing National Workrights Institute, Privacy Under Siege: Electronic Monitoring in the Workplace 19 (2005), *available at* http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf).

45. Privacy for Consumers and Workers Act, S. 984, 103d Cong. (1993).

46. Kaplan, *supra* note 37, at 110.

47. Privacy for Consumers and Workers Act, H.R. 1218, 102d Cong. (1992).

48. S. 984, at § 2(2)(A); H.R. 1218, at § 2(1)(A).

49. S. 984, at § 2(2)(C) (i). The House version did not include this exclusion but instead exempted wiretapping. H.R. 1218, at § 1(C).

50. Because courts interpret e-mail to be stored at most points, it may not be covered by chapter 119 of title 18. *See* Laurie Thomas 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, 172 (1994).

> [I]f the ECPA is held to be applicable to employee E-mail actions, then the accessing and reading of E-mail files may fall outside of the proposed legislation. Under the

The Workers Act would have required that the Secretary of Labor provide employers a standard notice, such as that in use for the Fair Labor Standards Act ("FLSA") or the National Labor Relations Act ("NLRA"), to hang in a prominent place. The notice would have informed employees of their rights under the Workers Act, including when an employer must provide notice of monitoring.[51]

The Workers Act also would have required that employers provide notice of monitoring practices to each employee at the time employment is offered to the employee, if not before. The notice would have been required to specify the following: 1) the type of electronic monitoring that will be used; 2) the type of personal data that will be collected; 3) "the hours and days per calendar week" that monitoring will occur; 4) "the use to be made of personal data collected"; 5) interpretations of the data collected that are used;[52] 6) "[e]xisting production standards and work performance expectations;" 7) the methods for determining those standards and expectations;[53] 8) "a description of the electronic monitoring"; [54] and 9) an alert to the exception for monitoring without notice.[55]

The exception permits monitoring without otherwise applicable limitations on access,[56] intent,[57] or use of video[58] and without notice where the employer has a reasonable suspicion of unlawful conduct or "willful gross misconduct" and where that conduct "has a significant adverse effect involving economic loss or injury to the employer or the employer's employees."[59] In such circumstances, an employer would

---

ECPA, the prior consent or business use exemptions may pertain, and monitoring may be found permissible, at least on an interstate basis.

Id. *But see* Gantt, *supra* note 37, at 409 ("First although the House bill supplements ECPA protections for E-mail, the Senate version specifically excludes 'the interception of wire, electronic, or oral communications as described in [the ECPA],' and thus E-mail, from its definition of 'electronic monitoring.'").

51. S. 984, at § 4; H.R. 1218, at § 4.

52. Required only when the interpretation may affect one of the employees.

53. Required only if the methods affect the employees.

54. S. 984, at § 4(b)(8).

55. S. 984, at § 4(b). The Workers Act also contained provisions to protect prospective employees and customers. While discussion of such protections is beyond the scope of this article, it would certainly be workable to integrate such related protections into a unified law governing workplace privacy.

56. *See infra* note 75.

57. *See infra* note 71.

58. *See infra* note 76.

59. S. 984, at § 5(c)(1)(B). The House of Representatives version had a different exception limited to unlawful activity that "adversely affects the employer's interest or the interests of such employer's employees." H.R. 1218, at § 5(c)(1)(B).

have been permitted to monitor the suspected employee or the area in which the suspected activity is occurring. Before doing so, however, the employer would need to document "with particularity the conduct which is being monitored and the basis for the monitoring" and "the specific economic loss or injury to the business . . . or the employer's employees."[60] The employer would have been required to sign the statement and retain it for three years from the date of the monitoring or "until judgment is rendered in an action brought by an employee" under the Workers Act.[61]

In addition to providing for notice, the Workers Act would have prohibited random and periodic monitoring of certain groups of employees. Periodic or random electronic monitoring of new hires with sixty or fewer working days of employment was permissible. Random or periodic monitoring of those with sixty-one days to five years of employment was permitted if their work group[62] was monitored only for two hours or less per calendar week.[63] Periodic or random monitoring of employees with more than five years' employment was prohibited.[64]

The Workers Act would not have prohibited continuous electronic monitoring. But employers could not simultaneously review any data from continuous electronic monitoring on a periodic or random basis "unless the electronic data was obtained from the use of an electronic identifier or accessor, such as an electronic card or badge access system, [or] telephone call accounting system" or unless "the data is continuously monitored by an employer or appears simultaneously on multiple television screens or sequentially on a single screen."[65] Additionally, an employer could have reviewed data from continuous electronic monitoring after the monitoring was complete "only if review was limited to specific data that the employer has reason to believe contains information relevant to an employee's work."[66]

The Workers Act would also have provided a right of review for the employee. In all cases except those involving monitoring for reasonable suspicion, the employer was required to provide the

60. S. 984, at §5 (c)(2)(B).

61. S. 984, at § 5(c).

62. S. 984, at § 5(b) (defining a work group as "a group of employees employed in a single facility and engaged in substantially similar work at common time and in physical proximity to each other.").

63. S. 984, at § 5(b)(2) (requiring the notice of monitoring to be provided to these employees between twenty-four and seventy-two hours before the monitoring).

64. S. 984, at § 5(b).

65. S. 984, at § 6(a).

66. S. 984, at § 6(b).

employee "with a reasonable opportunity to review . . . a copy of all personal data obtained or maintained by electronic monitoring . . . ."[67] The collective bargaining representative and an authorized agent would have the same right. All would have the additional right to request a copy of the data.[68]

In cases involving monitoring for reasonable suspicion, the employee would have a more limited right of review. The employee would have a right to review the data after the investigation was completed or when disciplinary action had been initiated, whichever occurred first. The employee would also be able to request a copy of the data and to review and request a copy of any interpretation of the data.[69]

The Workers Act also would have provided limitations on discipline based on technological monitoring. Data could be used as a basis for discipline only if all provisions of the Workers Act were followed. Additionally, quantitative data obtained through monitoring could not be used as the sole basis for performance evaluations or "setting production quotas or work performance expectations . . ."[70] except when an employer had only the data as a basis for evaluation of telecommuters.

The Workers Act would have prohibited intentionally collecting "personal data about an employee through electronic monitoring if the data are not confined to the employee's work."[71] Yet collection of some data not confined to work was permissible as long as the purpose and principle effect was to collect work-related data.[72] And, the Workers Act would not have applied to "electronic monitoring conducted by employers in connection with the investigation of a workers' compensation claim unless there is reasonable suspicion of fraud or the claim involves at least $25,000."[73] Indeed, the House bill only applied to monitoring conducted on the employer's worksite.[74]

Additionally, employers would not be permitted to monitor bathrooms, locker rooms, or dressing rooms.[75]

---

67. S. 984, at § 7 (a).
68. *Id.*
69. S. 984, at § 7(b)(2).
70. S. 984, at § 8(b)(2).
71. S. 984, at § 10(a); Privacy for Consumers and Workers Act, H.R. 1218, 102d Cong. § 9(a)(1) (1992).
72. S. 984, at § 10(f).
73. S. 984, at § 13(b).
74. S. 984, at § 12(b).
75. S. 984, at § 10(b).

Additional prohibitions included one prohibiting monitoring with a video camera that is not visible to the subject unless the monitoring was based on reasonable suspicion.[76]

The Workers Act also provided that: "An employer shall not intentionally use or disseminate personal data obtained by electronic monitoring of an employee when the employee is exercising First Amendment rights," but such data could permissibly be incidentally collected.[77]

The Workers Act also would have restricted which employers could access the information collected. An employer could access data only if "the employer's employee who maintains such data is not available" and the employer had an "immediate business need for specific data."[78] Even in this instance, the employer could not access "visual images, audio impressions or data that can be used to create visual or auditory information."[79] Rather, the employer could access only alphanumeric data, defined as "data consisting entirely of letters, numbers, and other symbols."[80] The data obtained could not be "used for the purpose of discipline or performance evaluations," and the employer must, within a reasonable time after accessing the data, notify "the employee who maintains such data that the employer has accessed such data."[81]

The employee who would collect the personal data obtained by electronic monitoring could not disclose it to others except in limited circumstances. These included disclosure to "officers and employees of the employer who have a legitimate need for the information in the performance of their duties" and to "the exclusive bargaining representative."[82] The House bill included an exception for disclosure "pursuant to the order of a court of competent jurisdiction."[83]

The provisions would have applied to third parties engaging in monitoring on behalf of employers.[84]

The Workers Act included an anti-retaliation provision.[85]

---

76. S. 984, at §§ 11(2), 13(b).

77. S. 984, at § 10(c) (1993); Privacy for Consumers and Workers Act, H.R. 1218, 102d Cong. § 8(c)(1) (1992).

78. S. 984, at §9(a).

79. S. 984, at §9(b).

80. *Id.*

81. S. 984, at § 9(a)(3).

82. S. 984, at § 10(d).

83. H.R. 1218, at § 9(b)(C).

84. S. 984, at § 13(d).

85. S. 984, at § 11(4).

The Workers Act included the following enforcement provisions and penalties. It included a civil penalty up to $10,000. The Secretary of Labor would determine the amount of the penalty after considering "the previous record of the person in terms of compliance with this Act and the gravity of the violation."[86]

The Workers Act would have provided jurisdiction for the federal district courts to decide actions brought by the Secretary of Labor. The district courts could "restrain violations" of the Workers Act and issue injunctive relief requiring compliance with the Workers Act, and legal, equitable, and declaratory relief incident thereto, including "reasonable attorney fees and other litigation costs reasonably incurred."[87]

The Workers Act also would have provided a private right of action for aggrieved employees in any "Federal or State court of competent jurisdiction."[88] The same relief available in an action brought by the Secretary of Labor was available in a private suit.[89]

The Workers Act included a three-year statute of limitations.[90]

No right or procedure provided by the Workers Act was waivable "by contract" or otherwise unless part of a "written settlement agreed to and signed by the parties to a pending action or complaint under this Act."[91]

The Workers Act would not "restrict, limit, or eliminate a requirement of the Federal Government, or a State or political subdivision of a State or of a collective bargaining agreement relating to privacy or electronic monitoring that is more stringent than any requirement of this Act."[92]

The Secretary of Labor was to issue regulations to carry out the Workers Act.[93]

The Workers Act would have been a solid framework to protect employees' privacy from technological monitoring. Further, at least some employer representatives recognized that the Workers Act would

86. S. 984, at §12(a)(2).
87. S. 984, at § 12(b).
88. S. 984, at §12(c)(2).
89. S. 984, at § 12(c).
90. S. 984, at § 12(c)(3).
91. S. 984, at § 12(d).
92. S. 984, at § 15.
93. S. 984, at § 14.

also provide assurance to employers acting in compliance with it that they were acting appropriately when monitoring their employees.[94]

The Workers Act was purportedly defeated, however, because it was perceived as containing burdensome notice requirements and regulating employers in too great of detail.[95] Yet, notice requirements are necessary and important to provide adequate protection for employees and respect for their dignity. Notice requirements are not generally unduly burdensome for employers, many of whom adopt policies on human resources matters simply as a matter of good business practice. Nevertheless, the Proposed Act contains notice requirements that are slightly less onerous than those of the Workers Act. The exception providing for monitoring without notice encompasses more circumstances than the Workers Act, permitting employers to use other safeguards in lieu of notice. When notice is required, the annual individual notice[96] need not include the times monitoring will occur or the methods for determining standards and expectations.[97] The Proposed Act does not require a poster notice. The Proposed Act does, however, require employers to notify employees of a right to consultation before instituting a technological monitoring policy.

Moreover, the Proposed Act provides employers greater latitude to monitor employees, provided appropriate safeguards are in place, than did the Workers Act, particularly when monitoring on-duty conduct. It contains no ban on random monitoring of any category of employees' workplace actions or communications. While using seniority is a laudable safeguard that makes sense given that generally long-term

94. Christopher S. Miller & Brian D. Poe, *Employment Law Implications in the Control and Monitoring of E-mail Systems*, 6 U. MIAMI BUS. L.J. 95, 96, 118 (1997) (encouraging voluntary compliance with the Workers Act should it pass).

95. Kaplan, *supra* note 37, at 110 (discussing how employer lobbying, including arguments that notice was unduly burdensome, defeated the bill); Yung, *supra* note 37, at 212 (discussing how requiring both general notice of monitoring and a detailed individual notice is not necessary and suggesting just the individualized notice with signed acknowledgment).

96. Boehmer, *supra* note 18, at 817 (discussing how requiring a new notice "each time that one of the seven required elements of the notice is changed in any respect" is "unduly onerous").

97. Laurie Thomas Lee, *supra* note 50, at 171 (1994) (discussing how providing "exact days and hours . . . may go too far in stripping employer of the ability to access company computer files outside of specified monitoring periods."); Shefali N. Baxi & Alisa A. Nickel, *Big Brother or Better Business: Striking a Balance in the Workplace*, 4 KAN. J.L. & PUB. POL'Y 137, 145 (1994) ("A requirement of notice so time-specific that it details the days and hours monitoring will take place allows employees to conform their behavior to the standards of their employer during monitoring and to do substandard work the rest of the time."); Donald R. McCartney, Comment, *Electronic Surveillance and the Resulting Loss of Privacy in the Workplace*, 62 UMKC L. REV. 859, 887 (1994) ("When the employees realize that they will be monitored at a specific time, it may cause them to conduct work at lower performance levels at other times.").

employees have proven that they have the employer's interest at heart, some employers may feel the need to monitor long-term employees because of difficulties targeting only certain employees or because of poor morale, even among long-term employees, at their workplace.[98]

While the Proposed Act is designed to permit employers more flexibility to monitor,[99] in some respects it guarantees employees a greater level of privacy than the Workers Act. For instance, types of monitoring covered by the ECPA are not excluded, providing employees safeguards from types of technological monitoring that were not covered by the Workers Act. Additionally, the Proposed Act places somewhat greater restrictions on monitoring off-duty employees. It prohibits monitoring within the home[100] and in secluded areas and requires that an employer have "reasonable grounds to believe that the employee is engaging in conduct that will cause a significant concrete harm to the employer" before monitoring an off-duty employee.[101]

2. Notice of Electronic Monitoring Act

The Notice Act was initially introduced in 2000 by Senator Charles Schumer and Representative Charles Candy.[102] A "'less ambitious'" piece of legislation "than its predecessor,"[103] it simply would have required that employers provide notice before monitoring employees'

98. Lee, *supra* note 50, at 171 (discussing how "restrictions that limit monitoring to only new employees . . . are too inflexible"); Baxi & Nickel, *supra* note 97, at 145 (discussing how technology, like a video camera, may be unable to differentiate by longevity of worker and how some long-term employees "may have become complacent"); Alexander I. Rodriguez, Comment, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439, 1465 (1998) (discussing how PCWA created "an unreasonably strict standard for employers to justify the monitoring of experienced employees, regardless of the type of work with which an older worker may be involved"). Recently, for example, in Kentucky, an employee of approximately nine years, responsible for inspecting mine safety, allegedly failed to perform any mine inspections for at least a year. R.G. Dunlop, *Worker Faked Mine Reports, State Says*, COURIER-JOURNAL, April 20, 2009.

99. Boehmer, *supra* note 18, at 740 ("In addition, increased flexibility is needed in certain aspects of pending legislative proposals.").

100. The Proposed Act includes an exception for monitoring the employer's equipment.

101. The Workers Act requires only that the employer "has reason to believe [the reviewed data obtained from continuous monitoring] contains information relevant to an employee's work." This distinction may be particularly relevant in cases where employees blog or tweet.

102. Jacobs, *supra* note 37, at 865.

103. Yung, *supra* note 37, at 207 (quoting Charles E. Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. LAW. 857, 869 n.86 (2002)).

communications and computer use in the workplace.[104] It would have barred such monitoring without providing notice before monitoring and annually thereafter.[105] Notice would also have to be provided "[b]efore implementing a material change in an electronic monitoring practice."[106] The Notice Act did not cover employees' actions (which might be monitored by silent video or GPS) and may not have extended to monitoring of employees' communications and computer use outside the workplace.[107]

The Notice Act required "clear and conspicuous notice."[108] Moreover, the notice must have "in a manner reasonably calculated to provide actual notice" described: 1) the "form of communication or computer usage that will be monitored"; 2) "the means by which such monitoring will be accomplished"; 3) "the kinds of information that will be obtained through such monitoring, including whether communications or computer usage not related to the employer's business are likely to be monitored"; and 4) "how information used by such monitoring will be stored, used, or disclosed."[109]

There are some very limited circumstances in which notice would not have been necessary. An employer could monitor when it "has reasonable grounds to believe" 1) that an employee is violating the "legal rights of the employer or another person" and thereby causing significant harm to the victim and 2) that the monitoring will provide evidence of the violation.[110]

An employee would have been able to bring a civil action in United States District Court if an employer violated the Notice Act.[111]

104. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000). The operative language might be interpreted to extend protection to any type of monitoring of computer usage whether electronic or not, but given the statement of purpose, the drafters more likely intended only intentional monitoring by electronic means to be covered. "[A]n employer who intentionally, by any electronic means, reads, listens to, or otherwise monitors any wire communication, oral communication, or electronic communication of any employee of the employer, or otherwise monitors the computer usage of an employee of the employer . . ." H.R. 4908, at § 2(a)(1)(B). The National Workrights Institute recommends a Workplace Privacy Act that is substantially the same as the Notice Act. NATIONAL WORKRIGHTS INSTITUTE, PRIVACY UNDER SIEGE: ELECTRONIC MONITORING IN THE WORKPLACE 20-22 (2004), http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf.

105. H.R. 4908, at § 2(a)(1)(B).

106. *Id.*

107. H.R. 4908, at §§ 2, 2(a)(1)(B). While the operative language provides no such limitation, the statement of purpose and two titles indicate the bill addresses monitoring in the workplace.

108. H.R. 4908, at § 2(a)(1)(B).

109. *Id.*

110. *Id.*

111. *Id.*

Remedies were: 1) actual damages, "but not less than liquidated damages in the amount of $5,000"; 2) punitive damages; 3) reasonable attorney's fees and costs; and 4) other preliminary and equitable relief.[112] Money damages could not exceed $20,000, and an aggregate award for one violation could not exceed $500,000.[113]

The Notice Act would have imposed a two-year statute of limitations.[114]

The Notice Act was a straightforward attempt to provide a minimum level of protection for employees. While it was limited in scope, covering only a sub-set of technologies and possibly limited only to workplace monitoring, it would have been relatively easy to interpret and apply. It purportedly failed to pass because of employer opposition, referencing the increased workload for human resources employees and the potential increase in litigation.[115] Others, however, criticized the Notice Act for providing notice but no actual protection of employees' privacy.[116]

In some respects, the Proposed Act provides more flexibility to employers than the Notice Act[117] but is intended to provide a higher level of protection for employees' privacy. The Proposed Act extends to monitoring of employees' actions, not only their communications, and covers all employee behavior, whether within or outside of the workplace. The Proposed Act also provides employees more significant protections beyond notice, including a right to review certain categories

112. *Id.*

113. *Id.*

114. *Id.*

115. Nathan Watson, Note, *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?*, 54 FED. COMM. L.J. 79, 80 (2001). ("Unfortunately, employer groups succeeded in getting the Judiciary committee to pull the bill from further consideration. They cited a potential increase in litigation and more work for human resources professionals in complying with NEMA. The bill also languished in the Senate."). Some employers typically object to any legislation of the employment field. Yet, as noted by several scholars, several good reasons counsel passage of legislation protecting employees' privacy despite these protests: 1) employees "are now subject to oppressive invasions of monumental caliber" that require redress; 2) international standards, particularly those of Europe, are creating pressure to provide more adequate privacy protection; and 3) arguably, monitoring without restraint actually creates high costs to employers "in lost productivity and profit." Laura B. Pincus & Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers*, 33 AM. BUS. L.J. 51, 81-82 (1995); Wilborn, *supra* note 18, at 885-86.

116. Todd M. Wesche, *Reading Your Every Keystroke: Protecting Employee E-mail Privacy*, 1 J. HIGH TECH. L. 101, 114 (2002) ("NEMA's focus is disclosure, not elimination, of monitoring, and the requirement of notice may operate more as a disclaimer of liability as opposed to an actual protection of employee's privacy.").

117. See *supra* notes 96-97 and accompanying text.

of collected information and prohibitions on monitoring in certain locations, such as changing areas within the workplace and employees' homes.[118]

C. State Legislation

There are several different kinds of state legislation providing some protection for employees' privacy from employer monitoring. Two states require notice of electronic monitoring;[119] two states provide protection from monitoring, whether technological or not, of non-employment activities; and four states protect against discharge or adverse action because of lawful off-duty conduct.[120]

1. Notice of Electronic Monitoring

Two states, Connecticut and Delaware, require that employers provide employees notice of electronic monitoring.[121]

a. Connecticut's Notice of Electronic Monitoring Act

Connecticut has a statute governing "employers engaged in electronic monitoring"[122] ("Connecticut Act"). The Connecticut Act

118. An exception is provided for monitoring the employer's property.

119. Similar legislation has been considered, but not implemented in other jurisdictions. *See* Matthew E. Swaya & Stacey R. Eisenstein, *Emerging Technology in the Workplace*, 21 LAB. LAW. 1, 13 (2005) (discussing proposal in California); Jarrod J. White, Commentary, *E-Mail@work.com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079, 1099 (1997) (discussing proposals in Arkansas and Oklahoma).

120. Lawful activity bills were considered but failed to pass in Michigan and Pennsylvania. Sonne, *supra* note 18, at 176-77. At least six states "provide 'a criminal sanction for employers who restrict their employees' freedom to shop, trade, or patronize where they will.'" Sonne, *supra* note 18, at 172 (quoting Finkin, *supra* note 18, at 425). Four states also prohibit "employers from embedding radio frequency identification chips in their employees." Sprague, 42 *supra* note 17, at 86. The Proposed Act absolutely prohibits technological monitoring of certain off-duty behavior and permits other such monitoring only with substantial justification. It would apply to RFID chips as well as any other form of technological monitoring, but the topic of legislation particularly addressing RFID chips is beyond the scope of this article.

121. Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. & POL'Y J. 471, 477-78, n.36, n.37 (citing CONN. GEN. STAT. § 31-48d (1999), DEL. LAWS CODE, tit. 19, § 705(b) (Supp. 2002)).

122. CONN. GEN. STAT. § 31-48d (2008). The ACLU has proposed a Model Electronic Privacy Act. American Civil Liberties Union, *Legislative Briefing Kit on Electronic Monitoring*, ACLU, Mar. 11, 2002, http://www.aclu.org/privacy/gen/14798res20020311.html. It is a notice act which contains provisions similar to the Workers Act, the Notice Act, and the Connecticut Act. *See id.* Rather than prohibiting monitoring, it permits monitoring at the workplace that is related to work, including incidental collection of non-work related information. *See id.* § 2. It requires "prior written notice" of all electronic monitoring, including notice of the "times at which the monitoring

prohibits only monitoring which takes place at the workplace.[123] The definition of electronic monitoring is broader than that in the Notice Act because it includes monitoring an employee's "activities or communications by any means other than direct observation."[124] It exempts "collection of information for security purposes in common areas of the employer's premises which are held out for use by the public."[125]

Before monitoring, an employer must provide written notice "to all employees who may be affected."[126] The notice must state "the types of monitoring which may occur."[127] Notice of "the types of" monitoring in which "the employer may engage" must be posted in a "conspicuous place."[128]

The Connecticut Act includes an exception from notice when the "employer has reasonable grounds to believe that employees are engaged in conduct . . . which violates the law" and the "monitoring may produce evidence of this misconduct."[129]

---

is to occur" and "the location of the monitoring equipment." *See id.* § 3. The exception to providing notice mirrors that in the Notice Act. *See id.* § 3(b); *supra* note 110 and accompanying text. When employers randomly monitor, they must additionally provide notice at the time of actual monitoring, unless doing so as part of a specific defined type of quality control program. *See* American Civil Liberties Union, *supra*, at § 4. It also contains a provision similar to the Workers Act prohibiting monitoring in private areas. *See id.* § 5. It prohibits disclosure of collected information except to law enforcement agencies or "officers, employees, or authorized agents of the employer who have a legitimate need for the information" unless the employee provides "prior written consent" that "shall not be a condition of employment." *See id.* § 6.

123. Electronic monitoring is defined to include only "collection of information on an employer's premises." CONN. GEN. STAT. § 31-48d(a)(3) (2008). Two unpublished decisions confirm that monitoring off of the employer's premise is not addressed by the act. Gerardi v. City of Bridgeport, No. CV084023011S, 2007 WL 4755007, at *7 (Conn. Super. Ct. Dec. 31, 2007); Vitka v. City of Bridgeport, No. CV08040229615, 2007 WL 4801298, at *7 (Conn. Super. Ct. Dec. 31, 2007).

124. CONN. GEN. STAT. § 31-48d(a)(3) (2008).

125. § 31-48d(a)(3).

126. § 31-48d(b)(1).

127. *Id.*

128. *Id.* While the statute's language suggests that the posted notice satisfies the requirement of providing employees prior written notice by stating: "Such posting shall constitute such prior written notice," the Attorney General has stated that, "[t]his section requires that written notice be given to each employee whose conversations will be monitored and the posting of notices regarding the monitoring." 2001 Conn. AG LEXIS 1 (2001).

129. CONN. GEN. STAT. § 31-48d(b)(2) (2008) (The exception also applies when there is "reasonable grounds to believe" the employee's conduct "violates the legal rights of the employer" or a co-employee or "creates a hostile" work "environment." But these would seem to be encompassed by the broader first exception.).

No individual remedy appears to be provided by the statute.[130] Instead, the Connecticut Labor Commissioner may "levy a civil penalty."[131] The penalty for the first offense is $500; for the second offense, the penalty is $1000; and for each offense thereafter the penalty is $3000.[132] Additionally, the Labor Commissioner may request the Attorney General to seek an additional penalty of $300 for each violation.[133] The additional penalty is deposited for use by the Labor Department in enforcing the act and other employment regulations.[134]

The Connecticut Act probably serves an important educational function by alerting some employees that their behavior in the workplace may be monitored and by explaining the types of monitoring that may occur. Additionally, the broad definition of electronic monitoring will likely ensure that the Connecticut Act keeps apace with changing technology. For this reason, the Proposed Act adopts a similar definition of technological monitoring. [135]

Additionally, the Connecticut Act provides for a penalty to fund the Connecticut Department of Labor's enforcement mechanisms which is a reasonable means to address concerns about the cost of enforcing employees' privacy rights.[136] The Proposed Act also provides for a civil penalty to help fund the Department of Labor's enforcement efforts.

The Connecticut Act does not, however, appear likely to provide significant actual protection of employees' privacy. The permissive wording of the notice, indicating an employer "may" monitor would not definitively indicate to employees that monitoring is occurring. Indeed, in a workplace where monitoring does not normally take place, employees may have a false sense of security that monitoring is not actually taking place,[137] but the notice would permit the employer to assert the employee was warned that monitoring "may" take place. Thus, when notice is required by the Proposed Act, the notice must be

130. *See* Stephen B. Harris, 14 CONN. PRAC., EMPLOYMENT LAW § 3:3 (2008) ("No private right of action is provided for in the Electronic Monitoring Act."). Despite the apparent lack of a private right of action, the Connecticut Superior Court has decided in two cases seeking injunctive relief that the Connecticut Act was not violated. Gerardi v. City of Bridgeport, No. CV084023011S, 2007 WL 4755007, *8 (Conn. Super. Ct. Dec. 31, 2007); Vitka v. City of Bridgeport, No. CV0804022961S, 2007 WL 4801298, at *8 (Conn. Super. Ct. Dec. 31, 2007).

131. CONN. GEN. STAT. § 31-48d(c) (2008).

132. § 31-48d(c). There is an exemption from the section for criminal investigations. § 31-48d(c).

133. CONN. GEN. STAT. § 31-69a(a) (2008).

134. § 31-69a(b).

135. *See infra* notes 532-33 and accompanying text.

136. § 31-69a(b).

137. Levinson, *supra* note 14, at 669 & n.306.

more explicit in explaining that monitoring is occurring. Additionally, the Connecticut Act fails to provide protection from monitoring in the cases where monitoring is most intrusive: when the employee is off-duty and away from the workplace. Moreover, the apparent lack of an individual remedy is likely to lead to under-enforcement.[138]

b. Delaware's Notice of Monitoring Requirement

Delaware prohibits monitoring of "telephone transmissions, electronic mail and Internet usage" without notice ("Delaware Act").[139] The Delaware Act applies inside and outside the workplace, but only to these narrow categories of behavior.

The employer must provide one of two types of notice: 1) an electronic notice "at least once during each day the employee accesses the employer-provided e-mail or Internet access services" or 2) a written or electronic notice, before monitoring, of the governing policies, which is acknowledged by the employee "in writing or electronically."[140]

There is an exception for "processes that are designed to manage the type or volume of incoming or outgoing electronic mail or telephone voice mail or Internet usage, that are not targeted to monitor or intercept the electronic mail or telephone voice mail or Internet usage of a particular individual, and that are performed solely for the purpose of computer system maintenance and/or protection."[141]

The Delaware Act is enforceable in court and imposes a civil penalty of $100 for each violation.[142]

The Delaware Act is a laudable attempt to ensure that employees have notice before their communications are monitored. It extends protection outside the workplace to off-duty behavior, the monitoring of which is highly likely to intrude on an employee's privacy.[143] The Delaware Act, however, lacks clarity about what content the notice must contain. Must it merely state that "communications may be monitored"? Must it specify which communications are being monitored? Must it specify particular details about not only which communications are being monitored but the method by which they are being monitored?

138. *See* Cynthia Estlund, *The Story of* NLRB v. Washington Aluminum*, in* EMPLOYMENT LAW STORIES 175, 209 (Samuel Estreicher & Gillian Lester, eds., Foundation Press, 2007) (discussing how fear of litigation "can be an excellent stimulus" for internal employer reforms).

139. DEL. CODE ANN. tit. 19, §§ 705, 705(b) (2008).

140. tit. 19, §§ 705(b)(1), (b)(2).

141. tit. 19, § 705(e).

142. tit. 19, § 705(c).

143. tit. 19, § 705

Unfortunately, the requirement has not been fleshed out in any decisions that the author could obtain.

Overall, the Delaware Act is unlikely to provide adequate protection for employees. The notice provisions lack clarity; the Delaware Act fails to provide safeguards other than notice for employees' privacy; and the penalty is minimal and obtainable only through court action. Moreover, the Delaware Act targets limited types of communications, likely failing to protect communications made by newly developed and future technologies.[144] Thus, the Proposed Act specifies different types of notice that should be provided, varying with the level of intrusion; includes safeguards beyond notice; and contains more substantial penalties, available either through administrative procedure or court action.[145] Additionally, the Proposed Act contains a broad definition of technological monitoring enabling it to adapt to the development of new technology.[146]

2. Prohibitions on Monitoring Related to Integrity of Personnel Records

Two states, Michigan and Illinois, integrate prohibitions on collecting information, by technological monitoring or otherwise, about certain employee behavior into statutes which govern the use of personnel records.[147]

a. Michigan's Prohibition on Monitoring

Michigan forbids employers from gathering or keeping a record of "an employee's associations, political activities, publications, or communications of nonemployment activities" ("Michigan Act").[148] If, however, the employee authorizes, in writing, such monitoring, then the employer may gather or keep a record of such information.[149] Additionally, the prohibition does not apply to "activities that occur on the employer's premises or during the employee's working hours . . .

144. *Id.*

145. *Id.*

146. *Id.*

147. Bullard-Plawecki Employee Right to Know Act, MICH. COMP. LAWS § 423.508 (2008); 820 ILL. COMP. STAT. 40/9 (2008); *see also* Finkin, *supra* note 121, at 491 & n.112.

148. "Keeping record of employee's nonemployment activities prohibited, exception; part of personnel record." MICH. COMP. LAWS § 423.508(8)(1) (2008).

149. § 423.508(8)(1). The law also permits keeping a record of information the employee provides in writing.

that interfere with the performance of the employee's duties or duties of other employees."[150]

An employee may sue an employer who is engaging in prohibited monitoring for an order to cease monitoring and for actual damages and costs. If the employee proves the violation was "willful and knowing" the court will award "$200.00 plus costs, reasonable attorney's fees, and actual damages."[151]

The Michigan Act also provides that any record permissibly kept because of the employee's authorization or because of the exception for interference with duties must be part of the employee's personnel record.[152]

The Michigan Act provides employees the right to review the personnel record approximately twice in a calendar year at a reasonable time and location convenient to the employee.[153] After reviewing the record, the employee may obtain a copy, for which the employer may charge a fee equal to actual copying costs. Alternatively, if an employee is unable to review the record "at the employing unit," the employer will mail a copy to the employee per written request.[154]

Employees also have a right to contest erroneous information contained in the personnel record. If the employer does not agree that the information is incorrect then an employee statement addressing the allegedly incorrect information, of a limited length, must be included in the personnel record. Additionally, the employee or the employer, may sue to have information knowingly placed "in the personnel record" that "is false" removed.[155]

The Michigan Act permits, however, keeping information gathered when the "employer has reasonable cause to believe that an employee is engaged in criminal activity which may result in loss or damage to the employer's property or disruption of the employer's business operation" separate from the personnel record.[156] The employee has no right to review such information but must receive notice of the investigation,

150. § 423.508(8)(1) (While it is possible to read the language as indicating that all monitoring on the employer's premises is exempt, the restrictive clause "that interfere with the performance of the employee's duties . . ." probably modifies that phrase.).

151. MICH. COMP. LAWS § 423.511 (2008).

152. MICH. COMP. LAWS § 423.508(2) (2008).

153. MICH. COMP. LAWS § 423.503 (2008).

154. MICH. COMP. LAWS § 423.504 (2008).

155. MICH. COMP. LAWS § 423.505 (2008). Additionally, the law protects against employers using information about employees in judicial and "quasi-judicial proceedings" without the employee having an opportunity to review the information. MICH. COMP. LAWS § 423.502 (2008).

156. MICH. COMP. LAWS § 423.509 (2008).

upon its completion or within two years, "whichever comes first."[157] If disciplinary action does not result, the material must be destroyed.[158]

The Michigan Act provides one potential framework to protect employees from some range of technological monitoring both on and off duty.[159] The right of review and to contest records of monitoring is an important safeguard against collection of personal information without an employee's knowledge and against maintenance of incorrect information. The Proposed Act adopts a similar review procedure, absent the right to sue for removal of information. The ability to contest the accuracy of information via a statement should sufficiently protect employees without imposing the costs of a suit on the employee, employer, and court system.

Yet, the Michigan Act's protections are more limited than those of the Proposed Act, which extends protection to technological monitoring of all on-duty and off-duty behavior. Moreover, the Michigan Act's authorization requirement probably effectively permits most monitoring, leaving only the safeguard of a right to review and contest. Authorization, similar to consent, is not generally a realistic protection in the workplace because of the unequal bargaining power, in most instances, between an employer and an employee.[160] Most employees

157. *Id.*

158. *Id.*.

159. A relatively recent unpublished decision may considerably narrow the categories of prohibited monitoring. Goodrich v. Home Depot, No. 281652, 2009 WL 154341, at *3-4 (Mich. Ct. App. Jan. 22, 2009). The decision appears to apply the modifier "nonemployment activities" to each listed type of activity rather than only to communications (an interpretation potentially suggested by the section title "Keeping record of employee's nonemployment activities prohibited."). *Id.* at *3. Additionally, the decision holds that an activity prohibited by an employer policy, in this case a romantic relationship with a subordinate, is an employment activity, with the caveat that whether an activity constitutes a nonemployment activity must be "decided on a case-by-case basis." *Id.* Under this rationale, an employer could, for instance, ban any non-work use of a computer and then argue that a personal e-mail is an employment activity.

160. *See* Gantt, *supra* note 37, at 407 ("Especially considering the recent decline in the percentage of employees involved in collective bargaining, employees today often must either accept the employer monitoring, protest and face possible termination, or voluntarily terminate employment."); Pauline T. Kim, *Privacy Rights, Public Policy, and the Employment Relationship*, 57 OHIO ST. L.J. 671, 720 (1996) ("While theorists may disagree about the conditions under which consent is truly voluntary, the courts have increasingly been willing to acknowledge that in the employment context 'freedom of contract' may at times be illusory. Because employer and employee 'do not stand on equal footing,' employer power may be wielded to achieve socially undesirable ends."); Boehmer, *supra* note 18, at 814 ("Of course, the employee who is unwilling to modify her expectations always has the theoretical option to terminate the employment relationship or to assert pressure on the employer to cease the monitoring as a condition of maintaining the employment relationship. These theoretical alternatives are unlikely to be practical alternatives to the vast majority of workers, who do not have the luxury of quitting based on a difference in principle with the employer and who stand in an inferior bargaining position to the employer.");

do not have multiple job opportunities at one time and so will be under great pressure to sign a consent form rather than lose their jobs. While consent, as a form of notice, and a right of review may adequately protect employees' privacy from monitoring of on-duty conduct where the privacy intrusion is least invasive, the Proposed Act provides greater protection from monitoring of on-duty communications and computer use and of off-duty behavior because the privacy intrusion is greater in those situations.

Further, as to on-duty communications, it may be difficult for employers not to monitor "communications of nonemployment activities" because an employer may incidentally monitor personal nonemployment communications while monitoring employment communications.[161] The Proposed Act adopts a framework that is intended to provide employers greater guidance and more flexibility to monitor employees' communications while at the same time providing adequate protection for employees from monitoring of non-employment related communications.

The exception in the Michigan Act effectively permits monitoring on-duty behavior that "interferes with the performance of employees' duties"[162] with only a right to review and contest the gathered information. The Proposed Act attempts to more clearly define the standards under which monitoring of on-duty behavior is appropriate and to provide employers more flexibility to monitor. It also provides employees with safeguards in addition to the right to review and contest because of the invasive nature of secret monitoring.

Ultimately the Michigan Act is a laudable attempt to protect employees from collection and recording of private information.

Michael Ford, *Two Conceptions of Worker Privacy*, 31 INDUS. L.J. 135, 154 (2002) ("An individual model of information and consultation is hardly sufficient, since it will suffer from the same difficulties that bedevil consent: in the context of unequal bargaining power it will rarely be genuine."). *See* Childrey v. Capital Area Cmt. Sers., Inc., Nos. 204050, 207843, 1999 WL 33453925, at *3 (Mich. Ct. App. Mar. 5, 1999) (affirming the trial court's grant of summary judgment to the defendant for the plaintiff's claim under the Employee Right to Know Act, noting that the while the plaintiff refused to authorize the defendant to collect her personal information, the plaintiff failed to show that the defendant actually collected such information).

161. For instance, even if an employer requested employees to mark e-mail "personal," an employee might forget resulting in monitoring of a personal e-mail. Or an employer might reasonably believe an employee is using e-mail marked personal to share trade secrets, but discover it is incorrect after monitoring the e-mail.

162. The standard for the exception is not clear. The employer may have to have concrete outside evidence from non-monitoring that the activity is interfering with work before monitoring. Or, for example, the employer may be able to assert that use of e-mail for personal purposes generally interferes with work and, thus, will monitor all e-mail use without further safeguard.

However, a law such as the Proposed Act, that more directly and extensively addresses protection from technological monitoring, whether as a stand alone bill, part of a personnel record act, or part of another privacy scheme, would more adequately balance the protection of employees' rights to privacy with employers' legitimate needs to technologically monitor.

b. Illinois' Prohibition on Monitoring

The Illinois statute ("Illinois Act") prohibits monitoring of "communications," unmodified by the term "nonemployment," and of "nonemployment activities" in addition to prohibiting monitoring of "associations, political activities, [or] publications."[163] It, thus, appears to provide somewhat broader protection than the Michigan Act. Like the Michigan Act, it provides an exception when the employee authorizes the monitoring in writing."[164]

Like the Michigan Act, the Illinois Act permits monitoring "[a]ctivities that occur on the employer's premises or during the employee's working hours" that[165] "interfere with the performance of the employee's duties or the duties of other employees."[166] While a literal reading of the Illinois Act suggests that there is no exemption to monitor communications in any circumstances because only "activities" are exempted, the legislature likely intended the exceptions to apply to all the categories for which monitoring is prohibited.[167] Also, like the Michigan Act, any records permitted by this exception must be part of the employee's personnel record and subject to the employee's review.[168]

The Illinois Act, however, treats criminal conduct differently from the Michigan Act. Rather than provide a right to monitor certain criminal conduct without permitting review of the resultant records by the employee, the Illinois Act permits monitoring of any criminal conduct without review unless "the employer takes adverse personnel action based on" the collected information.[169] Information gathered under exceptions for activities that "may reasonably be expected to harm

163. 820 ILL. COMP. STAT. 40/9 (2008).

164. *Id.*

165. *Id.* The statute says "which," leading to a bit of ambiguity as to whether all on-duty activities can be monitored, but the phrase appears to be limiting, not explanatory. *See* 40/9.

166. *Id.*

167. *Id.*

168. *Id.*

169. 820 ILL. COMP. STAT. 40/10(g) (2008).

the employer's property, operations or business," and activities that could "cause the employer financial liability"[170] are treated the same.

Unlike the Michigan Act, however, the remedial procedure involves an administrative agency, the Illinois Department of Labor ("Department"). The employee must file a claim with the Department.[171] The Department can obtain a "subpoena to inspect the files of the employer."[172] The Department will first attempt conciliation. If conciliation is not successful and the Department "finds the employer has violated the Act," the Department may commence a court action, including an action to obtain an injunction against prohibited monitoring.[173]

If the Department elects not to file suit, then the employee may file suit.[174] The employee may obtain damages and injunctive relief. Additional remedies like those of the Michigan Act are available for willful violations. The Illinois Act also provides criminal sanctions and an anti-retaliation provision.[175]

The Illinois Act permits an employee to review certain information collected.[176] The employer may require requests to be in writing on an employer provided form.[177] The right of review is for information that is, has been, or is "intended to be used in determining that employee's qualifications for employment, promotion, transfer, additional compensation, discharge or other disciplinary action . . . ." Employers must grant at least two reviews per calendar year.[178] In addition to requirements like those in the Michigan Act regarding the time and location of the review, the Illinois Act requires that the review take place within seven "working days after the employee makes the request." [179] The employer is also entitled when necessary to an additional seven-day extension.[180] In addition to requirements, like those in the Michigan Act, permitting the employee to copy information, the Illinois Act

170. § 10(g).

171. 820 ILL. COMP. STAT. 40/12(b) (2008).

172. § 12(b).

173. 820 ILL. COMP. STAT. 40/12(b) (2008).

174. 820 ILL. COMP. STAT. 40/12(c) (2008). This is a traditional exhaustion requirement, but the employer must assert failure to exhaust as an affirmative defense. *See* Robinson v. Morgan Stanley, No. 06 C 5158, 2007 WL 2815839, at *12 (N.D. Ill. Sept. 24, 2007).

175. 820 ILL. COMP. STAT. 40/12(f) (2008).

176. 820 ILL. COMP. STAT. 40/2 (2008).

177. § 2.

178. § 2. The reviews must be "at reasonable intervals," and a collective bargaining agreement can provide for less than two reviews. *Id.*

179. *See supra* notes 153-154 and accompanying text; § 2.

180. § 2.

requires the employer to let the designated representative of an employee who is involved in a grievance review relevant information.[181]

The process for contesting information is similar to that in the Michigan Act, but without a limit on the length of the statement an employee may submit to contest information.[182]

The Illinois Act also contains a provision limiting disclosure of "disciplinary action" to a third party.[183]

Like the Michigan Act, the Illinois Act contains extensive procedures for review and contest of information that the Proposed Act relies on as a model to ensure accuracy and reliability of information collected by technological monitoring.[184] Additionally, the Illinois Act uses an enforcement procedure that involves an administrative agency.[185] The Proposed Act also integrates an administrative agency into the enforcement procedure on the rationale that involvement of an administrative agency saves resources, permits employers more flexibility, and is less costly for employees.[186]

The Illinois Act appears to protect more types of conduct from monitoring than the Michigan Act and to provide employers more flexibility to monitor. But the Illinois Act has several of the same drawbacks as the Michigan Act, including the failure to extend protection to monitoring of all employee behavior and the minimal level of protection provided by authorization and a right to review.

3. Protection of Off-Duty Behavior

New York, North Dakota, and Colorado protect against discharge or adverse action based on off-duty behavior.[187]

---

181. 820 ILL. COMP. STAT. 40/5 (2008).

182. 820 ILL. COMP. STAT. 40/6 (2008); *see supra* note 155 and accompanying text.

183. 820 ILL. COMP. STAT. 40/7 (2008).

184. *See generally* 820 ILL. COMP. STAT. 40 (2008).

185. *See generally* 820 ILL. COMP. STAT. 40 (2008).

186. *See infra*, Section VI. N.

187. Gely & Bierman, *supra* note 19, at 320. California has a provision that might be interpreted as a similar statute prohibiting employers from discriminating on the basis of "conduct occurring during nonworking hours away from the employer's premises." It permits the Labor Commissioner to take assignment of any such claim filed by an employee. The provision has, however, been interpreted by published California Court of Appeals decisions, to date, to provide only a procedural means to vindicate constitutional privacy rights. Grinzi v. San Diego Hospice Corp., 120 Cal. App. 4th 72, 86 (2004); Barbee v. Household Automotive Finance Corp., 113 Cal. App. 4th 525, 532 (2003); *see* John S. Hong, Comment, *Can Blogging and Employment Co-Exist*, 41 U.S.F.L. Rev. 445, 462-65 (2007). Several employees have brought unsuccessful claims for invasion of privacy under the California constitution pursuant to the statute when their employers terminated them because of off-duty relationships. *Barbee*, 113 Cal. App. 4th at 531-32; Paloma v.

a. New York's Statute Prohibiting Discrimination against Certain Off-Duty Activities

New York enacted a limited off-duty activities[188] statute in 1992 ("New York Act").[189] The New York Act prohibits not only termination, but also refusal "to hire, employ or license" and any discrimination "in compensation, promotion or term, conditions or privileges of employment" based on several categories of conduct.[190] An employer is prohibited from discriminating against an employee based upon the employee's political activities, "legal use of consumable products," or legal recreational activities "outside work hours, off of the employer's premises and without use of the employer's equipment or other property."[191]

"Recreational activity" is defined as "any lawful, leisure-time activity, for which the employee receives no compensation and which is generally engaged in for recreational purposes . . ."[192] The definition includes the following illustrative examples "sports, games, hobbies, exercise, reading and the viewing of television, movies and similar

City of Newark, No. A098022, 2003 WL 122790, at *14 (Cal. App. Jan. 10, 2003); Agabao v. Delta Design, Inc., No. D039642, 2003 WL 194950, at * 4 (Cal. App. Jan. 30, 2003); Tavani v. Levi Strauss & Co., No. A095770, 2002 WL 31623684, at *17 (Cal. App. Nov. 21, 2002), and it appears to be an open issue whether termination for other types of off-duty conduct would violate the California constitutional right to privacy, *Grinzi*, 120 Cal. App. 4th at 80 n.3. A discussion of that topic is beyond the scope of this article. Additionally, off-duty activity bills were introduced but did not pass in Michigan and Pennsylvania. Sonne, *supra* note 18, at 176-77. Some states more narrowly prohibit employers from restricting "employees' freedom to shop, trade or patronize where they will." Sonne, *supra* note 18, at 172 & n.229. Connecticut provides protection for private employees discharged for exercising the right to free speech about a matter of public concern. Jon Darrow & Steve Lichtenstein, *Employment Termination for Employee Blogging: Number One Tech Trend for 2005 and Beyond, or a Recipe for Getting Dooced?*, 2006 UCLA J.L. TECH. 4, at 50-59 (2006). Some scholars also classify Massachusetts' statute that protects against "unreasonable . . . interference with" privacy as a lifestyle discrimination statute. *See, e.g.*, Sonne, *supra* note 18, at 177; Aaron Kirkland, Note, *"You Got Fired? On Your Day Off?!": Challenging Termination of Employees for Personal Blogging Practices,* 75 UMKC L. REV. 545, 556-57 (2006).

188. The types of statutes discussed in this section are commonly referred to as off-duty activity or lifestyle discrimination statutes.

189. Some in New York refer to the New York Act as the Lawful Activities Law or the Legal Activities Law.

190. Discrimination against the engagement in certain activities, N.Y. LAB. LAW § 201-d(2) (McKinney 1992). One category is membership in a union or exercise of civil service rights.

191. § 201-d(2)(a) – (c). *See id.* § 201-d(1)(a) (defining "political activities").

192. § 201-d(1)(b).

material." The definition also excludes discrimination because of other employment.[193]

The definition of "recreational activities" is broad enough to encompass much behavior that might be easily technologically monitored, such as blogging, tweeting, or using Facebook.[194] Blogging, tweeting, and using Facebook are generally engaged in as a leisure activity and, thus, would not run afoul of any interpretation of the New York Act requiring that the activity be done for leisure.[195] The New York Act may not, however, extend to protect other types of behavior that might be technologically monitored, such as dating someone of a different race or associating with convicts, because this behavior may be classified as a relationship rather than an activity. In fact, the New York courts have generally read the statute restrictively to include only activities like those listed and to exclude romantic relationships.[196]

The definition of work hours extends to "all time the employee is actually engaged in work."[197] Thus an employer can discriminate against an employee based on behavior that takes place at home while working. For instance, if an employee is working on a computer at home and smoking, the employer can terminate the employee for smoking while working. Or, if an employee's tweet stated the employee is working and also engaging in behavior of which the employer disapproves, the employee can be terminated for the disapproved behavior or even for the tweeting itself. The definition also extends to "paid and unpaid breaks and meal periods."[198] The inclusion of break time is particularly problematic because if an employee engages in political activity during break, the employee can be discriminated against.

---

193. *See* Cheng v. N.Y. Tel. Co., 64 F. Supp. 2d 280, 285 n.2 (S.D.N.Y. 1999) (holding claim brought by employee whose duties included installing telephone equipment and who was installing telephone equipment for personal profit was frivolous).

194. *Cf.* Cavanaugh v. Doherty, 243 A.D.2d 92, 100 (N.Y. App. Div. 1998) ("having alleged that she was terminated as a result of a discussion during recreational activities outside of the workplace in which her political affiliations became an issue, she has also stated a cause of action for a violation of Labor Law § 201-d"); Richardson v. Saratoga Springs, 246 A.D.2d 900, 902 (N.Y. App. Div. 1998) ("a reasonable factfinder could conclude he was discriminated against in compensation and promotion because of his political activities outside of working hours.").

195. While the statute requires only that the activity occur during leisure time, whether or not done for leisure, one court has limited the activities to those done for leisure, linking the leisure and recreational activity requirements. Kolb v. Camilleri, 02-CV-0117A(Sr), 02-CV-0117A, 2008 U.S. Dist. LEXIS 59549, at *36 (W.D.N.Y. Aug. 1, 2008) (holding that picketing engaged in as a protest is not a recreational activity because not engaged in "for his leisure").

196. *See infra* note 211 and accompanying text; Hong, *supra* note 187.

197. § 201-d(1)(c).

198. § 201-d(1)(c).

Finally, there are numerous exceptions, two of which warrant further discussion.[199] The exception for conflicts of interest exempts activity which "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest."[200] Whether a material conflict with a business interest is meant to be narrowly related to information similar to proprietary information or expands the definition to encompass working for another business in a related field is unclear. For instance, would a newspaper reporter who freelanced for sports teams on which he reported be engaged in activity creating a material conflict of interest with the employer's business interest?[201] One federal court has interpreted the exception broadly to permit "an employer" to discharge an employee "for conduct that is detrimental to the company or that impacts an employee's job performance."[202]

Another exception exempts employers who discriminate because they believe that: 1) their actions are "required by statute, regulation, ordinance or governmental mandate"; 2) their actions are "permissible pursuant to an established substance abuse or alcohol program or workplace policy, professional contract or collective bargaining agreement"; or 3) the employee's conduct was "deemed . . . illegal or to constitute habitually poor performance, incompetency or misconduct."[203] Ascertaining how broad these exemptions are is difficult.[204]

An aggrieved employee may sue for "equitable relief and damages."[205] Additionally, the attorney general may seek injunctive relief and "a civil penalty in the amount of three hundred dollars for the first violation and five hundred dollars for each subsequent violation."[206]

Only one reported case addresses a situation where an employer discovered some of the contested activity via technological

199. § 201-d(3).

200. § 201-d(3)(a).

201. *See, e.g.*, St. Louis Post-Dispatch, 117 Lab. Arb. Rep. (BNA) 1274 (2002) (Daly, Arb.).

202. Pasch v. Katz Media Corp., 94 Civ. 8554 (RPP), 10 I.E.R. Cas. (BNA) 1574, 1995 U.S. Dist. LEXIS 11153, at *5 (S.D.N.Y. Aug. 7, 1995). *But see* McCavitt v. Swiss Reinsurance Am. Corp., 237 F.3d 166, 168 (2d Cir. 2001). *See also* Aquilone v. Republic Nat'l Bank of N.Y., 98 Civ. 5451 (SAS), 1998 U.S. Dist. LEXIS 19531, at *17 (S.D.N.Y. Dec. 15, 1998).

203. § 201-d(4).

204. One decision interprets the provision broadly to permit an employer to "discharge an employee for conduct that is detrimental to the company or that impacts an employee's job performance." *Pasch,* 1999 U.S. Dist. LEXIS 11153 at *5. *But see McCavitt* 237 F.3d at 168. *See also Aquilone*, 1998 U.S. Dist. LEXIS 19531, at *17.

205. § 201-d(7)(b).

206. § 201-d(7)(a).

monitoring.[207] In *Cheng*, an employee whose job duties included installing telephone equipment was discovered installing telephone equipment for a number of competing businesses. One of the methods used by the security investigator assigned to investigate the matter was reviewing the employee's "personal telephone billing records."[208] He discovered through these records that the employee "had telephoned from his home a competing telecommunications vendor."[209] Because the case so clearly did not involve recreational activity, it does not provide guidance on whether the New York Act would generally provide any protection against employer technological monitoring of employees.

Many of the cases address the issue of whether, in various different circumstances, an employer can terminate an employee for "a romantic relationship" with a co-worker.[210] The majority of courts have held that an employer may do so,[211] though not without some dissent.[212] And one federal district court decision suggested that an employer may not[213] but was impliedly overruled by the Second Circuit.[214] While the issue is an important one that the highest court of New York, the New York Court of Appeals, has not yet addressed, it is not crucial when considering the off-duty activities statutes as potential models for providing that appropriate safeguards for employee privacy are in place when they are technologically monitored by their employers.[215]

---

207. *See* Cheng v. N.Y. Tel. Co., 64 F. Supp. 2d 280 (S.D.N.Y. 1999).

208. *Id.* at 282.

209. *Id.*

210. *See infra* note 211.

211. State v. Wal-Mart Stores Inc., 207 A.D.2d 150, 152 (N.Y. App. Div. 1995) (Yesawich, J. dissenting); McCavitt v. Swiss Reinsurance Am. Corp., 89 F. Supp. 2d 495, 497-98 (S.D.N.Y. 2000) *aff'd* 237 F.3d 166 (2d Cir. 2001); Hudson v. Goldman Sachs & Co., 283 A.D.2d 246 (N.Y. App. Div. 2001); Bilquin v. Roman Catholic Church, 286 A.D.2d 409 (N.Y. App. Div. 2001).

212. *Wal-Mart Stores Inc.*, 207 A.D.2d at 152; *see also McCavitt*, 237 F.3d 166 (2d Cir. 2001) (McLaughlin, J., concurring) (urging New York Appellate Court to adopt the position advanced in Judge Yesawich's dissent).

213. Pasch v. Katz Media Corp., 94 Civ. 8554 (RPP), 10 I.E.R. Cas. (BNA) 1574, 1995 U.S. Dist. LEXIS 11153 (S.D.N.Y. Aug. 7, 1995). *But see McCavitt*, 237 F.3d at 168. *See also* Aquilone v. Republic Nat'l Bank of N.Y., 98 Civ. 5451 (SAS), 1998 U.S. Dist. LEXIS 19531, at *17 (S.D.N.Y. Dec. 15, 1998) (holding that friendship is a protected recreational activity).

214. *McCavitt*, 237 F.3d at 168 ("To the extent that *Pasch* and *Aquilone* suggest a contrary result, for the foregoing reasons, we disagree.").

215. For instance, under the Proposed Act, firing someone for having a relationship would be perfectly appropriate. In all of these situations reported in the New York decisions, the employer learned of the relationship by some manner other than technological monitoring. The Proposed Act would prohibit technological monitoring of off-duty relationships in the home and at times that off-duty employees are in private areas. And in most instances, a relationship would not have a concrete significant harm on the employer's business and so an employee could not be technologically monitored for off-duty relationships at all.

The New York Act may provide some protection for an employee's privacy from being monitored off-duty because an employee could not be disciplined for much behavior that might be discovered as a result of monitoring, rendering the monitoring unnecessary. Yet, employees would not have protection from any monitoring that led to a termination for behavior that falls under the exceptions.[216] In contrast, the Proposed Act would permit technological monitoring to discover off-duty behavior that would have a significant, concrete harm on the employer, such as the employee who was working for competitors in the *Cheng* case, but it would protect employees' privacy by providing that employers implement certain safeguards.

Furthermore, the nature of the invasion of privacy resulting from the monitoring is not addressed by the off-duty activity statutes. Rather, similar to many arbitration decisions in discharge cases, the focus is on job security and correcting inequitable discipline. A statute more focused on protecting employees' privacy from technological monitoring, such as the Proposed Act, would more clearly remedy the invasion of privacy resulting from the monitoring itself.

b. North Dakota's Statute Protecting Lawful Off-Duty Activity

As part of its anti-discrimination statute, North Dakota prohibits employers from "failing or refusing to hire a person," discharging an employee, or according "unequal treatment to" an employee "with respect to . . . a term, privilege, or condition of employment . . ." because of "participation in lawful[217] activity off the employer's premises during nonworking hours[218] which is not in direct conflict with the essential business-related interests of the employer."[219] ("North Dakota Act").

216. *See, e.g.,* Reiseck v. Universal Commc'n of Miami, 06 Civ. 0777 (TPG), 2009 U.S. Dist. LEXIS 26013, at *11 (S.D.N.Y. Mar. 26, 2009) (deciding that an employer, located in New York City, did not terminate an employee who traveled to Florida on the weekends "because she spent her free time traveling as a leisure activity" but because the employer "believed that her job performance would be impacted by the long-distance commute.").

217. Hougum v. Valley Mem'l Homes, 574 N.W.2d 812, 822 (N.D. 1998) (holding that there was a factual question as to whether a plaintiff's conduct was lawful).

218. *See* Jose v. Norwest Bank N.D., N.A., 599 N.W.2d 293, 298 (N.D. 1999) (holding that participating in an internal employer investigation of another employee did not involve off-duty activity).

219. N.D. CENT. CODE § 14-02.4-03 (2008). The Supreme Court of North Dakota decided that, in a case where a chaplain for a memorial home was terminated for masturbating in a Sears restroom, there was a factual issue as to whether the plaintiff's conduct directly conflicted with the employer's business–related interests. *Hougum*, 574 N.W.2d at 822.

The broad ban would appear to reach much conduct that might be technologically monitored. [220] It extends to protecting an employee's right to work at another job unless the other job is directly in conflict with an essential interest of the employer.

An exception nevertheless permits an employer "to discharge" an employee if participating in the lawful activity "is contrary to a bona fide occupational qualification that reasonably and rationally relates to employment activities and the responsibilities of a particular employee or group of employees . . . ."[221] The exception suggests employers may terminate employees for a range of activity that is not contrary to the employer's essential business interest. And the Eight Circuit has interpreted the requirement that the qualification relate to a particular employee or group of employees, rather than all employees, to encompass any activity that would not be problematic if done by some other employee.[222]

Because the off-duty conduct prohibition is part of the larger anti-discrimination statute, an employee may elect either to file a claim with the North Dakota Department of Labor or to file a suit.[223] The employee may obtain injunctive and equitable relief, including two years of back pay. A court may grant the prevailing party attorney's fees. The Department is authorized to investigate complaints, conciliate, hold hearings, and educate the public and employers. The statute also contains an anti-retaliation provision.[224]

---

220. *See* Hong, *supra* note 187, at 470 (emphasizing that the conflict must be direct and must relate to an essential business interest not simply any business interest); Lichtenstein & Darrow, *supra* note 187, at 38 (noting blogging "could meet the statutory requisites of being carried out in a lawful manner off the employer's premises during non-working hours.").

221. N.D. CENT. CODE § 14-02.4-08 (2008). It also permits an employer to "fail or refuse to hire" on the same basis. *Id.* In *Hougum*, the court also held there was a factual issue as to whether the exception for a bona fide occupational qualification applied. 574 N.W.2d at 822. The court must have reasoned that unlike a claim where a financial impact is at stake, the particular facts of the business and the plaintiff's role as a chaplain would need to be considered to determine if a conflict existed or whether the exception applied. *See id.* Because it is part of the anti-discrimination statute there is also an exception for "a bona fide seniority or merit system, or a system which measures earnings by quantity or quality of production." N.D. CENT. CODE § 14-02.4-09 (2008).

222. Fatland v. Quaker Corp., 62 F.3d 1070, 1073 (8th Cir. 1995). Indeed the Eighth Circuit interpreted the exception to encompass an employee's violation of a conflict of interest policy when he used his position that required interacting with clients to obtain information from the client that he then used in his business that was in competition with the client's business. *Id.* The court reasoned that while the conflict-of-interest policy would apply to the janitor, engaging in an analogous business would not be a conflict for the janitor because the janitor's position would not require interaction with clients. *Id.*

223. N.D. CENT. CODE § 14-02.4-19(2) (2008).

224. N.D. CENT. CODE § 14-02.4-18 (2008).

Like the New York Act, the North Dakota Act may provide employees some protection from technological monitoring. Because it permits employees to elect whether to file claims with the Department or in court, it likely provides employees who desire an efficient or cooperative outcome a good process while also ensuring that employers comply due to the threat of lawsuits.

Yet, also like the New York Act, the North Dakota Act is not designed to adequately safeguard employees' privacy. [225] As one commentator has noted, the requirement that the off-duty conduct be lawful does not appear to relate to the impact the conduct may have on the employer's business.[226] The Proposed Act does not distinguish between monitoring lawful and unlawful off-duty conduct but rather requires that the conduct will cause a significant harm to the employer. Additionally, the North Dakota Act's use of the bona fide occupational qualification exception creates confusion as to what off-duty behavior employers may base disciplinary decisions on.[227]

c. Colorado's "Legal Activities" Statute

The Colorado statute, enacted in 1990, prohibits employers from terminating an employee for "engaging in any lawful activity off the premises of the employer during nonworking hours . . ."[228] ("Colorado Act").

There are three exceptions. First, an employer can terminate an employee if the employee violates a "bona fide occupational requirement."[229] It is unclear what is meant by "bona fide occupational requirement."[230] Could an employer prohibit employees from blogging about work, or sending an e-mail about work to a friend? In one case, a federal district court indicated that a bona fide occupational requirement

225. See *supra* discussion in Section III.C.3.a.

226. Jason Bosch, Note, *None of Your Business (Interest): The Argument for Protecting All Employee Behavior with No Business Impact*, 76 S. CAL. L. REV. 639, 657 (2003).

227. Terry Morehead Dworkin, *It's My Life – Leave Me Alone: Off the Job Employee Associational Privacy Rights*, 35 AM. BUS. L.J. 47, 82-83 (1997) (discussing how the use of the term "bona fide occupational qualification" to substitute for "business necessity" rather than to mean the extremely difficult standard to meet that it connotes in the Title VII context creates great "possibilities for confusion.").

228. COLO. REV. STAT. § 24-34-402.5(1) (2007).

229. § 24-34-402.5(1)(a).

230. Dworkin, *supra* note 227, at 82-83; Gwin v. Chesrown Chevrolet, Inc., 931 P.2d 466, 471 (Colo. App. 1996) (holding that the exception did not apply when an employee demanded a refund from a motivational speaker that the employer had encouraged, but not required, employees to attend).

includes a duty of loyalty to the company when engaging in public communications.[231] But the Colorado court of appeals stated that no Colorado court has approved the holding that a duty of loyalty is a bona fide occupational requirement.[232]

Second, an employer can terminate an employee if "the employee violates a restriction reasonably and rationally related to the employment activities and responsibilities of a particular employee or a particular group of employees . . ."[233] The federal court also indicated that the exception relating to a particular employee or group of employees was probably intended to apply to "certain high profile members" of an employer's staff and that to expand the exception "to include all members of the workforce" would mean that the exception would "swallow the general rule."[234]

Third, an employer can terminate an employee to avoid the appearance of or a conflict of interest "with any responsibilities of the employer."[235] The exception appears very broad; an employer could probably bar an employee from doing contract work or volunteering at certain organizations. Yet, the federal district court interpreted it narrowly to involve only situations where fiduciaries stand to obtain a private gain or to disregard their duty to the employer because of private interest or another duty.[236]

An aggrieved employee may sue in court for damages and for lost wages and benefits.[237] If successful, the employee is entitled to court costs and reasonable attorney's fees from the employer.[238]

Notably a statute of limitations is not specified, which led to litigation over the appropriate statute of limitations.[239]

---

231. Marsh v. Delta Air Lines, Inc., 952 F. Supp. 1458, 1463 (D. Colo. 1997). The employer terminated the employee for writing a letter critical of the employer to the newspaper. *Id.* at 1460. The court reasoned that the plaintiff's letter was simply a "disgruntled worker venting his frustrations" without using the proper internal channels. *Id.* at 1463; *see* Elizabeth R. Rita & Eric D. Gunning, *Navigating the Blogosphere in the Workplace*, 35-MAY COLO. LAW 55, 57-58 (2006) (concluding the statute probably protects blogging, but employees may violate the duty of loyalty by blogging about work).

232. Watson v. Public Serv. Co. of Colo., 207 P.3d 860, 865 (Colo. App. 2008).

233. COLO. REV. STAT. § 24-34-402.5(1)(a) (2007).

234. *Marsh*, 953 F. Supp. at 1463-64.

235. § 24-34-402.5(1)(b).

236. *Marsh*, 953 F. Supp. at 1464.

237. § 24-34-402.5(2)(a). *But see Watson*, 207 P.3d at 865 (interpreting the Colorado Act to provide for back pay as the sole remedy).

238. § 24-34-402.5(2)(b)(I).

239. Galieti v. State Farm Mut. Auto. Ins. Co., 840 F. Supp. 104, 105-06 (D. Colo. 1993) (applying six-month statute of limitations); Galvan v. Spanish Peaks Reg'l Health Ctr., 98 P.3d 949, 951 (Colo. App. 2004) (declining to follow *Galieti* and apply a six-month statute of limitations);

Of the three states' off-duty activity statutes, the Colorado Act has arguably been interpreted by the courts in a manner that is most protective of employees. Although it likely provides some protection from monitoring of off-duty behavior, it suffers from the same difficulties as the North Dakota Act. Additionally, it is limited to a prohibition on termination so employers may be more likely to monitor employees for the purpose of implementing discipline less than termination.

D. International Law

Legislation and other procedures that have been enacted by other countries that protect employees from employer technological monitoring are also helpful to consider as starting points for legislation. Many regions and countries have laws governing how employers may monitor their employees. And several articles have investigated one or another of these systems.[240]

This section focuses on the laws of the European Union as a useful source.[241] While the history of both workplace rights and protection of employees' autonomy are different in Europe than in the United States, both the United States and the member states of Europe are developed Western countries[242] and the United States Department of Commerce has adopted principles to comply with European privacy principles.[243] Moreover, recently, a group of large multi-national companies has called for the United States to enact a comprehensive privacy protection law to "harmonize" the United States' approach with that of the European Union.[244]

Keynen J. Wall & Jacqueline Johnson, *Colorado's Lawful Activities Statute: Balancing Employee Privacy and the Rights of Employers*, 35-DEC COLO. LAW. 41, 44 (2006) (stating that a two-year statute of limitations applies).

240. See *infra* note 374.

241. It is beyond the scope of this article to investigate all the possible foreign models. Such an investigation would likely be voluminous enough for a book.

242. *Cf.* Yohei Suda, *Monitoring E-mail of Employees in the Private Sector: A Comparison Between Western Europe and the United States*, 4 WASH. U. GLOBAL STUD. L. REV. 209, 213, 261 (2005) (concluding that "the level of employee privacy protection [from e-mail monitoring] is similarly low in both Western Europe and the United States" but predicting that Western Europe will likely "increasingly limit e-mail monitoring").

243. Evans, *supra* note 18, at 1142 (noting that England shares a legal heritage with the United States and has changed toward a European approach in privacy law and that "the very existence of the EU and English law favoring protection of employee privacy is putting pressure on the United States to adopt similar law.").

244. Schwartz, *supra* note 25, at 904.

The governing legislative bodies of the European Union, The European Parliament and the Council of the European Union, adopted a Directive, designed to respect the fundamental right of privacy when processing personal data, in 1995.[245] The Directive was based on the longstanding European understanding set out previously by the European Convention for the Protection of Human Rights and Fundamental Freedoms that "[e]veryone has the right to respect for his private and family life, his home and correspondence"[246] and by the extension to respect of "communications" in the Charter of Fundamental Rights of the European Union.[247] The use of the word "communications" in place of "correspondence" was to modernize the principle to keep pace with advancing technology and the reality that many now communicate online.[248]

The Directive's Article 29 established an independent Working Party on The Protection of Individuals with Regard to the Processing of Personal Data (Working Party) to serve an advisory role, including drafting documents to deal with particular privacy situations.[249] Several have been issued that deal with workplace privacy and employer technological monitoring.[250] Additionally, the Directive mandated the member countries to establish national privacy agencies.[251]

This section first discusses the Working Party documents, then the rules governing establishment of national privacy agencies. Finally, it discusses the framework adopted by the United States Commerce Department to permit United States companies to continue to process European personal data.

245. Council Directive 95/46, 1995 O.J. (L 281) (EC), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. & http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf. [hereinafter *Directive*]; *see also* Council Directive 2002/58, 2002 O.J. (L 201/37) (EC); Council Directive 2006/24, 2006 O.J. (L 105/54) (EC) (amending Council Directive 2002/58, 2006 O.J. (L 105/54) (EC).

246. ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON THE SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE 7 (2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf.

247. *Id.* at 10.

248. *Id.*

249. *Directive*, *supra* note 245, article 29.

250. *See* discussion *infra* Section III.D.1

251. *See* discussion *infra* Section III.D.2.

1. The Working Party Documents

The Working Party functions as an advisory group. It fosters uniformity in the implementation of the Directive across member countries.[252] Four of the Working Party documents are particularly helpful to examine as potential models for an act protecting privacy from employer technological monitoring.[253] These address "the processing of personal data in the employment context," workplace surveillance of electronic communications, video surveillance, and employee location data.[254]

a. General Principles Governing Processing of Personal Data

One Opinion of the Article 29 Working Party addresses the "processing of personal data in the employment context."[255] The opinions are numbered, and this one is designated Opinion 8/2001. Opinion 8/2001 deals with "the processing of personal information in the employment context."[256] Opinion 8/2001 interprets the Directive as it applies to the employment setting.[257]

These "data protection requirements apply to the monitoring" of employees, including e-mail use, Internet use, "video cameras or location data."[258]

Opinion 8/2001 outlines seven "fundamental data protection principles" that employers must comply with whenever monitoring employee's personal data.[259] These principles are somewhat similar to the safeguards that arbitrators in the United States use to protect employees' workplace privacy.[260] The principles are: 1) finality; 2)

252. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 8/2001 ON THE PROCESSING OF PERSONAL DATA IN THE EMPLOYMENT CONTEXT 2 n.1 (2001), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp48en.pdf.

253. *See also* ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON BIOMETRICS (2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp80_en.pdf; *see generally* ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION ON THE PROPOSALS AMENDING DIRECTIVE 2002/58/EC ON PRIVACY AND ELECTRONIC COMMUNICATIONS (E-PRIVACY DIRECTIVE) (2009), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp159_en.pdf.

254. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 2.

255. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 2.

256. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 2.

257. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 2.

258. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 24.

259. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 3; *see also Directive, supra* note 245, art. 6, 7, 17.

260. *See supra* Section III.A for a discussion of the safeguards.

transparency; 3) legitimacy; 4) proportionality; 5) accuracy and retention of data; 6) security; and 7) awareness of the staff.[261]

Finality requires that an employer collect data "for a specified, explicit and legitimate purpose" and use the data only in a manner compatible with that purpose.[262] It is similar to the legitimate business interest requirement for monitoring on-duty communications and computer use imposed by the Proposed Act but requires additional restrictions on use.

Transparency is a minimum requirement. Employers should provide notice of the data they are collecting and the purposes of the collection.[263] Employers should also provide the employee access to the collected data. Additionally, employers should notify the appropriate national authority of the collection of the data.[264] Transparency encompasses concepts similar to the notice safeguards and the safeguard of reliability and accuracy of records in the Proposed Act.

Legitimacy requires that the data processing be "'necessary for' the achievement of the objective in question."[265] Examples include data processing "necessary for the performance" of the employment contract; data processing "necessary for compliance with a legal obligation" such as reporting to the tax authorities; or data processing necessary "for the purposes of the legitimate interest pursued by the" employer unless the interest is outweighed "by the interests for fundamental rights" of the employee.[266] The latter is a balancing test that balances the employer's interests versus the employee's interests, and the employee "retains the right to object to the processing" when the employee has "compelling grounds" to do so.[267] The Legitimacy of processing certain types of data is even more limited.[268] These types of data reveal "racial or ethnic origin, political opinions, religious or philosophical beliefs, [or] trade union membership" or concern "health or sex life . . . offences, criminal

261. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 3; *see* Herbert, *supra* note 25, at 403 (discussing these principles).

262. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 3; *see also Directive, supra* note 245, art. 6.

263. *See Directive*, *supra* note 245, art. 10.

264. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 3.

265. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 15.

266. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 15; *see also Directive*, *supra* note 245, art. 7.

267. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 15; *see also Directive*, *supra* note 245, art. 14.

268. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 16-17; *see also Directive*, *supra* note 245, art. 8.

convictions or security measures."[269] Alternatively, the employer can obtain an employee's "unambiguous consent" to the data processing.[270] Consent is valid only where an employee may "withdraw consent without prejudice."[271] If the loss of a job opportunity results from refusing or withdrawing consent, the consent is not valid.[272] Thus, the Working Party advises employers not to rely on consent.[273] While the Proposed Act does not contain an analogous safeguard, the premise underlying the Proposed Act is that it appropriately balances employees' right to privacy and employers' legitimate interests in technological monitoring. Additionally, in some instances, under the Proposed Act, employers must use the safeguard of exhaustion, which requires exhaustion of other methods of verification or discovery before resorting to monitoring.

Proportionality requires that the data be "adequate, relevant and not excessive in relation to the purposes for which they are collected."[274] It further requires that the data processing "be fair" to the employee and processed "in the least intrusive way."[275] While there is no analogous safeguard in the Proposed Act, the framework of the Act which requires more safeguards the more invasive the type of intrusion is intended to limit excessive monitoring. Additionally, in some instances, under the Proposed Act, employers may use the safeguard of limited monitoring, which requires monitoring to be no more extensive than necessary.

Accuracy and Retention of the Data requires that employers keep accurate records, erasing and rectifying information that is incorrect.[276] The Proposed Act's safeguards for accuracy and reliability of information are designed to ensure correctness of maintained information.

Security requires employers to maintain the information collected in a secure manner by taking appropriate technological and personnel

269. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 16.

270. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 16. Consent for processing of the data that are more highly protected must be "explicit." ARTICLE 29 OPINION 8/2001, *supra* note 252, at 23.

271. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 23.

272. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 23.

273. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 23.

274. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 3, 21; *see also, Directive, supra* note 245, art. 6.

275. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 21.

276. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 21; *see also Directive*, *supra* note 245, art. 6.

measures.[277] The Proposed Act contains a mandate for employers to maintain information in a secure manner.

Awareness of the staff requires employers to properly train those responsible for "processing of personal data."[278] The summary asserts that "[w]ithout an adequate training of the staff handling personal data, there could never be appropriate respect for the privacy of workers in the workplace."[279] The Proposed Act does not mandate training though many employers would likely train their employees to foster compliance with the Proposed Act.

Employees have the right to damages for "any act incompatible with data protection legislation."[280]

b. Rules Governing Workplace Surveillance of Electronic Communications

Supplementing Opinion 8/2001 is a May 2002 Working Document on the Surveillance of Electronic Communications in the Workplace.[281] The Document outlines the minimum requirements employers must include in their policies governing e-mail and Internet use. Further elaboration by employers in their policies "taking into account the peculiarities of a given company" are appropriate.[282]

The Document begins with the precept that private life "is not limited to life within home" and "does not exclude" an employee's professional life.[283] The Document interprets the European Convention for the Protection of Human Rights and Fundamental Freedoms and decisions[284] under it by the European Court of Human Rights to establish

277. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 22; *see also Directive*, *supra* note 245, art. 14.

278. ARTICLE 29 OPINION 8/2001, *supra* note 252, at 22.

279. *Id.*

280. *Id.* at 24; *see also Directive*, *supra* note 245, art. 22, 23 (member countries must provide judicial remedy, including compensation).

281. ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON THE SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE (2002), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf; *see* Herbert, *supra* note 25 at 401-02 (discussing the working document).

282. SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE , *supra* note 281, at 4.

283. SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE, *supra* note 281, at 6.

284. *See generally* Niemietz v. Germany, App. No. 13710/88, 16 Eur. H.R. Rep 97 (1992), *available at* http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=13710/88&sessionid=27644349&skin=hudoc-en (holding that an attorney had a right of privacy in his

three sub-principles. First, employees "have a legitimate expectation of privacy at the workplace" that is not outweighed by use of an employer's "communication devices" or "other business facilities."[285] The expectation may be reduced but not eliminated by providing notice of monitoring.[286] Second, private correspondence include "communications at the workplace," including e-mail. Third, an employer's "legitimate need for surveillance measures" is limited by employees' right "to establish and develop relationships with other human beings," including in the workplace.[287]

The Document then interprets the Directive as applied to monitoring of e-mail and Internet use. It requires compliance with each of the seven principles described in Opinion 8/2001.[288]

The Document further elaborates on the meaning of transparency. No covert e-mail monitoring is permitted except in limited circumstances, such as to investigate a criminal act or where "national laws" permit employers to monitor employees to detect workplace infractions and provide "necessary safeguards."[289]

The Document divides transparency into two aspects. The first is the obligation to provide employees "with a readily accessible, clear and accurate" statement of the policy on monitoring e-mail and Internet use.[290] The policy should: 1) describe in detail the extent to which personal use of company technology is permitted; 2) provide the "reasons and purposes for which surveillance . . . is being carried out"; 3) state the "details of the surveillance measures," including who and what will monitor, how the monitoring will work, and when the monitoring will take place; and 4) provide "[d]etails of any enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any such claims against them."[291] As to enforcement, the Working Party recommends immediately notifying an employee "when misuse of

business which was searched by police); Halford v. United Kingdom, 24 Eur. Ct. H.R. 523, 551 (1997) (holding that intercepting an employee's phone calls violated the convention).

285. SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE, *supra* note 281, at 9.

286. *Id.* at 17-18.

287. *Id.* at 8-9.

288. *See supra* notes 259-261 and accompanying text.

289. SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE, *supra* note 281, at 14.

290. *Id.*

291. *Id.* at 15.

electronic communications" is detected.[292] They suggest using "software such as warning windows, which pop up and alert" the employee "that the system has detected an unauthorized use of the network."[293] The Working Party also mentions Directive 2002/14/EC that requires "information and consultation of employees on decisions likely to lead to substantial changes in work organization or in contractual relations" and its applicability to monitoring electronic communications.[294]

While this framework provides for somewhat more extensive notice, particularly of enforcement procedures, than the Proposed Act, the Proposed Act similarly makes extensive use of the safeguard of notice, requires notice in most circumstances, and limits monitoring without notice to situations where the employer provides other adequate safeguards. The Proposed Act also incorporates employee participation, although not to the extent of the Directive.

The second aspect of transparency provides employees a right of access to information collected by electronic monitoring. The Document quotes the Directive:

> [E]very data subject is entitled to obtain from the controller (the employer in this case):
>
> a) without constraint at reasonable intervals and without excessive delay or expense:
>
> Confirmation as to whether or not data relating to the worker are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipient or categories of recipients to whom the data are disclosed,
>
> Communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,
>
> Knowledge of the logic involved in any automatic processing of data concerning him at least in the case of automated decisions;
>
> b) as appropriate the rectification, erasure or blocking of data the provision of which does not comply with data protection law, in particular because of the incomplete or inaccurate nature of the data;
>
> c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in

292. *Id.*
293. *Id.*
294. *Id.*

> compliance with the previous obligations, unless this proves impossible or involves a disproportionate effort.[295]

The Proposed Act also grants a right of review and to contest information.[296] The right of review in the Proposed Act applies to certain categories of information, rather than all information collected. The rationale is that this permits the employee to review the information the employee is most likely to be interested in, including that upon which decisions about individual terms and conditions are made, but reduces the administrative expense from that incurred to provide review of all collected information.

The Document also provides specific guidance on proportionality as applied to e-mail and Internet use. "Blanket monitoring of individual e-mails and Internet use of all staff" is prohibited "other than where necessary for the purpose of ensuring the security of the system."[297] The Document suggests monitoring only "traffic data on the participants and time of a communication rather than the contents."[298] The Document further suggests that if necessary to monitor content, the employer should include a warning that content is monitored on all outgoing messages. As to Internet use, the Document recommends using "blocking, as opposed to monitoring, mechanisms."[299] The Proposed Act is not as inflexible in its requirements although it does guarantee that in most instances blanket monitoring will not occur and that in other instances other appropriate safeguards will protect employees' privacy.

As to security, the Document states, "It is of great importance that the system administrator and anyone else who has access to personal data about workers in the course of monitoring, is placed under a strict duty of professional secrecy with regard to confidential information, to which they have access."[300] This requirement is similar to the Proposed Act's safeguard of confidentiality, which some employers may elect to use.

The Document specifically enumerates another three mandatory principles: 1) necessity; 2) notifying the supervisory authority before carrying out automatic surveillance; and 3) providing employees access

---

295. *Directive*, *supra* note 245, art. 12.
296. *Directive*, *supra* note 245, art. 12.
297. SURVEILLANCE OF ELECTRONIC COMMUNICATIONS IN THE WORKPLACE, *supra* note 281, at 17.
298. *Id.*
299. *Id.* at 18.
300. *Id.* at 19.

to the fruit of the surveillance.[301] The latter two requirements were required by the Opinion 8/2001 but were not explicitly enumerated.

Necessity "means that the employer must check if any form of monitoring is absolutely necessary for a specified purpose before proceeding to engage in any such activity."[302] The Working Document states, "Traditional methods of supervision, less intrusive for the privacy of individuals, should be carefully considered and, where appropriate, implemented before engaging in any monitoring of electronic communications."[303] The requirement of necessity permits monitoring an employee's e-mail or Internet use only in "exceptional circumstances," such as to verify criminal activity or actions for which the employer is liable or "to guarantee the security of the system."[304] Necessity also requires that an employer maintain the collected data no longer than necessary.[305] While this requirement is similar to the exhaustion safeguard in the Proposed Act, the Proposed Act does not limit the circumstances in which an employer may monitor to such a great degree.

The Document also makes several other suggestions. The Document suggests that employers provide employees "with two e-mail accounts," one for work use and one for personal use.[306] The account for work use could be monitored by meeting the requirements of the Document. The account for personal use could "only be subject to security measures and would be checked for abuse in exceptional cases."[307] While the suggestion of permitting a personal account for personal messages is appealing, there are several difficulties with it. First, from the employee's perspective, someone may send a personal message to the employee on the work account. Additionally, the employee may send a message containing both work and personal information or may inadvertently send a personal message on the work account. Second, from the employer's perspective, there is no reason that an employee could not engage in a host of problematic uses of the personal e-mail account for which the employer would desire to monitor, such as competitive activity, revelation of trade secrets, harassing or defamatory statements.

---

301. *Id.* at 13-16.
302. *Id.* at 13.
303. *Id.*
304. *Id.* at 13-14.
305. *Id.* at 14.
306. *Id.* at 5. Alternatively, the employer could provide employees access to webmail. *Id*.
307. *Id.*

The Document also suggests that technology should be used to prevent Internet misuse and that "a blanket ban on personal use of the Internet by employees does not appear to be reasonable."[308] The Document reiterates three principles. First, "prevention should be more important than detection."[309] Second, only when less invasive checks such as of time spent on the Internet or of "sites most frequently visited by a department" disclose potential misuse of the Internet should additional monitoring be implemented.[310] Third, employers should "exercise caution" before determining an employee has engaged in misuse because unintended visits to webpages happen for a variety of reasons.[311] The Proposed Act prohibits a ban on personal use of the employer's communications technology. This advice is all solid in light of that prohibition although the Proposed Act provides considerable flexibility to employers to decide whether or not to follow these suggestions.

c. Rules Governing Video Surveillance

In 2004, the Working Party issued an opinion addressing "processing of personal data by means of Video Surveillance."[312] It contains a section on video surveillance "in the employment context."[313] It generally prohibits "video surveillance systems aimed directly at controlling, from a remote location, quality and amount of working activities . . . ."[314] Video may, however, be used, "subject to appropriate safeguards, to meet production and/or occupational safety requirements . . . ."[315] It further prohibits video surveillance in areas "reserved for employees' private use or . . . not intended for the discharge of employment tasks—such as toilets, shower rooms, lockers and recreation areas."[316]

There are also restrictions on discipline and requirements for access and reliability of the data. It prohibits using video images obtained "to safeguard property" or "detect or prevent serious offenses" to "charge an

308. *Id.* at 4.
309. *Id.* at 24.
310. *Id.*
311. *Id.*
312. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 4/2004 ON THE PROCESSING OF PERSONAL DATA BY MEANS OF VIDEO SURVEILLANCE 1 (2004), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2004/wp89_en.pdf.
313. *Id.* at 24.
314. *Id.*
315. *Id.*
316. *Id.*

employee with minor disciplinary breaches."[317] It requires that employees can use the images "to lodge their counterclaims."[318]

While more restrictive than the Proposed Act, the rules governing video surveillance of on-the-job activity do contain some similarities. Notice is a key safeguard before monitoring.[319] Additionally, the requirement of access and reliability of the data are similar to those required by the Proposed Act. The Proposed Act does not restrict employers from technologically monitoring work activity to determine its quality or quantity. Thus, to the extent that silent video is encompassed in the Working Party opinion, it is more restrictive than the Proposed Act. Like the Proposed Act, video is prohibited in certain areas reserved for private use, but the Proposed Act does not extend the protection to recreation areas that are not typically used to change where employees bodily integrity is not an issue.

d. Rules Governing the Use of Employee Location Data

The Working Party promulgated an opinion on the use of location data with a view to providing value-added services in November 2005.[320] The Opinion is not limited to the employment context but contains a section on "location of employees."[321] The Opinion reiterates the applicability of Opinion 8/2001. As noted by William Herbert, the Working Party was particularly concerned with two issues: "the degree of monitoring . . . that is acceptable" and "the illusive line between work and private life.[322]

The Opinion states that "the processing of location data on employees must correspond to a specific need on the part of the company which is connected to its activity."[323] The Opinion provides the following examples of permissive monitoring: monitoring an employee who transports people or goods; monitoring with the goal of improving "distribution of resources for services in scattered locations"; and monitoring to maintain the security of the employee or property the employee is responsible for. The Opinion provides the following

317. ARTICLE 29, OPINION 4/2004, *supra* note 312, at 25.

318. *Id.*

319. *Id.*

320. ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 11/2005 ON THE USE OF LOCATION DATA WITH A VIEW TO PROVIDING VALUE-ADDED SERVICES 1 (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf.

321. ARTICLE 29, OPINION 11/2005, *supra* note 320, at 9.

322. Herbert, *supra* note 25, at 408.

323. ARTICLE 29, OPINION 11/2005 , *supra* note 320, at 10.

examples of excessive monitoring: monitoring when "employees are free to organize their travel arrangements as they wish," and monitoring "an employee's work where [it] can be monitored by other means."[324]

The Opinion prohibits employers from monitoring an employee's location "outside" the employee's "working hours."[325] The Opinion recommends "that equipment made available to employees, especially vehicles that can also be used for private purposes, be equipped with a system allowing employees to switch off the location function."[326]

The Proposed Act uses a similar framework that permits more extensive monitoring of employees activity via GPS when on-duty than when off-duty. However, as to monitoring on-duty conduct via GPS, the Proposed Act provides employers more leeway to monitor provided appropriate safeguards, such as notice, are in place. As to off-duty behavior, some monitoring is permitted in certain specified circumstances.

2. Rules governing establishment of national privacy agencies

Under the Directive, each member state must establish "an independent governmental entity, known as a supervisory authority, to ensure compliance with the national legislation enacted consistent with the Privacy Directive."[327] The supervisory authorities are similar to federal and state administrative agencies.[328] The supervising authority must be "consulted when drawing up administrative measures or regulations relating to the protection of individuals' rights and freedoms with regard to the processing of personal data."[329] Additionally, they have the following powers: 1) "investigative powers"; 2) the power to intervene, such as to block, erase, or destruct data, to impose "a temporary or definitive ban on processing," or to refer the matter to higher authorities;[330] 3) the power to "hear claims" of violations of the Directive;[331] and 4) the power to "engage in legal proceedings" or to bring violations "to the attention of the judicial authorities."[332] Those aggrieved by the supervising authorities' decisions may appeal to the

324. *Id.*
325. *Id.*
326. *Id.*
327. Herbert, *supra* note 25, at 390; *Directive*, *supra* note 245, art. 28.
328. Herbert, *supra* note 25, at 390.
329. *Directive*, *supra* note 245, art. 28.
330. *Id.*
331. *Id.*
332. *Id.*

courts.[333] The supervising authority must regularly issue public reports concerning its activities.[334] The "members and staff of the supervisory authority" are subject to "a duty of professional secrecy."[335]

The establishment of a federal agency and related state agencies devoted to privacy issues related to new technologies may be ideal.[336] But because establishment of such an agency is unlikely to pass as part of employment legislation and because, in the United States, privacy issues addressed in other areas are often neglected in the employment sphere, the Proposed Act places responsibility for enforcement of the Proposed Act with the DOL. The DOL is, however, bestowed with broad adjudicatory, educational, advisory, and compliance guidance responsibilities.

3. The U.S. Department of Commerce Safe Harbor Procedure

Because the United States does not provide an adequate level of protection for personal data to satisfy the requirements of the Directive, the European Commission negotiated a solution with the United States.[337] An agreement was reached in 2000.[338]

---

333. *Id.*

334. *Id.*

335. *Id.*

336. *See generally* Schwartz, *supra* note 25.

337. Herbert, *supra* note 25, at 391; ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 1/99 CONCERNING THE LEVEL OF DATA PROTECTION IN THE UNITED STATES AND THE ONGOING DISCUSSIONS BETWEEN THE EUROPEAN COMMISSION AND THE UNITED STATES GOVERNMENT, 2 (1999) *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp15en.pdf. There are other means available for entities in the United States to ensure that data imported from Europe is in compliance with the Directive. Schwartz, *supra* note 25, at 926. One means is for multi-national companies or groups of affiliated entities to enter into Binding Corporate Rules. Binding Corporate Rules are corporate codes that must integrate the principles of the Directive. While they must contain provisions that it would be useful to consider relating to disclosure of personal information, such as requiring a designated privacy officer, training of employees dealing with personal data, and sanctions, such as discipline, for employees violating the principles of the Directive, their focus is on enabling global transfer of information, an issue beyond the scope of this paper. *See* ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON FREQUENTLY ASKED QUESTIONS (FAQS) RELATED TO BINDING CORPORATE RULES (2008) *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp155_rev.04_en.pdf; ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT SETTING UP A TABLE WITH THE ELEMENTS AND PRINCIPLES TO BE FOUND IN BINDING CORPORATE RULES (2008), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp153_en.pdf; ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT SETTING UP A FRAMEWORK FOR THE STRUCTURE OF BINDING CORPORATE RULES (2008), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_en.pdf; ARTICLE 29 DATA PROTECTION WORKING PARTY, RECOMMENDATION 1/2007 ON THE STANDARD APPLICATION FOR APPROVAL OF BINDING CORPORATE RULES FOR THE TRANSFER OF PERSONAL DATA (2007),

As a result of the agreement, the U.S. Commerce Department provides a "safe harbor framework."[339] An employer can certify that it complies with the "safe harbor framework" to assure European Union organizations that the employer provides adequate privacy protection.[340] The Commerce Department maintains a "regularly updated" list of companies "that have self-certified to the safe harbor framework" on a publicly available webpage.[341]

To avail itself of the safe harbor framework, an employer must adopt a "published privacy policy statement" that states its adherence to

---

available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2007_en.htm; ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ESTABLISHING A MODEL CHECKLIST APPLICATION FOR APPROVAL OF BINDING CORPORATE RULES (2005), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp108_en.pdf; ARTICLE 29 DATA PROTECTION WORKING PARTY, WORKING DOCUMENT ON TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES: APPLYING ARTICLE 26(2) OF THE EU DATA PROTECTION DIRECTIVE TO BINDING CORPORATE RULES FOR INTERNATIONAL DATA TRANSFERS (2003), *available at* http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf; *See also* Miriam Wugmeister, Karin Retzer & Cynthia Rich, Morrison & Foerster LLP, *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 GEO. J. INT'L L. 449 (2007). Another means is to enter into a standard contractual clause with the European entity exporting the data to the United States. This framework is not discussed here because the contractual obligation is not involved in establishing a legislative framework that applies directly to United States companies; in other words, there is no contract between entities involved. *See* Commission Decision 2001/497/EC, 2001 O.J. (L 181) 19 (on standard contractual clauses for the transfer of personal data to third countries); Commission Decision 2002/16/EC, 2002 O.J. (C) (on standard contractual clauses for the transfer of personal data to processors established in third countries); Commission Decision 2004/915/EC, 2004 O.J. (L 385/74) (EC) (as of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries); Commission Staff Working Document SEC(2006) 95 on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC); ARTICLE 29 DATA PROTECTION WORKING PARTY, OPINION 3/2009 ON THE DRAFT COMMISSION DECISION ON STANDARD CONTRACTUAL CLAUSES FOR THE TRANSFER OF PERSONAL DATA TO PROCESSORS ESTABLISHED IN THIRD COUNTRIES, UNDER DIRECTIVE 95/46/EC (data controller to data processor) (2009).

338. ARTICLE 29, OPINION 1/99, *supra* note 337, at 2; Commission Decision 2000/520/EC, 2000 O.J. (L 215/7) pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce [hereinafter *Commission Decision*]; Letter from John Mogg, Director European Commission, to Robert LaRussa, Under Secretary for International Trade of the United States Department of Commerce, (July 17, 2000) (*available at* http://www.export.gov/safeharbor/eu/eg_main_018486.asp); Letter from Robert Pitofsky, of the FTC, to John F. Mogg, Director European Commission (July 27, 2000) *available at* http://www.export.gov/static/FTCLETTERFINAL_Latest_eg_main_018266.pdf.

339. Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited June 10, 2009).

340. Safe Harbor Overview, *supra* note 339.

341. *Id.*

the safe harbor requirements.[342] The employer must also "self certify annually to the Department of Commerce in writing that it agrees to adhere to the safe harbor's requirements."[343] To ensure self-regulation, the employer can join a self-regulatory privacy program that adheres to the safe harbor's requirements; or (2) develop its own self-regulatory privacy policy that conforms to the safe harbor.[344]

The employers must comply with "seven safe harbor principles:" 1) notice, 2) choice, 3) transfer to third parties, 4) access, 5) security, 6) data integrity, and 7) enforcement.

First, notice requires that an employer notify employees "about the purposes for which" the employer collects and uses information, how to make an internal inquiry or complaint, "the types of third parties to which it discloses the information," and the means for limiting use and disclosure.[345]

Second, choice requires that employees be provided an opportunity to opt out of disclosure of personal information to third parties and of use "for a purpose incompatible with the purpose for which it was originally collected." Choice also generally requires that employees opt in to disclosure of sensitive information.[346] There is an exception, however, when processing is "necessary to carry out the organization's obligations in the field of employment law."[347]

Third, transfers to third parties, or onward transfer, requires that when disclosing information to agents, without notice and choice, the agents "subscribe to the safe harbor principles," are "subject to the Directive or other adequacy finding," or enter into a written agreement to "provide at least the same level of privacy protection as required by the relevant principles."[348]

Fourth, access requires an employee have access to information collected "and be able to correct, amend, or delete that information where it is inaccurate" unless the burden "of providing access would be disproportionate to the risks to the individual's privacy" or "the rights of persons other than the individual would be violated."[349]

---

342. *Id.*
343. *Id.*
344. *Id.*
345. *Id.*
346. *See supra* note 269 and accompanying text.
347. Export.gov, FAQ – Sensitive Data, http://www.export.gov/safeharbor/eu/eg_main_018375.asp (last visited June 10, 2009). There are also five other exceptions. *Id.*
348. Safe Harbor Overview, *supra* note 339.
349. *Id.*

Fifth, security requires that the employer "take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction."[350]

Sixth, data integrity requires that information must be "relevant for the purposes for which it is to be used," accurate, complete, current, and "reliable for its intended use."[351]

Finally enforcement consists of three requirements. There must be an affordable, independent, and "readily available" mechanism to resolve disputes and, "where the applicable law or private sector initiatives so provide," award damages.[352] There must be "procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented."[353] And, the employer must be obligated to "remedy problems arising out of a failure to comply with the principles."[354] "Sanctions must be sufficiently rigorous to ensure compliance. . . ."[355] "[T]hey must include publicity for findings of non-compliance and deletion of data in certain circumstances."[356]

For human resources data, a Data Protection Panel (DPP), "composed of representatives of various EU data protection authorities," serves as the dispute resolution mechanism.[357] For other types of data, a company may choose the DPP as the mechanism or may choose a private dispute resolution mechanism.[358]

The Federal Trade Commission (FTC) can seek "civil penalties of up to $12,000 per day for violations" by self-certified companies subject to its jurisdiction.[359] The FTC has jurisdiction under Section 5 of the

350. *Id.*
351. *Id.*
352. *Id.*
353. *Id.*
354. *Id.*
355. *Id.*
356. *Id.*
357. Data Protection Panel (related to FAQ's 5 and 9 issued by the US Department of Commerce, and annexed to Commission Decision 2000/520/EC on the adequacy of the "safe harbor" privacy principles) July 25, 2005, http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/information_safe_harbour_en.pdf; Export.gov, Helpful Hints Prior to Self-Certifying to the Safe Harbor, http://www.export.gov/safeharbor/eg_main_018245.asp (last visited June 10, 2009); *see also* Jorg Rehder & Erika C. Collins, *The Legal Transfer of Employment-Related Data to Outside the European Union: Is It Even Still Possible*, 39 INT' L LAW 129, 148 (2005).
358. Helpful Hints, *supra* note 357.
359. Safe Harbor Overview, *supra* note 339. The FTC does not have jurisdiction over "banks, saving and loans and credit unions; telecommunications and interstate transportation common carriers, air carriers and packers and stockyard operators, and some of the business of the insurance industry." *Commission Decision*, *supra* note 338, Annex VII, at *47. The Department of

Federal Trade Commission Act over "unfair or deceptive acts or practices in or affecting commerce."[360] The FTC's position is that "a company's failure to abide by a stated privacy policy is likely to be a deceptive practice."[361] The FTC, however, does not "resolve individual consumer disputes" so it would pursue an individual's complaints only when "the company has engaged in a pattern of improper conduct."[362] The FTC has nevertheless assured the Commission of the European Union that it will give priority to claims "of non-compliance with safe harbor principles from EU Member States."[363] The FTC can issue cease and desist orders after conducting "a formal hearing" and it can "seek a temporary restraining order or temporary or permanent injunction in U.S. district court."[364]

Companies that "persistently fail" to comply with the safe harbor principles will lose their certification.[365]

If the FTC, the DOT, or any other "body responsible for ensuring compliance with the Principles implemented"[366] is not enforcing the safe harbor principles, the Commission can inform the Department of Commerce and revoke agreement to the safe harbor framework as to the companies who are under that agency's jurisdiction.[367]

The safe harbor framework applies to "employment-related data."[368] The FTC has concluded that it "has the same jurisdiction in the employment-related data situation as it would generally under Section 5 of the FTC Act."[369] Thus, the FTC can take action in a case when "a company that represents it complies with U.S. safe harbor principles . . . transfers or uses employment-related data in a manner that violates these principles."[370] Nevertheless, the majority of employment-related cases

---

Transportation has authority to enforce the safe harbor framework as to U.S. air carriers or ticket agents. Helpful Hints, *supra* note 357.

360. *Commission Decision*, *supra* note 338, at *7.

361. Letter from Robert Pitofsky to John F. Mogg, *supra* note 338, at 5.; *Commission Decision*, *supra* note 338, at *41.

362. *Commission Decision*, *supra* note 338, at *41.

363. Letter from Robert Pitofsky to John F. Mogg, *supra* note 338, at 2; *Commission Decision*, *supra* note 338, at *40.

364. Export.gov, Safe Harbor Enforcement Overview, http://www.export.gov/safeharbor/eu/eg_main_018481.asp (last visited July 30, 2009).

365. Export.gov, Safe Harbor Overview, http://www.export.gov/safeharbor/eg_main_018236.asp (last visited July 30, 2009).

366. *Commission Decision*, *supra* note 338, at *9.

367. Letter from Robert Pitofsky to John F. Mogg, *supra* note 338.

368. *Id.* at 5; Export.gov, FAQ – Human Resources, http://www.export.gov/safeharbor/eu/eg_main_018381.asp (last visited June 10, 2009).

369. *Commission Decision*, *supra* note 338, at *42.

370. *Id.*

will be handled by the Data Protection Authority and the DPP.[371] When an organization refuses to comply with the advice of the Data Protection Authority, the Data Protection Authority can ask the FTC to prosecute or can revoke the self-certification of the organization.[372]

Like the safe harbor framework, the Proposed Act relies on employers to adopt policies to protect employees' privacy. The benefits of flexibility for employers inherent in the framework are, thus, also inherent in the Proposed Act. Also similar to the safe harbor framework, which requires a fee to cover the expenses associated with certifying a company, the Proposed Act includes a fee to cover the expenses associated with providing opinions on whether a policy satisfies the mandates of the Proposed Act. Additionally, the relatively successful implementation of the safe harbor framework illustrates that employers in the United States are able to adapt to and comply with a somewhat sophisticated privacy regulation, particularly when guidance is provided by an administrative agency, as in the Proposed Act.

Unlike the safe harbor framework, the Proposed Act does not rely on a process of self-certification, which might create unnecessary administrative burden. Rather, employers are expected to adopt policies that comply with the law. The DOL will make available model policy provisions that an employer can adopt and will provide opinions on other policies that strive to incorporate greater protection than that provided by the model policy provisions. Thus, an employer is provided a level of assurance of compliance, similar to the safe harbor framework certification.

IV. PREVIOUSLY PROPOSED SOLUTIONS: SCHOLARS ADDRESS THE PROBLEM

Various academic proposals address how to best protect employees' privacy at work, some of which propose legislation that would protect employees from technological monitoring.[373] Some

371. *See* Export.gov, *supra* note 368; Data Protection Panel, (related to FAQ's 5 and 9 issued by the US Department of Commerce, and annexed to Commission Decision 2000/520/EC on the adequacy of the 'safe harbor' privacy principles) *supra* note 357.

372. Export.gov, FAQ – The Role of the Data Protection Authorities, http://www.export.gov/safeharbor/eu/eg_main_018378.asp (June 10, 2009).

373. Sherman, *supra* note 18, at 653 ("employers should be allowed unfettered monitoring of email transmitted over their own email systems. However, the characteristics of webmail support a parallel conclusion that employers should not be permitted to monitor email communications when workers use their webmail."); Jacobs, *supra* note 37, at 878 (suggesting federal statute based on the Workers Act that contains provisions for "notice, audit, and remedies."); William A. Wines & Michael P. Fronmueller, *American Workers Increase Efforts to Establish a Legal Right to Privacy*

scholars rely on the law of other countries as a foundation for legislation in the United States.[374] Others endorse the Workers Act,[375] and several recommend notice provisions similar to those in the Notice Act or those currently in force in Connecticut and Delaware.[376] Many authors address protecting employees from discharge based on off-duty activity, in a manner similar to the off-duty activity statutes,[377] although the proposals generally do not address monitoring of such activity.[378]

---

as Civility Declines in U.S. Society: Some Observations on the Effort and Its Social Context, 78 NEB. L. REV. 606, 642 (1999) (proposing, among other requirements, good cause for termination and monitoring only with notice and consent); *see generally* Thomas R. Greenberg, Comment, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U.L. REV. 219 (1994) (proposing amendments to the ECPA); McCartney, *supra* note 97, at 891 (proposing federal legislation "that provides a generalized protection for the right to privacy" and establishes a Data Protection Board to administer the Act).

374. Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829, 884-90 (2005); Robert G. Schwartz, Jr., *Privacy in German Employment Law*, 15 HASTINGS INT'L & COMP. L. REV. 135, 167 (1992) (proposing German example as a "useful guide"); Evans, *supra* note 18, at 1148 (proposing federal legislation based on English law); Ray Lewis, Comment, *Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom*, 67 LA. L. REV. 959, 962 (2007) (proposing "abandonment of the ECPA and the adoption of legislation that mirrors the provisions, ideas, and foundations of electronic privacy law of the United Kingdom—the Data Protection Act."); *see also* Fiore & Weinick, *supra* note 3 at 529 (relying on European concept of dignity to justify proposed federal legislation regulating employers who use video surveillance).

375. Amanda Richman, Note, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337, 1360-61 (2001); *see generally* Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256 (1994) (supporting Workers Act with only minor revisions); David Neil King, Note, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging Privacy Gap*, 67 S. CAL. L. REV. 441, 471-73 (1994) (endorsing Workers Act with only two misgivings); *see generally* Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (endorsing PCWA with only minor revisions); *see also* Kevin J. Conlon, *Privacy in the Workplace*, 72 CHI.-KENT L. REV. 285, 294-95 (1996) (proposing provisions similar to the Workers Act but more protective of employees privacy); *see generally* Susan Ellen Bindler, Note, *Peek & Spy: A Proposal for Federal Regulation of Electronic Monitoring in the Work Place*, 70 WASH. U. L.Q. 853 (1992) (proposing substantial changes to the Workers Act); Boehmer, *supra* note 18, at 812-19 (proposing substantial changes to the PCWA).

376. Frayer, *supra* note 103, at 874 (2002); Nathan Watson, Note, *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?*, 54 FED. COMM. L.J. 79, (2001); Lois R. Witt, Comment, *Terminally Nosy: Are Employers Free to Access our Electronic Mail?*, 96 DICK. L. REV. 545, 569-70 (1992) (endorsing notice provisions of Workers Act).

377. William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must be Honest*, 12 EMPLOYEE RTS. & EMP. POL'Y J. 49, 104 (2008) (suggesting that state laws could place "express statutory limitations on the scope of employer electronic surveillance" of off-work activities); *see generally* Hong, *supra* note 187, (proposing lifestyle discrimination statutes as a means to protect employee's privacy to blog when off-duty).

378. *See generally* Shelbie J. Byers, Note, *Untangling the World Wide Weblog: A Proposal for Blogging, Employment-At-Will, and Lifestyle Discrimination Statutes*, 42 VAL. U. L. REV. 245 (2007) (proposing lifestyle discrimination statutes be extended to cover speech as well as activity

In addition to these statutory solutions that are reflected in the previously discussed proposed legislation or law, some scholars have proposed activity-specific regulation,[379] such as laws targeted to protect blogging or e-mailing, and others have proposed regulation of a particular means of monitoring, such as by video or GPS.[380] While these solutions are practical, they fail to address the problem of technological monitoring of employees in a comprehensive manner. [381]

A few scholars have previously proposed broader legislation to address employees' privacy, including from technological monitoring.[382] For example, one proposal recommends federal legislation with a business-necessity test for collection of information about employees.[383] The proposal would require "notice of the type of information that will be collected and the purpose for which it will be collected"[384] and would require the use of the least intrusive manner of collection.[385] It

and conduct as a means to protect employees from termination from adverse employment action based on blogging); Ann L. Rives, Note, *You're Not the Boss of Me: A Call for Federal Lifestyle Discrimination Legislation*, 74 GEO. WASH. L. REV. 553 (2006) (proposing federal lifestyle discrimination statute that covers personal relationships as well as other conduct); *see also* Kirkland, *supra* note 187 (proposing federal lifestyle discrimination statute); Dworkin, *supra* note 227, at 84 (proposing use of a "reasonable business necessity standard" to justify termination based on an employee's associations); Hill & Delacenseri, *supra* note 42, at 55 (proposing just cause as solution to problem of lack of privacy for off-duty activity).

379. *See generally* Gely & Bierman, *supra* note 19 (legislation to protect blogging); Gantt, *supra* note 37 (proposing legislation to protect use of e-mail at work); Hong, *supra* note 187 (proposing lifestyle discrimination statutes as a means to protect employee's privacy to blog when off-duty); Peter J. Isajiw, Comment, *Workplace E-Mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH. J. 73, 99 (2001); Rodriguez, *supra* note 98, at 1442 (proposing "statutory presumption, whereby an employee would be presumed to have reserved her right to e-mail privacy unless expressly waived, as a possible means for strengthening the right to e-mail privacy in the private sector workplace."); Peter Schnaitman, Comment, *Building a Community Through Workplace E-Mail: The New Privacy Frontier*, 5 MICH. TELECOMM. & TECH. L. REV. 177, 214 (1998-1999) (proposing federal legislation that requires employers to adopt e-mail policies.).

380. *See* Yung, *supra* note 37 (legislation to address monitoring via GPS); Fiore & Weinick, *supra* note 3 (legislation to address monitoring via video surveillance); *Cf.* Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 HOFSTRA LAB. & EMP. L.J. 395, 416 (2008) (suggesting amending "'lawful conduct' statutes to prohibit employers from using publicly available personal information that could be obtained through Internet search in their hiring decisions or imposing requirements similar to those applicable to credit reports on the use of such information).

381. Levinson, *supra* note 14, at 628.

382. Wilborn, *supra* note 18, at 876 (proposing "a comprehensive federal statute based on our broad constitutional principles of privacy"); Pincus & Trotter, *supra* note 115; *see also* Lee, *supra* note 50, at 171 (proposing federal legislation governing use of employers' communication technology that would require monitoring to be reasonable).

383. *See generally* Pincus & Trotter, *supra* note 115.

384. *Id.* at 86.

385. *Id.*

additionally incorporates a confidentiality requirement[386] and some limitations on disclosure of information to third parties.[387] The comprehensive nature of the proposal is exemplary, and the Proposed Act contains similar safeguards, as well as additional protections for employee privacy from technological monitoring. But the Proposed Act is intended to allow employers more flexibility to monitor than a proposal with across-the-board requirements for business necessity and use of the least intrusive manner of collection.

Moreover, despite the variety of proposals to address the problem, few scholars have proposed an actual draft of an act,[388] and the majority that have done so propose off-duty conduct statutes.[389] An actual draft is important to show how protections could be put into practical effect. A draft statute may help those suggesting various methods of protecting employees' privacy from workplace technological monitoring think more concretely about the particulars of how to protect workplace privacy. Thinking about the particulars may cause scholars to refine, or even reconsider the workability of, prior proposals that sketch their ideas about workplace privacy protection in broader strokes.[390] Additionally, an actual draft may be helpful in pushing legislatures to adopt real change. Providing a legislature with a draft rather than only ideas may result in a more receptive audience because a draft appears to provide a more definite course for reform and to be less onerous than starting from scratch. The legislature may have to assess every provision and may decide to change every one, but by providing a starting point, the process of beginning may be made easier.[391]

---

386. *Id.* at 87.

387. *Id.* at 88.

388. Blackowicz, *supra* note 37, at 105-06 (proposing a draft of a section amending the ECPA that would "address the proper scope of disclosure.").

389. Marisa Anne Pagnattaro, *What Do You Do When You Are Not at Work? Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U PA. J. LAB. & EMP. L. 625, 680-82 (2004) (proposing an off-duty conduct statute); Byers, *supra* note 378 (proposing lifestyle discrimination statutes extended to cover speech as well as activity and conduct as means to protect employees from termination from adverse employment action based on blogging); Rives, *supra* note 378 (proposing federal lifestyle discrimination statute that covers personal relationships as well as other conduct); Kirkland, *supra* note 187 (proposing federal lifestyle discrimination statute); Hong, *supra* note 187, at 460 (draft language of a lifestyle discrimination statute that specifically includes protection for "engaging in Internet communications").

390. *Cf.* Nicole B. Porter, *The Perfect Compromise: Bridging the Gap Between At-Will Employment and Just Cause*, 87 NEB. L. REV. 62, 84 (2008) (describing how she changed her thoughts about how to best protect employees from unwarranted terminations when she drafted a proposed statute).

391. *See* Solove & Hoofnagle, *supra* note 2, at 358 ("it is imperative to have a discussion of concrete legislative solutions to privacy problems" to "provide useful guidance to legislators").

V. PROPOSED SOLUTION: AN ACT TO ENSURE PRIVACY FOR EMPLOYEES FROM TECHNOLOGICAL MONITORING

A draft of the Proposed Act is set out in this section, V. The Proposed Act is annotated with footnotes to disclose the specific sources, most of which have been discussed above, from which the language or ideas are drawn. In the next section, VI., some of the major considerations that went into the choices underlying the proposal, which may not be apparent from the text of the Proposed Act, are discussed. More minor choices are included in the footnotes annotating the statute in this section, V.

The Proposed Act is not necessarily intended as a model but rather as a deliberate effort to draft statutory language that appropriately balances the need of employers to monitor with the right of employees to appropriate safeguards for their privacy. The author believes that further academic scholarship, the wisdom of practitioners, and the expertise of legislatures and their staffs, will further refine the proposal into a piece of legislation that can fill an important legal gap. The author also believes that the Proposed Act would be only one step in addressing the privacy issues raised by new technologies, in the employment setting, at a comprehensive level.

A. Short Title

This Act may be cited as the Privacy Protection in Employment Act.

B. Purpose and Findings

1. Purpose. This Act safeguards the privacy of employees who are or may be technologically monitored by their employers.

2. Findings. Current law fails to adequately protect employees' privacy when the employees are technologically monitored by their employers.[392]

An estimated 77 percent of employers technologically monitor their employees. Approximately, 14 million "are under 'continuous' surveillance . . . for their Internet access or e-mail usage."[393] Yet, approximately two out of every three "corporate workplaces have no

392. *See supra* note 18.

393. Levinson, *supra* note 14, at 616.

policy requiring their employees to manifest consent to electronic monitoring or acknowledging their workplace monitoring activities."[394]

The European Union considers current United States law inadequate to protect employees' privacy.[395]

Technological monitoring involves interstate commerce and is of cross-border concern. Many of the communications or actions monitored, such as e-mail messages or Internet hits, occur across interstate lines. The issue is, thus, one of national importance.[396]

C. Definitions

Technological Monitoring. Technological monitoring is the collection of information about an employee "conducted by a [means] other than direct observation by another person."[397] Technological monitoring includes electronic monitoring, monitoring by means of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic, photo-optical system, GPS, RFID, and video surveillance whether or not silent.[398]

Employer. Employer means any person, including "any individual, corporation, partnership, [firm], labor organization, unincorporated association, or any other legal business"[399] who is engaged in commerce and for whom an individual performs work "for more than one quarter of the year"[400] and any agent of such a person.[401] Employer excludes the Federal Government and any State or political subdivision thereof.

Employee. Employee means any person who works, including part-time, for an employer "in exchange for financial remuneration."[402]

---

394. Rustad & Paulson, *supra* note 374, at 830 (quoted in Levinson, *supra* note 14, at 616).

395. *See supra* note 25.

396. *See infra* note 512.

397. Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 2(2)(A) (1993). *See also* CONN. GEN. STAT. § 31-48d (2008) (defining electronic monitoring as "the collection of information on an employer's premises concerning employees' activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photoelectronic or photo-optical systems . . .").

398. CONN. GEN. STAT. § 31-48d (2008); MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 1(a).

399. S. 984; *see* DEL. CODE ANN. tit. 19, § 705(a) (2008).

400. N.D. CENT. CODE § 14-02.4-02(8) (2008).

401. MICH. COMP. LAWS § 423.501(2)(b) (2008).

402. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 1(b). The Proposed Act does not cover applicants for employment. The focus of this article is rectifying the failure of the law to adequately protect employees from technological monitoring. Monitoring of applicants raises issues different than monitoring of employees, which are beyond the scope of this article. *See* Boehmer, *supra* note 18, at 814-15 (discussing how more liberty to monitor applicants may lead to less monitoring of employees).

Employee includes persons "subject to recall after layoff or leave of absence with a right to return" to a position with the employer.[403]

On Duty. On duty means all time an employee is "expected to be engaged in work" or is "actually engaged in work."[404] If not working, an employee is not on-duty during breaks, including meal period breaks, or during leaves of absence, including time for family medical leave or disability leave.

Off Duty. Off duty means any time an employee is not engaged in, or expected to be engaged in, work.

D. Monitoring On-Duty Behavior

An employer must not technologically monitor an employee's on-duty behavior unless it institutes the following safeguards:

1. Notice of Monitoring. The employer must provide the employee individualized advance notice in writing that technological monitoring will take place. The notice must be clear and conspicuous and reasonably calculated to provide the employee actual notice of the monitoring. [405] A notice that provides monitoring "may" take place or that the employer "reserves the right" to monitor will not suffice.

2. Notice of Type of Monitoring. The notice must specify the type of monitoring that will occur, such as specifying that e-mail will be monitored by software or by periodic review of the mail server, that content on the computer screen will be monitored by keystroke monitoring technology, that e-mail stored on the server will be reviewed in response to court-ordered discovery, or that video surveillance will occur.

3. Notice of Information Collecting. The notice must specify the type of information that will be obtained.[406]

4. Notice of Intended Use. The notice must specify how the employer will use the obtained information.[407]

5. Notice of Infractions. The notice must specify the types of infractions that, if discovered via the monitoring, will result in discipline.[408]

---

403. 820 ILL. COMP. STAT. 40/1(a) (2008).

404. NY McKinney's Lab. Law Sec. 201-d.

405. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(b) (2000).

406. H.R. 4908, at § 2711(b)(2).

407. *Id.* § 2711(b)(4). For instance, it might describe the manner in which it will be used to gauge productivity or how it will be used for disciplinary purposes.

408. Levinson, *supra* note 14, at 644. While other rules or policies may describe potential infractions, it is easy enough to reference those other rules or policies in the notice.

6. Annual Notice of Monitoring. When monitoring continues for more than a year, the employer must provide annual individualized written notice that the monitoring continues to take place and must specify the type of monitoring, the type of information that will be collected, and the intended use of the information.[409]

7. Accurate and Reliable Records. To ensure accuracy and reliability of information collected via technological monitoring, the employee must have the right to review, copy, and contest the information as set forth below.

a. Right to Review. The employer must provide each employee a "reasonable opportunity to review and, upon request, [obtain] a copy of"[410] any information collected that has been or will be used to make employment decisions about the employee, including promotions, transfer, counseling, assignments, compensation, scheduling, or discipline, including discharge.[411] This information does not include "materials relating to the employer's staff planning with respect to more than one employee,"[412] such as across-the-board "salary increases, management bonus plans,"[413] "business' development, expansion, closing or operational goals."[414]

Upon completion of the monitoring or upon initiating the process of making an employment decision, whichever occurs first, the employer must provide each employee" a "reasonable opportunity to review and, upon request, [obtain] a copy of" the required documentation and any information collected about the employee during monitoring without notice on reasonable grounds, under sections E (Monitoring On-Duty Actions Without Notice), G (Monitoring of On-Duty Communications Without Notice), or I.3 (Monitoring Off-Duty Behavior—Other Places).[415]

The employer must provide each employee" a "reasonable opportunity to review and, upon request, [obtain] a copy of" any information collected about the employee through which the employee is identifiable that will be released to a third party, such as through court discovery.[416]

---

409. *See* H.R. 4908, at § 2711(a)(2) (2000) (providing for annual notice).
410. Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 7(a) (1993).
411. *See* 820 ILL. COMP. STAT. 40/2 (2008).
412. MICH. COMP. LAWS § 423.501(2)(c)(ii) (2008).
413. § 423.501(2)(c)(ii).
414. 820 ILL. COMP. STAT. 40/10(c) (2008).
415. S. 984, at § 7(a).
416. S. 984, at § 7(a).

"The employer shall grant at least two inspection requests by an employee in a calendar year when requests are made at reasonable intervals."[417]

"The employer shall provide the employee with the inspection opportunity within [seven] working days after the employee makes the request or if the employer can reasonably show that such deadline cannot be met, the employer shall have an additional [seven] days to comply."[418]

"The review shall take place at a location reasonably near the employee's place of employment and during normal office hours. If a review during normal office hours would require an employee to take time off from work with that employer, then the employer shall provide some other reasonable time for the review. The employer may allow the review to take place at another time or location that would be more convenient to the employee."[419]

b. Right to Copy. "After the review . . . an employee may obtain a copy of the information or part of the information . . . . An employer may charge a fee . . . limited to the actual [cost of copying, for providing a copy of the information]. If an employee demonstrates that he or she is unable to review his or her personnel record at the employing unit, then the employer, upon that employee's written request, shall mail a copy of the requested record to the employee."[420]

c. Right to Contest. "If there is a disagreement with information . . . , removal or correction of that information may be mutually agreed upon by the employer and the employee. If an agreement is not reached, the employee may submit a written statement explaining the employee's position."[421] The statement must be maintained with the original information "as long as the original information" is maintained and "included when the information is divulged to a third party."[422]

d. Right to Agent. The employee has the right to choose an agent,[423] such as a co-worker, union representative, or attorney, to conduct the review of the information with the employee or to contest the accuracy of the information.

---

417. 820 ILL. COMP. STAT. 40/2 (2008).
418. 820 ILL. COMP. STAT. 40/2 (2008).
419. MICH. COMP. LAWS § 423.503 (2008).
420. MICH. COMP. LAWS §§ 423.503-423.504 (2008).
421. MICH. COMP. LAWS § 423.505 (2008).
422. § 423.505.
423. Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 7(B)(1) (1993) (uses the term "authorized agent").

E. Monitoring On-Duty Actions without Notice

Notwithstanding the requirements of Section D, 1-6, "if the employer has reasonable grounds to believe that" [424] an employee has engaged in a violation of a written work rule or written work policy, a violation of law, or behavior that has significantly and concretely harmed the employer, an employer may technologically monitor, without complying with Section D, 1-6, an employee or a suspected group of employee's on-duty actions or "an area [on the employer's premise] in which the" infraction occurred[425] by complying with the below safeguards and adopting and complying with a policy that adopts model provisions promulgated by the DOL for monitoring of on-duty actions without notice.[426]

1. Documentation. The employer must document in writing, before monitoring, the behavior suspected and the intended means of monitoring. The statement should include the grounds for suspicion, such as the names of witnesses and a summary of their testimony or a summary of relevant documentary evidence. Upon completion of monitoring, the employer must document in writing the means of monitoring used and the length of time of the monitoring. The documentation must be retained for three years or until any claim or suit brought under this Act is resolved.[427]

2. Qualification. An employer may not monitor under the provisions of this section, E., when the employer already has sufficient evidence, obviating the need to monitor, that a particular employee has committed an infraction.

---

424. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(c) (2000).

425. S. 984, at § 5(C)(1)(B).

426. Rather than use a "reasonable suspicion standard" the Proposed Act uses a "reasonable grounds" standard. The standard should not be confused with the Fourth Amendment standard, which may require particularized suspicion before monitoring an individual. Rather, if a known violation, such as theft or smoking, has occurred, the employer may monitor the area and any employees who enter the area. Relatedly, commentators have noted in relation to the Workers Act that:

> If notice needs to be given to employees who are not under suspicion, but who will be monitored, many complications are foreseeable. An example of this is a manufacturer who has reasonable suspicion that an employee is stealing merchandise. Although the employer can justify putting a hidden camera in the employee's area without informing the employee under suspicion, the Bill requires the employer to inform all other employees that may appear in the camera's range of the monitoring. It is reasonable to assume in many instances that the employee's friends will inform the suspect of the monitoring and the employer will not be able to discipline the wrongdoer.

Baxi & Nickel, *supra* note 97, at 146.

427. S. 984, at § 5(C)(2)(C).

F. Monitoring On-Duty Communications

An employer must not technologically monitor an employee's use of the employer's communications technology, including computers, or an employee's on-duty communications unless the employer has a legitimate business interest in prohibiting communications or use of the employer's communications technology that is likely to negatively impact the business or workplace. The employer must also comply with the below safeguards and must technologically monitor only pursuant to a written policy that adopts and complies with model provisions promulgated by the DOL for engaging in noticed monitoring of the employer's communications technology and on-duty communications.

1. Presumptions. The following types of use of an employer's technology or on-duty communications are presumed likely to negatively impact the business or workplace and to provide an employer a legitimate business interest for monitoring.

a. Unlawful Use. Unlawful use of the employer's technology, including unlawful use of a computer, and unlawful communications, such as downloading images of child pornography or making defamatory statements.

b. Offensive Communication. Viewing or making statements of a racially or sexually offensive nature.

c. Proprietary Information. Personal use of the employer's proprietary information.

d. Solicitation. Requesting donations for organizations for personal use.[428]

e. Disrespect. Communications that are disrespectful of management or criticize the employer.[429]

2. Minimal Negative Impact. When the negative impact on the business or workplace is likely to be minimal, the employer must mitigate the level of discipline imposed on a first-time violator, from that which would normally be imposed for any discovered infraction, in consideration of the private nature of the communication or use. The employer should consider the degree to which the prohibited information was kept private, such as whether it was shared with no one, shared only with the employee's friends or acquaintances, or the number of others with whom it was shared. The level of discipline imposed should be

428. This presumption does not include requests to join or support organizations and is not intended to change the protected nature of certain solicitations under the NLRA.

429. This is not intended to change the protected nature of certain disrespectful statements under the NLRA.

mitigated more considerably the more private the nature of the communications or use.

Presumptions. The types of use of an employer's communications technology or on-duty communications listed in F.1.d. & e. (Solicitation and Disrespect) are presumed to only minimally negatively impact the business or workplace.

3. Monitoring of Employee's Communications Technology on Employer's Property. An employer must not monitor an on-duty employee's employee-owned technological communications devices located on the employer's property, such as a cell phone or pager, without complying with the safeguards set forth in section I.3 (Monitoring of Off-Duty Behavior—Other Places).

Nothing in this Act prohibits an employer from banning employees' personal communications technology from the workplace or from prohibiting use of such technology in certain areas or at certain times.

G. Monitoring of On-Duty Communications without Notice

Notwithstanding the requirements of Section D, 1-6, "if the employer has reasonable grounds to believe that"[430] an employee has engaged in a violation of a written work rule or written work policy that is likely to negatively impact the business or workplace, a violation of law, or behavior that has significantly and concretely harmed the employer, an employer may technologically monitor, without complying with Section D, 1-6, an employee's use of the employer's communications technology, including computers, or an employee's on-duty communications by complying with the below safeguards and adopting and complying with a policy that adopts model provisions promulgated by the DOL for monitoring of the employer's communications technology and monitoring of on-duty communications without notice.[431] The employer must also comply with Section E.1. (Documentation).

1. Excessive Use. An employer may only monitor without notice for the purpose of discovering an employee's excessive use of the employer's communication technology when the employer has reasonable grounds to believe that the employee is engaged in excessive personal use of the technology that is likely to detrimentally impact the employee's job performance. The employer must exhaust other methods of verification

430. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(c) (2000).
431. S. 984, at § 4.

or discovery before resorting to the reasonable grounds surreptitious monitoring.

2. Qualification. An employer may not monitor under the provisions of this section, G., when the employer already has sufficient evidence, obviating the need to monitor, that a particular employee has committed an infraction.

H. Monitoring Prohibited on Premises

An employer must not technologically monitor in: "(1) bathrooms; (2) locker rooms;" [432] (3); "dressing rooms"; [433] (4) "shower facilities"; or (5) "other similar private" changing "areas."[434]

I. Monitoring Off-Duty Behavior

1. Homes. An employer must not technologically monitor its employees when they are inside their homes, except as provided in section I.4 (Monitoring the Employer's Property). This prohibition applies equally to technological monitoring of employees who are on-duty inside their homes.

2. Off Duty in Seclusion. An employer must not technologically monitor its employees who are off duty and either outside or at a private residence and who are alone or with only a few[435] other people.

3. Other Places. An employer must not technologically monitor an off-duty employee's behavior in circumstances other than those mentioned in Sections H.1 & 2 unless the employer "has reasonable grounds to believe that"[436] the employee is engaging in behavior that will cause a significant concrete harm to the employer and must do so only pursuant to a written policy that adopts and complies with model provisions promulgated by the DOL for engaging in monitoring off-duty behavior. The employer must also comply with Sections D.7 (Accuracy and Reliability) and E.1 (Documentation).

a. Presumptions of Significant Harm. The following types of off-duty behavior are presumed to cause a significant concrete harm to the employer.

---

432. *Id.* § 10(b).

433. *Id.*

434. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 5.

435. "Few" is left purposefully somewhat vague to account for differing circumstances. An actual number could easily be inserted instead.

436. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(c) (2000).

i. Competition. Behavior "in direct conflict with the essential business-related interests of the employer";[437]
ii. Reduction in Work. Behavior that causes a verifiable reduction in the quality or quantity of the employee's work;
iii. Harassment. Behavior that harasses another employee or the employee's family because of the employee's work-related actions;
iv. Obscene Role Models. Behavior by a children's role model that is obscene;
v. Financial Harm. Behavior that causes a verifiable financial harm which is more than minimal;[438]
vi. Complaints. Behavior that results in customer or client complaints;
vii. Refusal to Work. Behavior that results in co-employees refusing to work with the employee.
b. Presumptions of Insignificant Harm. The following types of off-duty behavior are presumed not to cause a significant concrete harm to the employer.
i. Office Morale. Behavior that negatively impacts office morale but does not cause a verifiable reduction in the quality or quantity of the employee's work;
ii. Injury to Reputation. Behavior that will potentially damage the company's reputation but has not resulted in customer or client complaints or cessation of business;
iii. Appearance of Conflict of Interest. Behavior that may result in a perception of an employee having a conflict of interest when the quality and quantity of the employees work is unaffected and there are no complaints from customers or clients.
c. Qualification. An employer may not monitor under the provisions of this sub-section, I.3., when the employer already has sufficient evidence, obviating the need to monitor, that a particular employee has committed an infraction.
4. Monitoring the Employer's Property. An employer may monitor the use of its own property by an off-duty employee, such as a computer or vehicle, including when the employee is located at home. In order to monitor such property, the employer must comply with the requirements set forth in sections F (Monitoring On-Duty Communication) or G (Monitoring of On-Duty Communications Without Notice). Monitoring

437. N.D. CENT. CODE § 14-02.4-02(6) (2008).
438. The term "minimal" leaves it for the decision makers to consider the particular facts, but a dollar amount could easily be inserted if the legislature preferred.

the property does not permit monitoring of behavior unrelated to use of the property.[439]

J. Employee Participation

1. Methods of Consultation. Before instituting a policy in compliance with this Act, an employer must consult with the employees, to whom the policy will be applicable, regarding which model policy provisions to adopt and which additional provisions, if any, to include. Methods of consultations that satisfy this requirement include the following:

1. Consultation with an exclusive bargaining representative;[440]
2. When employees are not represented by an exclusive bargaining representative, anonymous poll;
3. When employees are not represented by an exclusive bargaining representative, an employee or workplace committee with responsibility for workplace privacy or workplace technology issues;[441]
4. When employees are not represented by an exclusive bargaining representative, consultation with an attorney or union representative selected by the employees to assist them with providing input.[442]

2. Notice. Before instituting a policy in compliance with this Act, an employer must provide employees who are not represented by an exclusive bargaining representative notice of the right to consult regarding the policy and of the various methods available for consultation. The notice must be clear and conspicuous and reasonably calculated to provide the employee actual notice of the monitoring.

K. Maintenance of Records

1. Time Period. An employer must maintain any document that the employee has the right to review pursuant to Section D.7 (Accurate and

439. *See* Yung, *supra* note 37, at 213 (recommending that employer be permitted to monitor its asset "for the sole purpose of protecting the asset").

440. This provision does not abrogate any responsibility under the NLRA or a collective bargaining agreement to negotiate over the terms of the policy with the union.

441. Javier Thibault Aranda, *Information Technology and Workers' Privacy: The Role of Worker Representatives*, 23 COMP. LAB. L. & POL'Y J. 533, 536-37 (2002) (recommending a more robust system of consultation through joint committees, similar to those used for health and safety issues in Spain that investigate and negotiate).

442. The latter three methods are not intended to abrogate the prohibition on employer support and domination under § 8(a)(2) of the NLRA. Instead, these methods are intended to be carried out in a manner that complies with that provision.

Reliable Records) for a reasonable period of years, not fewer than three.[443]

2. Security. All records resulting from technological monitoring and maintained by the employer that contain information identifiable to individual employees must be maintained in a secure manner.

3. Disposal. All records resulting from technological monitoring that contain information identifiable to individual employees must be disposed of in a manner that eliminates risk of use of the information by others.

L. Disclosure of Information Collected

"[A]n employer" must "not disclose" information about an employee, through which the employee is identifiable, obtained through technological monitoring to third parties except in the following circumstances:[444]

(1) "to a law enforcement agency pursuant to a warrant issued under the Federal Rules of Criminal Procedure, an equivalent state warrant, a grand jury subpoena, or an administrative subpoena authorized by a Federal or State statute."[445]

(2) "pursuant to the order of a court of competent jurisdiction."[446]

(3) "to the exclusive bargaining representative, if any."[447]

An employer must notify third parties to whom the data have been disclosed of any erasure or correction to or of any employee statement responding to previously released information, pursuant to section D.7 (Accurate and Reliable Records), unless notification would be unduly burdensome.

M. Anti-Retaliation Provision

"No employer may" "discharge, discipline, or in any manner discriminate against an employee with respect to the employee's

443. *See* Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 5 (1993).

444. S. 984, at § 10 (1993).

445. S. 984, at § 10.

446. Privacy for Consumers and Workers Act, H.R. 1218, 102d Cong. § 9 (B)(c)(1992). Typically parties to a civil suit are entitled to discover information relevant through discovery that is not specifically ordered by a court, including in some jurisdictions mandatory initial disclosures. This provision will require employers to obtain a court order before providing such information in discovery. A different solution that protects employees' privacy and enables court suits to progress with more efficiency may be possible. But the details of disclosure protections are beyond the scope of this article.

447. S. 984, at § 10(D)(4).

compensation or terms, conditions, or privileges of employment because the employee (or any person acting pursuant to a request of the employee) has—[448]
(A) instituted [or is about to institute][449] any proceeding relating to a violation of this Act,"[450]
(B) "participated in enforcement actions under this"[451] Act,
(C) disclosed information that the employee reasonably believes evidences a violation of this Act,[452]
(D) "assisted other employees in asserting their rights"[453] under this Act, including acting as a representative pursuant to Section D.7.D (Right to Agent),
(E) participated in providing employee input into development of a policy in compliance with this Act pursuant to Section J (Employee Participation).

N. Responsibilities Designated to the Department of Labor

1. Office of Employee Privacy. The Office of Employee Privacy is hereby created within the Department of Labor. The Office of Employee Privacy will "be under the direction of an [a]dministrator . . . appointed by the President, by and with advice and consent of the Senate."[454] The Department of Labor, acting through the Office of Employee Privacy, is charged with the following responsibilities.
2. Safe-Harbor Policies. The Department of Labor will draft model policy provisions for adoption by employers.
a. On-Duty Actions without Notice. The DOL will promulgate at least three sets of model policy provisions for monitoring of on-duty actions without notice. Each set of model policy provisions will incorporate notice of the requirements of Section D.7 (Accurate and Reliable Records).
i. First Set of Model Policy Provisions. The first set of model policy provisions will include provisions implementing the following safeguards:

448. S. 984, at § 11(4).
449. *See* WILLIAM A. HERBERT, ADVANCED EMPLOYMENT RETALIATION ISSUES 5 (2005), http://works.bepress.com/cgi/viewcontent.cgi?article=1007&context=william_herbert (discussing 29 C.F.R. 24.2(b) using language "about to commence").
450. S. 984, at § 11(4).
451. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 7.
452. Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 11(4) (1993).
453. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 7.
454. 29 U.S.C. §204(a).

a) Notice of Monitoring. The employer must provide individualized advanced notice in writing to employees that they will be monitored when the employer has reasonable grounds to believe that an employee has engaged in a violation of a written work rule or written work policy, a violation of law, or behavior that has significantly and concretely harmed the employer. The notice must be clear and conspicuous and reasonably calculated to provide the employee actual notice of the potential monitoring.[455] A notice that provides monitoring "may" take place or that the employer "reserves the right" to monitor will not suffice.

b) Notice of Infractions. The notice must delineate the types of infractions for which such reasonable grounds monitoring will occur.

c) Explanation of Reasonable Grounds. The notice must explain what constitutes reasonable grounds, such as a statement from an identified co-worker[456] or evidence of an infraction that is not attributable to a particular individual.[457]

d) Annual Notice. If the employer continues to monitor based on reasonable grounds, it must provide the requisite notice annually.

e) Consistent Enforcement. The employer must consistently enforce the policy.

ii. Second Set of Model Policy Provisions. The second set of model policy provisions will include provisions implementing the following safeguards:

a) Exhaustion. The employer must exhaust other methods of verification or discovery before resorting to the reasonable grounds surreptitious monitoring.

b) Bonus. After completion of the reasonable grounds surreptitious monitoring, the employer must provide a bonus, within a year's time, to the employee to compensate for the invasion of privacy. The minimum amount of the bonus will be set out by schedule developed by the DOL and will account for the level of intrusiveness of the monitoring, by considering the means of monitoring, the behavior monitored, and the length of time monitoring occurs. The minimum amount must be no less than the equivalent of $300.00 in 2010, adjusted for inflation.

iii. Other On-Duty Model Policy Provisions. The other set(s) of model policy provisions for monitoring of on-duty conduct without notice must provide a minimum level of protection for employee's

455. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(b) (2000).

456. The term identified is intended to mean that the statement must not be anonymous. It is not intended to prevent the employee who supplies the statement from remaining confidential.

457. This may be necessary when there is evidence of theft or smoking, for instance.

privacy equivalent to the level of protection provided by the above mandates.

b. On-Duty Communications with Notice. The DOL will promulgate at least four sets of model policy provisions for monitoring of employee's use of the employer's communications technology and monitoring of on-duty communications with notice.

i. First Set of Model Policy Provisions. The first set of model policy provisions will include provisions implementing the following safeguards and the safeguard set out in N.2.a.i(e) (Consistent Enforcement).

a) Particulars of Monitoring. The notice must describe with particularity the method of monitoring.[458] It should include information about which parts of a communication or use are monitored, such as the heading or the body of an e-mail message or URL addresses; whether specified words are searched for; if so, the basis upon which those words are determined, whether the words are subject to change, and upon what basis; the frequency with which the communications or use are monitored;[459] and any type or number of collected data that leads to a higher level of monitoring. The notice must specify "whether communications or computer usage not related to the employer's business are likely to be monitored."[460]

b) Notice of Type of Use or Communication. The notice must delineate the types of communication or use for which such legitimate business interest monitoring will occur.

c) Confidential or Limited Monitoring. The employee or agent responsible for performing the monitoring must either retain personal information in confidence[461] or the review must be limited in scope.

1) Confidential Monitoring. The monitoring employee or agent must not disclose to anyone, including management, any personal

458. For instance, rather than stating only that Internet use is monitored to insure pornography is not downloaded, the policy would state that every hit on a website is monitored for a list of inappropriate words. It would provide examples of such words and notify the user that they are subject to change based on identified employee use of sites that are inappropriate but contain different words. The policy would notify the employees that when an employee hits a designated number, perhaps twenty, of sites with inappropriate words, then the full content of every site being visited by the employee is monitored.

459. H.R. 4908, at § 2711(b)(2).

460. H.R. 4908, at § 2711(b)(2).

461. Commentators have endorsed the idea of requiring a "data protection officer." *See, e.g.*, Aranda, *supra* note 441, at 23. BCR's often require that a privacy officer or office be established by each company or a responsible employee be designated. Wugmeister, *supra* note 337, at 485.

information, communication, or use that does not negatively impact the business or workplace.[462]

2) Limited Monitoring. The monitoring must be tailored to that necessary to discover only information, communications, or use related to the noticed legitimate business reason. The monitoring must be limited by part of the communication or use searched, search terms, time, duration, and frequency to that necessary to determine if communications or use negatively impacting the business or workplace are occurring.

ii. Second Set of Model Policy Provisions. The second set of model policy provisions will include provisions implementing the following safeguards and the safeguard set out in N.2.a.i(e) (Consistent Enforcement).

a) Automatic, Generalized Monitoring. The employer must use technology, and not human review, to monitor communications or use for the specified type or types of legitimate business reasons.[463] The monitoring must be limited to discovery of terms or parts of the communication, such as a URL address or e-mail "to" line. The actual content of an individual employee's communications or uses must be scrutinized further only when a particular term is located or a certain limit is reached.[464]

b) Confidential or Limited Monitoring. The employee or agent responsible for performing the monitoring must either retain personal information in confidence or the review must be limited in scope.

1) Confidential Monitoring. The employee or agent responsible for scrutinizing the actual content of the communication or use must not disclose to anyone, including management, any personal information, communication, or use that does not negatively impact the business or workplace.[465]

2) Limited Monitoring. The employee or agent responsible for scrutinizing the actual content of the communication or use must review the content only of those communications or uses that triggered the higher level of scrutiny.

---

462. For instance, if while monitoring for pornography, a reviewer found that an employee had paid an electric bill or checked library hours, this information would be held in confidence.

463. For instance, the program might monitor for all uniform resource locators (URLs) on a list of prohibited pornographic sites or for all e-mails that contain a certain term that might indicate proprietary information is enclosed in an e-mail.

464. Such as identifying twenty instances of attempting to access a pornographic site.

465. For instance, if while monitoring for pornography a reviewer found that an employee had paid an electric bill or checked library hours, this information would be held in confidence.

c) Mitigation of discipline. The employer must mitigate the level of discipline for a first-time offender, from that which would normally be imposed for any discovered infraction, in consideration of the private nature of the communication or use. The employer should consider the degree to which the prohibited information was kept private, such as whether it was shared with no one, shared only with the employee's friends or acquaintances, or the number of others with which it was shared. The level of discipline imposed should be mitigated more considerably the more private the nature of the communications or use.

iii. Other Noticed Communication Model Policy Provisions. The other sets of model policy provisions for monitoring of employer's communication technology and on-duty communications with notice must provide an intermediate level of protection for employee's privacy equivalent to the level of protection provided by the above mandates.

c. On-Duty Communications without Notice. The DOL will promulgate at least four sets of model policy provisions for monitoring use of employer's communications technology and of on-duty communications without notice. Each set of model policy provisions will incorporate notice of the requirements of Section D.7 (Accurate and Reliable Records).

i. First Set of Model Policy Provisions. The first set of model policy provisions will include provisions implementing the following safeguards and the safeguards in sections N.2.a.ii(a)(Exhuastion), N.2.a.ii(b)(Bonus) and N.2.b.ii(c)(Mitigation of Discipline).

a) Notice of Infractions. In advance of the monitoring, the employer must have provided the employee individualized notice in writing that is clear and conspicuous and reasonably calculated to provide actual notice that the type of infraction, for which the employer will monitor, is a violation of work rules or policy.

b) Notice of Discipline. The notice must include the potential level of discipline for engaging in the infraction.

c) Confidential or Limited Monitoring. The employee or agent responsible for performing the monitoring must either retain personal information in confidence or the review must be limited in scope.

1) Confidential Monitoring. The monitoring employee or agent must not disclose to anyone, including management, any personal information, communication, or use that does not negatively impact the business or workplace.

2) Limited Monitoring. The monitoring must be tailored to that necessary to discover only information, communications, or use related to the suspected infraction. The monitoring must be limited by part of

the communication or use searched, search terms, time, duration, and frequency to that necessary to verify whether the infraction has occurred.

ii. Second Set of Model Policy Provisions. The second set of model policy provisions will include provisions implementing the following safeguards and the safeguards in sections N.2.a.i(e) (Consistent Enforcement), N.2.b.i(a) (Particulars of Monitoring), N.2.c.i(a) (Notice of Infractions), N.2.c.i(b) (Notice of Discipline), and N.2.c.i(c) (Confidential or Limited Monitoring). It must also institute either the safeguards in section N.2.a.ii(b) (Bonus) or N.2.b.ii(c)(Mitigation of Discipline).

a) Notice of Monitoring. The employer must provide individualized advanced notice in writing to employees that they will be monitored when the employer has reasonable grounds to believe that[466] an employee has engaged a violation of a written work rule or written work policy that is likely to negatively impact the business or workplace, a violation of law, or behavior that has significantly and concretely harmed the employer. The notice must be clear and conspicuous and reasonably calculated to provide the employee actual notice of the potential monitoring.[467] A notice that provides monitoring "may" take place or that the employer "reserves the right" to monitor will not suffice.

iii. Other Un-Noticed Communication Model Policy Provisions. The other sets of model policy provisions for monitoring of employers' communication technology and on-duty communications without notice must provide an intermediate level of protection for employees' privacy equivalent to the level of protection provided by the above mandates.

d. Monitoring Off-Duty Behavior. The DOL will promulgate at least three sets of model policy provisions for monitoring of off-duty behavior. Each set of model policy provisions must incorporate the safeguards set forth in section D.7 (Accuracy and Reliability).

i. First Set of Model Policy Provisions. The first set of model policy provisions will include provisions implementing the following safeguards and the safeguards in sections N.2.a.i(e) (Consistent Enforcement), D.2 (Notice of Type of Monitoring), D.3 (Notice of Information Collecting), D.4 (Notice of Intended Use), E.1.B.i. (Exhuastion), N.2.a.i(b) (Notice of Infractions), and N.2.a.ii(b) (Bonus).

a) Confidential Monitoring. The monitoring employee or agent must not disclose to anyone, including management, any behavior, including

466. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(c) (2000).

467. *Id.* § 2711(b).

actions or communications, that does not evidence the infraction for which a reasonable grounds to monitor was documented. Other infractions incidentally discovered must not be disclosed. The monitoring employee or agent must disclose information that does evidence the infraction for which reasonable grounds to monitor was documented only to those with a need to know.

b) Limited Monitoring. The monitoring must be tailored to that necessary to discover only behavior related to the infraction for which reasonable grounds to monitor have been documented. The monitoring must be limited by type of action or communication monitored, part of the communication or use searched, search terms, time, duration, and frequency to that necessary to determine if the suspected infraction is occurring.

c) Notice of Monitoring. The employer must provide individualized advanced notice in writing to employees that they will be monitored when the employer has reasonable grounds to believe that[468] an employee is engaging in off-duty behavior that will cause a significant concrete harm to the employer. The notice must be clear and conspicuous and reasonably calculated to provide the employee actual notice of the potential monitoring.[469] A notice that provides monitoring "may" take place or that the employer "reserves the right" to monitor will not suffice.

d) Particulars of Monitoring. The notice must describe with particularity the method of monitoring. When employees' communications will be monitored, the notice should include information about which parts of a communication or use are monitored, such as the heading or the body of an e-mail message or URL addresses; whether specified words are searched for; and if so, the basis upon which those words are determined, whether the words are subject to change, and upon what basis; the frequency with which the communications or use are monitored;[470] and any type or number of collected data that leads to a higher level of monitoring.

e) Mitigation of Discipline. The employer must mitigate the level of discipline for a first-time offender, from that which would normally be imposed for any discovered infraction, in consideration of the private nature of the behavior. The level of discipline imposed should be mitigated more considerably the more private the nature of the behavior

468. *Id.* § 2711(c).
469. *Id.* § 2711(b).
470. *Id.*

monitored. When the infraction results from an employee's communications, the employer should consider the degree to which the prohibited information was kept private, such as whether it was shared with no one, shared only with the employee's friends or acquaintances, or the number of others with which it was shared.

ii. Second Set of Model Policy Provisions. The second set of model policy provisions will include provisions implementing the following safeguards and the safeguards in sections N.2.a.i.(e) (Consistent Enforcement), D.2 (Notice of Type of Monitoring), D.3 (Notice of Information Collecting), D.4 (Notice of Intended Use), E.1.B.i. (Exhaustion) N.2.a.ii(b) (Bonus), N.2.d.i(a) (Confidential Monitoring), N.2.d.i(b) (Limited Monitoring), and N.2.d.i(d) (Particulars of Monitoring).

a) Notice of Monitoring. After the discovery of the potential infraction and before monitoring the employee, the employer must provide the employee notice in writing that the employee will be monitored. The notice must be clear and conspicuous and reasonably calculated to provide the employee actual notice of the monitoring. [471]

b) Notice of Infraction. The notice must inform the employee of the infraction that is being monitored for with sufficient specificity to provide the employee actual notice of the particular problem.

c) Potential Discipline. The notice must inform the employee of the potential level of discipline for the alleged infraction.

d) Consistent Discipline. Similar infractions must be similarly disciplined.

iii. Other Off-Duty Model Policy Provisions. The other set(s) of model policy provisions for monitoring of employees' off-duty behavior must provide must provide a high level of protection for employees' privacy equivalent to the level of protection provided by the above mandates.[472]

3. Opinion Letters. Employers who decide to adopt policies containing additional provisions designed to provide greater protection than the model provisions promulgated by the DOL may contact the DOL for an opinion as to whether the policies comply with the Act. The representative of the employees, pursuant to Section J, may also request an opinion. The DOL will provide informal and formal opinion

471. *Id.*

472. In Europe, the European Commission, the executive branch of the European Union, sets out "standard contractual clauses" that employers in countries outside Europe can adopt in order to comply with the European standards. ARTICLE 29, OPINION 8/2001, *supra* note 252, at 26.

letters.[473] A fee to cover administrative expenses will be charged for each opinion letter requested. The fee will be set by the DOL but will be no less than the equivalent amount of $100.00 in 2010 adjusted for inflation.

4. Best Practices. The DOL will make recommendations as to best practices for employers on its Web page. The DOL will also provide compliance guidance on the Web[474] and via the DOL phone hotline.[475]

5. Education. The DOL will, through its web page and presentations at public venues, such as public libraries, educate the public about the privacy issues raised by employer technological monitoring.

6. Resolution of Disputes. The DOL will use procedures similar to those used under FLSA and for retaliation claims to resolve disputes arising under the Act. The DOL will investigate disputes and issue notices of determination and, when a violation is found, an order, including cease and desist orders, reinstatement orders, and orders for payment of back wages and damages.[476] The DOL must issue a notice of determination within sixty days of the filing of a claim with the DOL. A party who wishes to contest the notice of determination must file a request for an administrative hearing according to procedures analogous to those used in retaliation claims. The time limits and resultant hearing will also be conducted in accordance with those procedures.[477] The hearing must be conducted within thirty days of the filing of the request for an administrative hearing. A party who wishes to appeal the administrative law judge's recommended decision may petition for review with the Administrative Review Board (ARB) by following time-limits and procedures analogous to those used in retaliation claims.[478] The ARB will issue a final binding decision within the ninety day time limit applicable to retaliation claims.[479]

---

473. The DOL, Wage & Hour Division currently issues unofficial and official interpretations. *See* Final Rulings and Opinion Letters, http://www.dol.gov/whd/opinion/opinion.htm.

474. For an example of the current compliance guidance provided by the DOL, Wage & Hour Division, see Compliance Assistance - Laws of the Wage and Hour Division, http://www.dol.gov/whd/regs/compliance/ca_main.htm.

475. The DOL, Wage & Hour Division currently uses a help line, 1-866-4USWAGE, *see id.*

476. Herbert, *supra* note 449, at 6. Under the FMLA and the FLSA, the DOL receives, investigates, and attempts to resolve complaints of violations. *See* http://www.dol.gov/esa/whd/regs/statutes/fmla.htm#SEC_107_ENFORCEMENT; FLSA § 6 & 7, 29 U.S.C. § 206 & 207.

477. *See* Herbert, *supra* note 449, at 8 (discussing hearing in front of administrative law judge).

478. 29 CFR § 24.8; Herbert, *supra* note 449, at 9 (discussing review procedure).

479. *Id.* The ideal process would be an efficient binding agency adjudication process similar to that used by the California Department of Industrial Relations in wage and hour cases. The DOL's adjudicatory process most closely resembles this ideal. *See infra* notes 564-567 and accompanying

7. Investigative Authority. "The Administrator, or [the Administrator's] designated representatives may investigate and gather data regarding . . . conditions and practices of employment in any industry subject to this [Act], and may enter and inspect [and make copies of] . . . records, question . . . employees, and investigate . . . facts, conditions, practices or matters as [the Administrator] deems necessary or appropriate to determine whether any [employer] has violated" this Act or to "aid in the enforcement of" this Act.[480] State and local agencies may be collaborated with in the same manner as described in section 11(b) of the FLSA.[481]

8. Subpoena Power. The DOL "may issue a subpoena to compel [a] witness to appear or a subpoena duces tecum to compel the witness to appear and produce relevant book, record, document, data, or other object."[482] "If a person refuses to obey a subpoena [or subpoena duces tecum, a federal district court of competent jurisdiction] "may issue to the [witness] an order requiring that [witness to] appear and give evidence or otherwise produce documentary evidence requested by the department regarding the matter under investigation."[483]

9. Staffing. The Administrator will staff the office in the same manner as is required by subsection (b) of section 4[484] of the Fair Labor Standards Act. The DOL will hire at least one expert in technology, at least one expert in the area of privacy, and at least one expert in labor relations.[485]

10. Regulations. "The Secretary shall, within [six] months after the date of enactment of this Act, issue regulations to carry out this Act."[486]

---

text. Some commentators have suggested, however, that agencies cannot issue self-enforcing orders. *See, e.g.*, Marcia L. McCormick, *The Truth is Out There: Revamping Federal Antidiscrimination Enforcement for the Twenty-First Century*, 30 BERKELEY J. EMP & LAB. L. (2008) available at http://ssrn.com/abstract=1142979. If the described adjudicatory process is, thus, likely to lead to numerous appeals to court and long delays, as a practical matter, then an informal recommendation process similar to that used under the FMLA could be substituted for the adjudicatory process.

480. 29 U.S.C. § 211(a) (2009).

481. 29 U.S.C. § 211(b).

482. N.D. CENT. CODE § 14-02.4-22(2); 29 U.S.C. § 211(a) (2008).

483. N.D. CENT. CODE § 14-02.4-22(3).

484. 29 U.S.C. § 204.

485. *See* McCormick, *supra* note 479 (discussing use of experts in new agency to enforce Title VII).

486. Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 14 (1993).

O. Remedies

1. Administrative Claim or Civil Action. Any employee "whose rights under this [A]ct have been abridged,"[487] including by a failure of an employer to adopt a policy in compliance with this Act or by the failure of an employer to comply with the provisions of a policy adopted in compliance with this Act,[488] may file a claim with the DOL or "file a civil action"[489] "against the employer in any Federal or State court of competent jurisdiction."[490]

Any employee who refuses to be subject to technological monitoring which is inconsistent with an employer's written policy adopted pursuant to this Act and is terminated or otherwise disciplined for refusing the monitoring may file a claim with the DOL or "file a civil action" "against the employer in any Federal or State court of competent jurisdiction."[491]

2. Damages. Any employer who violates this Act is liable for actual damages incurred by the employee. Compensatory damages for a single violation may not exceed[492] the equivalent of $20,000 in the year 2010, adjusted for inflation. Additionally, an employer who violates this Act is liable to the affected employee for an amount equivalent to "any profits made . . . as a result of the violation."[493]

3. Equitable Relief. An employee is entitled to equitable relief, including mitigation or removal of any discipline imposed, reinstatement, promotion, back pay, and lost benefits.

4. Injunctive and Declarative Relief. "Any employer that commits, or proposes to commit, an act in violation of any provision of this Act may be enjoined therefrom by any court of competent jurisdiction."[494]

5. Punitive Damages. An employer who engages in willful repeat violations of the act is liable for punitive damages.[495]

---

487. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 8(b).

488. This section is intended to establish a claim for violation of the Proposed Act when an employer fails to comply with provisions required by the Proposed Act. However, in order not to discourage employers from adopting policies with greater protection than that provided for by the Proposed Act, this section is not intended to establish a claim for violation for failure to comply with additional provisions, beyond those required by the Proposed Act, that are provided for in an employer's policy.

489. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 8(b).

490. S. 984, at § 12(c)(2); Schwartz, *supra* note 25, at 944 (discussing how without a private cause of action, "there is likely to be significant underenforcement of privacy interests").

491. Kim, *supra* note 160, at 676 ("My central argument here is that any meaningful protection of employee privacy requires limitation of an employer's power to fire at will.").

492. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. §2711 (d)(3)(A) (2000).

493. Blackowicz, *supra* note 37, at 107.

494. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 8(c).

6. Attorneys Fees. "If the prevailing party in a civil action is the plaintiff [employee], the court [must] award the plaintiff court costs and a reasonable attorney fee."[496]

7. Representative Suit. The DOL may bring a civil action on behalf of an employee in the manner described in paragraphs 1-6. All "sums recovered" "on behalf of an employee"[497] "must be held in a special deposit account"[498] and must be "paid to the employee [or employees] affected" by the violation.[499] "Any such sums not paid to an employee because of inability to do so within a period of three years shall be" deposited into the Treasury of the United States and will be "credited to a separate nonlapsing appropriation to the"[500] DOL for use by the DOL, Office of Privacy.

8. Affirmative Defense. An employer has a full defense to any claim for failure to mitigate if it has taken the following actions.

a. Prior to disciplining the employee, the employer provided the employee with a written statement of what level of discipline would have been imposed prior to mitigation.

b. The statement describes the manner in which the private nature of the conduct was considered by the employer in determining the appropriate discipline.

c. The statement describes the level to which the discipline was mitigated as a result.

This defense does not apply to a claim of failure to consistently enforce a policy adopted in compliance with this Act or to consistently discipline infractions thereunder.

P. Civil Penalties

The DOL "may levy a civil penalty against" any employer the DOL "finds to be in violation of" this Act, "in an amount not more than $10,000"[501] as of 2010 adjusted for inflation, after a hearing.[502] To determine the amount of the penalty, the DOL must "take into account"

495. *See* Blackowicz, *supra* note 37, at 107.

496. COLO. REV. STAT. § 24-34-402.5(2)(b)(I).

497. 29 U.S.C. § 216(c).

498. *Id.*

499. The Family and Medical Leave Act of 1993 §107, 29 U.S.C. §2601 (2008), *available at* http://www.dol.gov/whd/regs/statutes/fmla.htm.

500. 29 U.S.C. § 216(c); CONN. GEN. STAT. ANN. § 31-69a(b).

501. Privacy for Consumers and Workers Act, S. 984, 103d Cong. § 16(C)(1) (1993).

502. CONN. GEN. STAT. ANN § 31-48d(c).

"the gravity of the violation" and "the previous record of the employer's compliance" or noncompliance with the Act.[503]

The DOL will hold the hearing and collect the penalty "in the same manner as is required by subsections (b) through (e) of section 503 of the Migrant and Seasonal Agricultural Worker Protection Act (29 U.S.C. 1853) with respect to civil penalties assessed under subsection (a) of such section." The penalty assessed will be held by the Treasury of the United States and will be "credited to a separate nonlapsing appropriation to the"[504] DOL for use by the DOL, Office of Privacy.[505]

Q. Nonwaiver of Rights

"The rights and procedures provided by this Act may not be waived by contract or otherwise, unless such waiver is part of a written settlement agreed to and signed by the parties to a pending action or complaint under this Act."[506]

R. Liberal Construction

This statute is intended as a remedial statute and should be construed liberally in favor of protecting employees' privacy.

S. Minimum Standards

"The provisions of this [Act] shall not be deemed to be an exclusive remedy and shall not otherwise limit or bar any person from pursuing any other remedies available under any other law, state or federal statute, or the common law."[507]

T. Statute of Limitations

No claim may be filed or "action may be commenced more than" three "years after the date –

(A) the employee . . . knew of, or

(B) the employee . . . could reasonably be expected to know of, the alleged violation."[508]

503. S. 984, at § 12(a).
504. CONN. GEN. STAT. ANN § 31-69a(b).
505. *Cf.* 29 U.S.C. § 1853(e).
506. S. 984, at § 16(D).
507. DEL. CODE ANN. tit. 19, § 705(d) (2008).
508. S. 984, at § 12(c)(3)(B).

VI. EXPLANATION OF PROPOSED SOLUTION: CONSIDERATIONS INVOLVED IN DRAFTING THE ACT

This section, VI, discusses some of the major considerations that went into the choices underlying the language in the Proposed Act, which may not be apparent from the text of the Proposed Act. More minor considerations are included in the footnotes annotating the draft of the Proposed Act.

A. Short Title—Federal Legislation

The common law has failed to adequately address the problem of employer technological monitoring of employees.[509] Development of a case-by-case approach under the current default rules that provide little protection for employee privacy would be too slow to deal with the rapidly changing technology, even if it could provide some adequate level of protection.[510] It is, thus, preferable to address the problem in a timely manner and to change the existing default rules and the balance between employer and employee concerns through legislation.[511] Thus, the Proposed Act is for federal legislation that provides a floor of protection, permitting state counterparts to provide similar or more significant protections.

Several rationales suggest that federal legislation is necessary. First, the problems relating to technological monitoring are national, and even international, in scope, suggesting that some level of consistency and coordination between states is necessary. Electronic mail, for instance, passes easily from an employee in California to one in Kentucky. Federal legislation is the most effective way to obtain such consistency and coordination.[512]

Second, because employers are well-organized while employees generally are not,[513] state-by-state legislation is likely to be obtained at a

509. *See supra* note 18.

510. *Cf.* Herbert, *supra* note 35, at 470 (discussing how ad hoc guidance of court decisions under the Fourth Amendment provides inadequate guidance for public employers).

511. *But see* Corbett, *supra* note 18, at 96.

512. Gantt, *supra* note 37, at 411 ("First, state legislation would be insufficient because only federal legislation can address E-mail communications that cross state lines."); Corbett, *supra* note 18, at 117 (noting that "most commentators hold out little hope for state legislative solutions for reasons such as . . . the ill fit between law limited by state boundaries and technology that realizes boundariless communication").

513. With the potential exceptions of union-represented employees and those supported by the tobacco lobby.

slower rate over a more extended time period than federal legislation.[514] While several states have passed legislation addressing or pertaining to the problem, legislation directly addressing the problem has been proposed twice at the federal level. Continuing to press for federal legislation will ensure, if passed, that protections are obtained nationwide at an equivalent time.[515]

Third, states that desire to pass workplace privacy protections are more likely to do so once federal legislation is in place.[516] Often times, providing protections for employees on a state-by-state basis can cause "a race to the bottom." States perceive that employers will prefer to do business in a state that does not heavily regulate employers. States will thus be reluctant to regulate employers more heavily than other states do.[517] Additionally, some states may even adopt less restrictive rules than other states with the purpose of luring business to their states.[518] The oft-mentioned example of such state purpose is that of Delaware in the incorporation context.[519]

Fourth, a level of consistency provided by federal legislation benefits employers who desire to protect their employees' privacy.[520] Some employers already provide notice of monitoring, protect employees' personal data from breach, or take other measures designed

514. Corbett, *supra* note 18, at 117 (noting that "most commentators hold out little hope for state legislative solutions for reasons such as business groups' lobbying"); Evans, *supra* note 18, at 1147 (noting that despite a strong employer lobby at the federal level, "comprehensive federal legislation has been possible in the medical and educational fields under HIPPA and FERPA"). *But see* Schwartz, *supra* note 25, at 932-33 (arguing that federal law is likely to pass only after state laws "because of the slow and sometimes difficult process of enacting federal legislation").

515. Gantt, *supra* note 37, at 411 ("[S]tate legislative efforts are more likely to be undermined by the apparent ability of prominent corporations to stymie state legislation that strengthens protections from employee privacy interests.").

516. *See* Schwartz, *supra* note 25, at 933 (discussing how "state law makers will act in reaction to federal activity when it occurs, and a process of experimentation, drawing on involvement by advocacy groups and other stakeholders, will continue").

517. Boehmer, *supra* note 18, at 812 ("The potential financial impact on a state due to lost business resulting from the enactment of such controversial legislation makes it unlikely that a comprehensive solution will be achieved in the states."); Porter, *supra* note 19, at 105 ("Furthermore, a federal statute would eliminate states having to compete for an employer's business."); Note, *Addressing the New Hazards of the High Technology Workplace*, *supra* note 375, at 1908-09 (discussing how some businesses warned they might leave the state of Massachusetts if the state adopted a law similar to the PCWA).

518. Wilborn, *supra* note 18, at 862 ("Attempted legislative action on the state level has been repeatedly blocked by company threats to move their business to a state without the proposed restrictions.").

519. Evans, *supra* note 18, at 1144 ("The law of corporations provides an example of this phenomenon—most corporations now incorporate in Delaware because of its lenient laws.").

520. *Cf.* Schwartz, *supra* note 25, at 923 (discussing how "omnibus laws . . . level the regulatory playing field").

to ensure a pleasant and productive work atmosphere for their employees.[521] When other employers use "sweatshop" type practices to achieve a short term gain over these employers, those employers already engaging in sound monitoring practices are disadvantaged. Ensuring that all employers must meet some minimum guidelines tends to level the playing field for the employers who are looking toward long-term sustainability of the company and following sound monitoring practices on their own initiative.

Fifth, to some degree, federal legislation minimizes the administrative burden on employers. Rather than needing knowledge about widely divergent practices in different states, some of which may deviate atypically from the norm,[522] employers will know the minimum obligations in all states.[523] Of course, federal legislation with a preemptive effect that does not permit states to pass higher standards would achieve the goal of minimizing the administrative burden on employers to a greater degree.[524] But the benefit of enabling states to adopt practices tailored to their own states,[525] of allowing experimentation in a rapidly evolving field (because of the rapidly evolving nature of the monitoring technology),[526] and of sharing resources[527] outweighs that higher level of administrative consistency.[528] Much has recently been written about the ultimate inability of federal schemes which preempt an entire area of employee protections from

521. *See* James J. Cappel, *Closing the E-mail Privacy Gap*, J. SYSTEMS MGMT., Dec. 1993, at 2 (discussing companies that place great emphasis on employee privacy in managing their e-mail systems); Schwartz, *supra* note 25, at 904 (listing companies calling for federal privacy regulation).

522. Such as Montana's "just cause for termination" requirement.

523. *See* Boehmer, *supra* note 18, at 812 ("Also this is an area in which nationwide uniformity is critical to aid business compliance without undue hardship."); Porter, *supra* note 19, at 105 (discussing how a federal statute "increases consistency between states" from which nationwide companies benefit by adopting "standardized rules."). *But see* Schwartz, *supra* note 25, at 904-05 (discussing how a coalition of companies seeks a broad privacy regulation on the collection of information but only if it includes broad preemption of state laws governing privacy).

524. Jeffrey M. Hirsch, *The Law of Termination: Doing More with Less*, 68 MD. L. REV. 89, 91 (2008).

525. *See* Corbett, *supra* note 18, at 117 & n.168 (noting that one commentator suggested passage of NEMA could serve as ''the foundation . . . for more expansive state . . . legislation'") (citing Frayer, *supra* note 103, at 874).

526. Schwartz, *supra* note 25, at 905, 928 (discussing how a privacy statute with strong preemption would negatively impact "experimentation in . . . state sectoral laws" and the statute itself would "ossify"); Cynthia L. Estlund, *The Ossification of American Labor Law*, 102 COLUM. L. REV. 1527, 1574 (2002).

527. Schwartz, *supra* note 25, at 944 (discussing how "limited resources" and advantages of collaboration support "joint federal-state governance").

528. *See generally* Benjamin I. Sachs, *Labor Law Renewal*, 1 HARV. L. & POL'Y REV. 375 (2007).

keeping pace with a rapidly changing workplace environment.[529] The anticipated related state laws, might, on the other hand, preempt tort causes of action for invasion of privacy. Workers compensation schemes provide an example of that type of preemption system as does the Montana Lawful Discharge Act.[530]

B. Purpose and Findings—Private Sector

The Proposed Act is applicable only to the private sector. Its provisions are tailored to the private sector and additional provisions that would be necessary for an act that also extends to the public sector are beyond the scope of this article. Significantly, if the Proposed Act is extended at any time to encompass public sector employers, it is necessary for the legislation to thoroughly document the problem addressed.[531]

C. Definitions

The definition of technological monitoring is purposefully broad to enable the statute to cover yet-to-be discovered technologies.[532] The broad definition has the related benefit of ensuring that employers will not simply turn to using methods of technological monitoring other than those addressed by the legislation. Thus, the Proposed Act errs on the side of overbreadth rather than underinclusiveness.

---

529. *See, e.g.*, Estlund, *supra* note 526.

530. *See* Andrew P. Morriss, *The Story of the Montana Wrongful Discharge from Employment Act: A Drama in 5 Acts, in* EMPLOYMENT LAW STORIES 237 (Samuel Estreicher & Gillian Lester, eds., Foundation Press, 2007).

531. Harper Jean Tobin, *The Genetic Information Nondiscrimination Act of 2008; A Case Study of the Need for Better Congressional Responses to Federalism Jurisprudence*, 35 J. OF LEG. (forthcoming) (explaining that, to extend jurisdiction to states, federal bills should express the intent to create remedies against states, require waiver of state immunity, and specifically enumerate remedies); Porter, *supra* note 19, at 106 (stating that Eleventh Amendment immunity will not likely be abrogated, preventing public employees from suing "state employers for money damages.").

532. *See* Wilborn, *supra* note 18, at 852 ("[T]o be effective, any federal statutory scheme must be adaptable to changes in technology. Any legislation which defines protection in terms of specific types of monitoring equipment will inevitably be rendered obsolete by newer employee-monitoring technology . . ."); Bindler, *supra* note 375, at 882-83 (suggesting that Congress should avoid defining the scope of protective legislation in terms of specific types of monitoring equipment). Such definitions inevitably render any monitoring legislation obsolete; rather the legislation should define "monitoring employers" in terms of the act of impersonal observation. *Id.* Boehmer, *supra* note 18, at 812 (If "device-specific" legislation is enacted, little will be accomplished). Employers will simply shy away from the regulated device and turn to other devices that may present even greater concerns. *Id.*

The definitions of employer and employee are also purposefully broad. The legislature might decide after further consideration to limit the definition by exempting employers who employ under a certain number of employees. But the rationale of the broad definition is that no employer is too small to take adequate protections to safeguard its employees' privacy. The literature dealing with defining employees is a complicated topic in its own right. The rationale behind the broad definition is to safeguard the privacy of as many employed individuals as possible. The legislature might decide, however, to limit the scope of persons covered to a narrower category more traditionally defined as employees, such as by using the right-of-control test or otherwise excluding independent contractors.

D. Monitoring On-Duty Actions

The safeguards to ensure accuracy and reliability are limited in two major ways. First, the procedure to ensure accuracy is simply document review by the employee and the employee's agent. Second, the scope of the information that must be disclosed is limited to three categories of information. The European framework, and even the Workers Act, suggest a broader framework should be implemented to ensure the accuracy of all data collected. Additionally, several scholars have called for more comprehensive assurances of the accuracy of the collected information, such as requiring employers to provide summaries of the collected data[533] to employees or requiring arbitration to settle disputes over the accuracy of the data.[534] While more comprehensive protection is certainly a laudable long-term goal, given limited employer resources, use of summaries would be wasteful because the manpower used to compile the summaries could be better used to provide notice of the monitoring, consistently enforce the monitoring policy, document the behavior suspected when conducting monitoring without notice, and foster employee input into adoption of the policies.[535] Additionally, while a decision by a neutral third party, a data protection authority, or a court as to the accuracy or reliability of data would be more definitive, the resources expended in such proceedings do not warrant the added advantage over permitting the employee to place a response alongside the allegedly erroneous information.

533. Jacobs, *supra* note 37, at 878.

534. Boehmer, *supra* note 18, at 818.

535. Some employees may not be interested in the summaries. Rather, many employees will be interested in the data only when it is relied upon to make a decision which impacts them directly.

Moreover, the right to choose an agent to help review and contest records is intended to ensure that the employee can make sense of the material but also serves the larger goal of encouraging collaboration and self-governance in the workplace. A federal agency may have difficulty finding resources to spot-check employers, but permitting employees to review their information with assistance is likely to provide a relatively high level of enforcement.[536] The right is modeled on the *Weingarten*[537] right provided under the NLRA. The *Weingarten* right guarantees an employee who is suspected of wrongdoing to have a union representative or co-employee present during any investigatory interview, and the National Labor Relations Board has often extended the right to non-unionized employees.[538] While the requirement could be eliminated and the Proposed Act would still arguably provide a minimal level of satisfactory privacy protection, making sense of complicated data is often difficult for one employee.[539] Normally, having more than one mind helps in assessing information. Additionally, contesting information may be uncomfortable for one employee because an employer generally holds more power over the employee than the reverse. Having a co-employee or union representative stand with the employee makes it more likely that employees will use the process.[540] Indeed, some existing legislation provide for such an agent in the review process.[541]

E. Monitoring On-Duty Conduct without Notice

The Proposed Act, like other proposals, creates flexibility for employers by permitting technological monitoring, subject to certain safeguards, of on-duty employees without notice when the employer has

536. *Cf.* Catherine L. Fisk, *Union Lawyers & Employment Law*, 23 BERKELEY J. EMP. & LAB. L. 58 & n.2 (2002) (discussing how OSHA is under-enforced in non-union workplaces).

537. NLRB v. J. Weingarten, Inc., 420 U.S. 251 (1975).

538. Epilepsy Found. Of Northeast Ohio, 331 N.L.R.B. 676, at 677 (2000), *overruled by* IBM Corp., 341 N.L.R.B. 1288, 1290 (2004).

539. Aranda, *supra* note 441, at 539.

540. Aranda, *supra* note 441, at 539.

> In addition to the above, I would suggest that it would be highly beneficial to allow worker representatives to become involved in the exercise by individual workers of their rights under data protection laws (such as the right of access to, and rectification and cancellation of, their personal data.) Clearly, it is difficult for workers to make use of such rights on their own, not only because they are inevitably in a position of weakness when faced with the computing power enjoyed by employers, but also because many workers simply do not understand the processes to which their data is subjected.

Id.

541. 820 ILL. COMP. STAT. 40/5 (2008).

"reasonable grounds to believe"[542] certain infractions have occurred. It additionally permits monitoring of "an area [on the employer's premise] in which the"[543] infraction occurred. This provision permits employers flexibility to monitor even those employees who are not suspected of misconduct or who are off-duty but enter the area being monitored. An employer may need to do so, for example, in situations where someone is known to be smoking in a nonsmoking area[544] or stealing from a certain stockpile.[545]

Putting these provisions in the context of the entire Proposed Act is helpful. An off-duty employee who enters a monitored area under this provision will be monitored subject to the low level of safeguards provided for monitoring of on-duty conduct. But, otherwise, an employee who is off-duty and on the employer's premises can only be monitored when the employer "has reasonable grounds to believe that" the employee is engaging in conduct that will cause a significant concrete harm to the employer and only subject to the high level of safeguards provided for monitoring of off-duty employee's behavior,[546] or for use of the employer's equipment subject to the intermediate level of protection provided for such use.[547]

F. Monitoring On-Duty Communications

One of the safeguards an employer can implement when monitoring on-duty communications is requiring that any information collected via the monitoring be kept in confidence by the employee performing the monitoring or review of the gathered information. Some privacy protection regulations require that a privacy office or officer be established by each company, in part to ensure employees who perform monitoring or data review are adequately trained in the requirements of

542. Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. § 2711(c) (2000).

543. H.R. 4908, at § 2711(c) (2000).

544. *See, e.g.*, Montgomery Gen. Hosp., 122 Lab. Arb. Rep. (BNA) 949 (2006) (Coyne, Arb.).

545. Commentators criticized the Workers Act on these grounds:

> If notice needs to be given to employees who are not under suspicion, but who will be monitored, many complications are foreseeable. An example of this is a manufacturer who has reasonable suspicion that an employee is stealing merchandise. Although the employer can justify putting a hidden camera in the employee's area without informing the employee under suspicion, the Bill requires the employer to inform all other employees that may appear in the camera's range of the monitoring. It is reasonable to assume in many instances that the employee's friends will inform the suspect of the monitoring and the employer will not be able to discipline the wrongdoer.

Baxi & Nickel, *supra* note 97, at 146.

546. See *supra* part VI.I.3.

547. See *supra* part VI.I.4.

confidentiality,[548] and several scholars have endorsed this requirement.[549] While a privacy office or officer in each company is a laudable long-term goal, especially in light of the serious security concerns raised by leakage of certain information, confidentiality is not an across-the-board requirement of the Proposed Act, and employers are permitted flexibility in determining whether to adopt a policy requiring it and how to insure confidences are maintained.

G. Monitoring of On-Duty Communications without Notice

One of the safeguards that an employer can implement when monitoring on-duty communications without notice is mitigation of any discipline imposed as a result of the monitoring. The intent of the provision is that because the employees are not on notice they are being monitored and, thus, likely believe the communication is private from their employer, this private nature of the communication renders it less problematic than a publicly acknowledged communication would be. The intent, however, is not to leave employers wide open to claims by employees that an inappropriate level of discipline was imposed.[550] In other words, the safeguard does not impose a "just cause requirement" or a "proportionality" requirement. Thus, an affirmative defense is provided in relation to this safeguard.[551] As long as the employer mitigates the discipline imposed in light of the private nature of the communication and documents its actions, the purposes of the mitigation safeguard are met.

H. Monitoring Prohibited on Premises

The Proposed Act prohibits monitoring in areas where employees typically undress. Many people consider monitoring of people's private bodily parts to be a severe intrusion on privacy. The need to protect such privacy outweighs an employer's countervailing need to technologically monitor in such areas in certain limited instances, such as to identify the perpetrator of a theft. The employer can investigate

548. Some binding corporate resolutions require that a privacy officer or office be established by each company or a responsible employee be designated. ARTICLE 29, TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES, *supra* note 337, at 16; Wugmeister, *supra* note 337, at 485.

549. Several commentators have endorsed the idea of requiring "data protection officer." *See, e.g.*, Aranda, *supra* note 441, at 540.

550. Employees who are treated disparately or are disciplined for refusal to permit monitoring that is out of compliance with the adopted policy may bring claims that inappropriate discipline or an inappropriate level of discipline was imposed.

551. *See supra* part V.O.8.

such circumstances through alternative means such as stationing a security officer in the area or monitoring the entrance or exit to the area.

I. Monitoring of Off-Duty Behavior

The Proposed Act prohibits monitoring of employees who are off-duty and in secluded locations.[552] While more robust privacy protection would be provided by also restricting monitoring of on-duty behavior in secluded locations, employers whose employees work away from the employer's premise in secluded locations, such as customers' homes, may need to monitor their employees' on-duty behavior. For this reason, when an employee is working at a friend's house or other secluded location, the employee will be adequately protected by the safeguards applicable to monitoring of on-duty actions and communications.

The Proposed Act also prohibits monitoring off-duty employees for behavior that will potentially damage the company's reputation but has not resulted in customer or client complaints or cessation of business. While arbitrators and scholars are divided over whether harm to an employer's reputation can justify termination or other discipline,[553] nothing in the Proposed Act prohibits employers from disciplining, including terminating, an employee based on such behavior. Rather the Proposed Act simply prohibits monitoring for that purpose. The significant level of intrusion into an employee's right to privacy incurred by off-duty monitoring outweighs the employer's need to monitor based on a speculative harm to reputation.[554]

J. Employee Participation

Several scholars have noted the benefits to employees and employers of employee participation in "defining workplace" policies.[555]

552. *See supra* part V.I.2.

553. Hill & Delacenseri, *supra* note 42, at 151 ("Indeed, some arbitrators have viewed 'business reputation' as too nebulous a concept to be useful, although these arbitrators are in the minority.").

554. Yung, *supra* note 37, at 213 (noting employers' "amorphous" interest in reputation).

555. Kesan relies on microeconomic agency principle models to recommend that employees participate in "defining workplace e-policies." Kesan, *supra* note 18, at 326. Employee participation benefits employers because it increases the employees' commitment to the policy. Kesan, *supra* note 18, at 327. Employees benefit because it ensures their "point of view is heard and accommodated." Kesan, *supra* note 18, at 327. *See* Ford, *supra* note 160, at 154 (proposing that "procedural model imposing duties to provide information to workers and, above all, requirements of collective consultation" is a better solution than minimum rights legislation."); Note, *Addressing the New Hazards of the High Technology Workplace*, *supra* note 375, at 1915 (proposes modifying

While the protections offered by the Proposed Act would be significant even without employee involvement, employee involvement is important for at least two reasons. First, input from employees is more likely to result in a policy that appropriately safeguards employees' rights. When an employer alone is responsible for drafting the policy, there is a higher likelihood the policy will be biased toward the employer's need to monitor. Second, litigation may be less likely to result when employees feel invested in the development of the policy.

From the vantage point of ensuring employee participation and increasing enforcement, a system by which employees would gain the equivalent of union representation for the purposes of consultation would be preferable to that in the Proposed Act.[556] However, effectively implementing such a requirement would be an extensive endeavor that is beyond the scope of this article.

K. Maintenance of Records

Ideally, maintenance of records resulting from technological monitoring, as well as other records which contain identifiable information about employees, will be the subject of separate legislation, or perhaps a comprehensive scheme to protect employees' privacy. Indeed, some state and federal laws already require secure maintenance of a variety of different types of employment records.[557] Fully addressing the topic is beyond the scope of this article.

L. Disclosure of Information Collected

The disclosure limitations in the Proposed Act mirror those contained in the Workers Act. Other potential models[558] as well as some commentators[559] call for more restrictive disclosure prohibitions. These include limiting disclosure to only those with a need to know the

---

the PCWA to "guarantee some employee participation in monitoring system design and implementation").

556. *See* Aranda, *supra* note 441, at 537.

557. *See* Joseph J. Lazzarotti, *The Emergence of State Data Privacy and Security Laws Affecting Employers*, 25 HOFSTRA LAB. & EMP. L.J. 483 (2008).

558. MODEL ELECTRONIC PRIVACY ACT, *supra* note 122, at § 6(b) (limiting disclosure without the employee's consent to those with "a legitimate need for the information").

559. Blackowicz, *supra* note 37, at 105-06 (limiting disclosure to certain categories of people including supervisors who have a "valid business interest" in the information); Boehmer, *supra* note 18, at 818 (recommending that "access should be limited to a discrete group with the need to know" and that confidentiality procedures that will guarantee this in-house confidentiality should be mandated).

information. That limitation is provided under certain of the policies set out in the Proposed Act. But requiring it in all circumstances for all monitoring would reduce the flexibility provided by the Proposed Act and reduce the likelihood that employers would support passage of the Proposed Act. Requiring confidentiality in all circumstances places a considerable training burden on employers.[560] Additionally, in order to enforce it, the law might have to require discipline or other sanction of those employees who breach their duty of confidentiality.[561] Such a framework would add additional complexity to the Proposed Act. While such internal disclosure limitations may appear more realistic in the United States at a later time, an approach limited to restricting disclosure to third parties appears more likely to gain support at this juncture.

M. Anti-Retaliation Provision

The reach of the anti-retaliation provision is purposefully broad to encourage employees to advocate for and enforce their rights to privacy.

N. Responsibilities Designated to the Department of Labor

Delegating responsibility for enforcement of the Proposed Act to an administrative agency rather than solely to the courts 1) allows a more proactive approach, such as through education, opinion letters, and safe harbor policies; 2) likely reduces the financial costs to the parties who need not elect costly litigation and to the federal government administering the Proposed Act; and 3) permits decision makers with expertise in the area to be involved.

The responsibility for enforcement of the Proposed Act is placed in an existing agency because a new office, similar to the European data protection offices, that has responsibility for privacy issues generally would not likely be created as part of legislation targeted at addressing an employment issue.[562] Moreover, it makes sense to have an agency

560. *See* Boehmer, *supra* note 18, at 818. Binding Corporate Resolutions that provide adequate protection by European standards, for instance, require that employees be trained as to the policy before handling data. ARTICLE 29, TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES, *supra* note 337, at 16

561. Binding Corporate Resolutions that provide adequate protection by European standards, for instance, require that employees who mishandle data be sanctioned, usually by discipline. Wugmeister, *supra* note 337, at 485. This ensures "a policy is known, understood and effectively applied." ARTICLE 29, TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES, *supra* note 337, at 16; Wugmeister, *supra* note 337, at 485.

562. Additionally, while a sub-department with expertise in workplace issues of an agency devoted to privacy issues might be ideal, it may be more realistic in terms of funding and political

that already has expertise with workplace issues administer the Proposed Act because privacy protections available in other contexts are often absent in the employment context.[563]

Among the potential agencies, the DOL is most likely to use an enforcement mechanism that is well suited to protecting employees' right to privacy. The agency already has in place mechanisms to provide compliance guidance, opinion letters, recommendations as to resolving disputes, and adjudicatory administrative hearings. While filing a claim with the DOL permits an employee a low cost means to settle a dispute, filing with the DOL is not generally a prerequisite to filing in court. Thus, employees are provided the option of a court suit rather than agency dispute resolution should they so prefer. The two other federal agencies that currently provide such adjudication, the EEOC[564] and the NLRB, are not known for the efficiency of their processes.[565] And use of their processes is, in most instances, mandatory before proceeding to court.[566] Additionally, while the EEOC certainly has expertise in dealing with workplace policies and ensuring that they are implemented in accordance with the law, the focus of the statutes it implements is on invidious discrimination, which differs from the across-the-board minimum-level protections guaranteed by the Proposed Act. As a law guaranteeing minimum protections, it is more similar to those

---

will to place the responsibilities with the DOL. *See* Herbert, *supra* note 35, at 469-70; Evans, *supra* note 18, at 1145.

> The United States may not be ready for an agency with the same powers of registration and enforcement as the English Information commissioner, due to American aversion to regulation of businesses. Nonetheless, some agency or governmental department could be designated to fill an advisory role similar to that of the English Commissioner under the Data Act. Employers would appreciate a resource to turn to for guidance in these issues.

Id. *But cf.* Schwartz, *supra* note 25, at 926 (suggesting that establishing "a federal information privacy agency" might go further toward having Europe recognize the United States as providing adequate privacy safeguards than establishing a "federal omnibus law").

563. For this reason, the FCC, though having expertise in privacy issues, was not selected to administer the Act. One commentator suggests the FCC as a potential agency because of its experience regulating privacy rights related to personal information. Yung, *supra* note 37, at 218.

564. Yung, *supra* note 37, at 216-17 (suggesting that the EEOC would be a possible agency with the advantage of providing an administrative hearing).

565. Yung, *supra* note 37, at 217 (noting that "the EEOC has been characterized as a cumbersome roadblock to the timely resolution of discrimination claims"); Arlen Specter & Eric S. Nguyen, *Representation without Intimidation: Securing Workers' Right to Choose Under the National Labor Relations Act*, 45 HARV. J. ON LEGIS. 311, 322 (2008) (discussing delays at the NLRB).

566. There are exceptions in the NLRA context. An employee can, for instance, file a suit for breach of the duty of fair representation and a related breach of contract claim against the employer directly in court.

administered by the DOL, such as the FLSA. And while the NLRB certainly has expertise in interpreting workplace policies, in guaranteeing minimum workplace rights (such as to associate and organize), and in fostering employee participation and self-governance (even in non-union settings), the limitations of its processes focusing primarily on adjudication make it an unlikely candidate for the type of educational and compliance role that the agency administering the Proposed Act will need to take.[567]

O. Remedies

The Proposed Act provides for equitable, compensatory, injunctive, and declaratory relief. It does, however, cap compensatory damages in an effort to create a level of certainty for employers. It provides for attorneys' fees for prevailing employees so that employees will be able to obtain representation in such actions, which is particularly necessary in light of the damages cap.[568]

P. Civil Penalties

In order to somewhat defer the cost of creating the office of privacy and of administering the Proposed Act, the Proposed Act provides for civil penalties. The Proposed Act also provides for a fee to cover the administrative cost of providing an opinion letter.

Q. Nonwaiver of Rights

Because the Proposed Act is designed to provide a minimum level of adequate protection for employees' right to privacy from technological monitoring, the rights and procedures provided may not be waived except as part of the settlement of a pending proceeding. The nonwaiver provision extends to the procedures, in addition to the rights, because the procedures are part of the comprehensive effort to fairly balance the employees' right to privacy against employers' need to

567. Another option would be to provide for private arbitration of claims rather than agency resolution or court action. The merits of private arbitration in the employment context are hotly contested, and full consideration of the topic is beyond the scope of this article. *Compare* Estlund, *supra* note 138, at 209 ("By the same token, defusing the fear of litigation, as some seek to do through mandatory arbitration, threatens to stall the engines of reform.") *with* Theodore J. St. Antoine, *Mandatory Arbitration: Why It's Better Than It Looks*, 41 U. MICH. J.L. REFORM 783, 812 (2008) ("Overall, my conclusion is that, whatever may be the contrary appeal of the siren song of perfection, mandatory arbitration is indeed better than it looks.").

568. Porter, *supra* note 19, at 113.

monitor. The Proposed Act provides enough flexibility to permit employers to adopt different safeguards when monitoring for different purposes that a prospective waiver of rights is not necessary.

R. Liberal Construction

This section is simply to emphasize that the statue is remedial and to insure that courts interpret it liberally.

S. Minimum Standards

For reasons discussed above in Section A, the Proposed Act sets a floor rather than preempting other potentially applicable laws.

T. Statute of Limitations

A discovery rule is used because employees are unlikely to know at the time of the occurrence of many violations of the Proposed Act, such as surreptitious monitoring without reasonable grounds, failure to document reasonable grounds for monitoring, or failure to provide for a confidential review, that a violation has occurred.

VII. CONCLUSION

This article describes the problem of the lack of legal protection for employees' privacy from technological monitoring by their employers. It proposes federal legislation to address the problem. By proposing an actual draft of the legislation, the intent is to aid scholars and those involved in the legislative process to think more concretely about precise issues which must be addressed. The intent is also to ease passage of legislation, because an actual draft of legislation provides a clear starting point upon which to base legislation.

While passage of legislation protecting employees' privacy from employer technological monitoring may face an uphill battle, it is possible and should be done. The lack of current adequate protection is well-documented, and the failure of the Workers Act and the Notice Act should not deter another attempt at passage of legislation. Drafting legislation that effectively protects employees yet allows employers necessary flexibility is difficult. But the Proposed Act serves as an excellent starting point for drafting such legislation. While the greatest challenge facing passage of such legislation may be the current lack of interest groups pushing for such legislation and a corresponding lack of broad-based support for such legislation among the public, a wide range

of entities, as different as the ACLU and Microsoft, are joining scholars in the call for legislation that addresses the need for privacy in the face of rapidly changing technologies. The lack of protection from employer monitoring is relatively easy to explain to the public, and the new technologies might actually help by providing low-cost means, such as the Internet and electronic mail, to raise awareness of the problem. Whatever legislation is ultimately proposed, whether all encompassing legislation or a series of separate acts addressing the interrelated privacy problems, the hope is that employees will not be left out.