INDUSTRIAL JUSTICE: PRIVACY PROTECTION FOR THE EMPLOYED

*Ariana R. Levinson**

> "Every legal structure has a central point on which all individual rules rest and from which all legal emanations proceed. In civil law, the central point is property. In labor law, humanity."[1]
>
> "Beggars can't be choosers."[2]

As the nineteenth century drew to a close, Samuel Warren and Louis D. Brandeis proclaimed that technological change necessitated new protections for the right to privacy. Today, new protections for the right to privacy are called for once again because, in the American workplace, technological change continues unabated and little privacy is afforded employees from employer monitoring via such technology. Moreover, employers are disciplining and terminating employees based on information uncovered through monitoring. Recently, many employees have been disciplined and terminated for activities such as off-duty blogging and using e-mail for personal reasons while at work. Employers have even relied on data from global positioning systems to discipline drivers and other employees.

This is the first academic article in over thirty years to provide a detailed review of labor arbitration decisions governing the right to privacy from employer monitoring. The Article uses the decisions on employee privacy and technologies, such as GPS, e-mail, and the Internet, as a springboard to propose privacy protections in the non-union private sector workplace. Thus, the Article fills a gap in the academic literature. The framework suggested provides the greatest protection for off-duty behavior, intermediate protection for on-duty expression of thought, such

---

* Assistant Professor, University of Louisville, Louis D. Brandeis School of Law; J.D., University of Michigan Law School. The author thanks Andrew Petti for his consistent support of this project.

[1] HUGO SINZHEIMER, DAS PROBLEM DES MENSCHEN IM RECHT (1939), reprinted in 2 HUGO SINZHEIMER, ARBEITSRECHT UND RECHTSSOZIOLOGIE 53, 61 (Otto Kahn-Freund and Thilo Ramm eds., 1976) (quoted and translated by Matthew W. Finkin, *Menschenbild: The Conception of the Employee as a Person in Western Law*, 23 COMP. LAB. L. & POL'Y J. 577, 620 & n.256) (2002) ("Jede Rechtsordnung hat ein Zentrum, auf das alle Einzelregelungen bezogen sind und von dem alle Einzelbefugnisse ausstrahlen. Dieses Zentrum ist im bürgerlichen Recht das Eigentum, im Arbeitsrecht das Menschentum.").

[2] This phrase is an American adage.

as through computer usage, and baseline protection for on-duty actions. It could be implemented through legislation of minimum employee privacy rights or mandates for employers to adopt safe-harbor policies.

INTRODUCTION 612
I. THE PROBLEM: NEW TECHNOLOGY CREATES PRIVACY ISSUES FOR EMPLOYEES 615
II. A BASIC AND BRIEF EXPLANATION OF PRIVACY 618
III. IN THE UNITED STATES, EMPLOYEES HAVE VERY LIMITED PROTECTION OF THEIR RIGHT TO PRIVACY 619
A. *Common Law Provides Only Limited Protection for the Privacy of Employees Whose Employers Conduct Surveillance of Their Behavior* 619
B. *Additional Statutory Protection for Employees' Right to Privacy is Generally Piecemeal* 620
IV. PROPOSALS TO ADDRESS THE PRIVACY ISSUES RESULTING FROM EMERGING TECHNOLOGY 623
A. *Professor Selmi Proposes a Dualistic System of Protection with a Nearly Absolute Right to Privacy While Off-Duty and Almost No Right to Privacy in the Workplace* 623
B. *Professors Gely and Bierman Propose Modifying State Legislation to Protect Blogging* 627
C. *Professor Rustad and Sandra Paulsson Propose a Federal Law Governing Monitoring of Computer Use Based on European Insights* 629
V. THE BACKDROP OF PRIOR PRECEDENT: LABOR ARBITRATION DECISIONS PROVIDE A LONG-STANDING, UNIQUELY AMERICAN PRECEDENT FOR ADDRESSING WORKPLACE PRIVACY ISSUES 630
A. *Professor Craver's 1970's Review of Arbitration Decisions Addressing Employer Monitoring of Employees and His Proposals for Adequate On-Duty Privacy Protections Serve as Background for Developing Workable Privacy Protections Based on Present Day Arbitration Decisions* 631
1. Polygraph Exams 632
2. Searches 633
3. Surveillance 634
B. *Professor Summers's Discussion of the Privacy Protections Provided for Off-Duty Behavior Provide Further Background for Developing Workable Privacy Protections Based on Labor Arbitration Decisions* 635

VI. RESEARCH METHODS 637
VII. FINDINGS AND CONCLUSIONS: THE LAW OF THE SHOP RECOGNIZES THAT EMPLOYEES HAVE A RIGHT TO PRIVACY 639
A. *Creative Yet Practical Means, Such as Minimal "Floors" of Privacy Protection or Safe-Harbor Policies, Can Be Used to Mimic Forbidding Employers from Unilaterally Imposing Policies that Invade Privacy Without Bargaining with the Union* .. 641
B. *Some Limits on Employer Conduct Generally Recognized by Arbitrators Might Serve as a Starting Point for Developing Minimal Privacy Protections or Safe-Harbor Policies* 643
1. Reasonable Rules 643
2. Notice 644
3. Thorough Investigation 644
4. Disparate Treatment 644
5. Progressive Discipline 644
6. Mitigating Circumstances, Including Seniority ... 645
7. Severity of Discipline Fits Infraction 646
C. *Arbitral Concepts Particular to Protecting Employees' Right to Privacy and to be Free of Technological Monitoring Can Serve as a Starting Framework for Regulation or Safe-Harbor Policies* .. 646
1. Affirmative or Negative Right to Privacy 647
a. Affirmative Right to Privacy for Off-Duty Behavior 647
b. Affirmative Right to Privacy for On-Duty Behavior 649
2. Monitoring of Employees' Actions While on Duty 651
a. Open Monitoring of Employees' On-Duty Conduct 651
b. Surreptitious Surveillance of On-Duty Conduct 654
c. The Quality of the Evidence 656
3. Monitoring of Employees' Computer Usage 657
a. Personal Use of Company Computers 658
b. Right to Privacy When Using Computer for Personal Reasons 660
c. Prohibited Types of Personal Use of Company Computers 662
d. Limiting Personal Use of Computer 666

e. Open Monitoring of Computer Use 668
f. Surreptitious Monitoring of Computer Use .. 670
g. Discipline for Computer Use 675
4. Off-Duty Behavior 676
a. Disciplining for Off-Duty Conduct 676
i) *Examples of Significant Concrete Harms* 677
ii) *Examples of Insufficient Harms* 681
b. Monitoring Off-Duty Behavior 681
c. Monitoring the Employer's Property on the Employee's Property 685
D. *Adequate Remedies for Violation of Protections Should Include the Safeguards Suggested by the Arbitration Decisions and Additional Sanctions* 686
E. *Some Level of Privacy Protection Must Be a Nonwaivable Right* 686
CONCLUSION 687

INTRODUCTION

Each employee is a human with private thoughts, private communications, and a private life. These remain as dear to the employee the moment after the employee steps into the workplace as the moment before. Yet if the employee needs the job, perhaps to pay the rent, feed her children, maintain a residence near her elderly parents, or even maintain her status in the community or her sense of self, then the American employee must, to a large extent, give up her privacy. The emergence of new technology has exacerbated this problem by providing new means of communication, blurring the boundary between work and private life, and providing employers with additional means of monitoring their employees.

Consider, for example, the case of Michael Smyth, whose employer terminated him for sending an electronic mail message (e-mail) to his supervisor that complained about management.[3] Despite management's promise that e-mails were private, would not be intercepted, and would not provide grounds for termination, the court upheld his termination.[4]

In another well-known decision, Robert Konop maintained a private website which was available only to restricted users who logged in with their individual usernames and passwords and agreed not to disclose the site's contents.[5] Most of these restricted users were his co-workers,[6] and

---

[3] *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 98–99 (E.D. Pa. 1996).
[4] *Id.* at 98.
[5] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872 (9th Cir. 2002).
[6] *Id.*

Konop posted remarks "critical of his employer" on his site.[7] Two co-workers who were authorized users permitted the Vice President to use their names in order to gain access to the site.[8] The court reasoned that the monitoring by the Vice President did not violate the federal Electronic Communications Privacy Act (ECPA) unless one of the co-workers had not actually used the website prior to providing the Vice President permission to log in with his username.[9]

Within the vast field of privacy, which ranges from Fourth Amendment rights to be free from unreasonable police searches and seizures, to the Constitutional right to an abortion, to tort suits by celebrities, only a small subset of esteemed academics has thought and written about the right to privacy in the workplace, even though it is the location that many people spend most of their waking-hours during their adult lives.[10] These scholars have attempted to define privacy;[11] they have discussed the difficulty of asserting workplace privacy rights in a legal system governed by at-will employment;[12] they have explored the overlap between the workplace and private non-work life;[13] they have discussed the relationship between the right to privacy and other human rights such as the right to speak freely, to associate with others,[14] and to be treated as an equal;[15] they have thought about the philosophical underpinnings of privacy as an individual or a group right;[16] and they have considered the differences between a collective union approach to asserting privacy

---

7 *Id.*

8 *Id.* at 873.

9 *Id.* at 880.

10 *See* Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035, 1036 (2006) ("Another curious aspect of the privacy literature, as well as the recent Congressional attention, is that it frequently ignores workplace issues, certainly one of the areas of greatest concern with respect to privacy encroachments.").

11 *Id.* at 1045.

12 *See* Anita Bernstein, *Foreword: What We Talk About When We Talk About Workplace Privacy*, 66 LA. L. REV. 923, 936 (2006); Charles B. Craver, *Privacy Issues Affecting Employers, Employees, and Labor Organizations*, 66 LA. L. REV. 1057, 1057–58 (2006); Pauline T. Kim, *Collective and Individual Approaches to Protecting Employee Privacy: The Experience with Workplace Drug Testing*, 66 LA. L. REV. 1009, 1024 (2006); Selmi, *supra* note 10, at 1036.

13 *See* Selmi, *supra* note 10, at 1037 ("[W]hat is sometimes called the boundaryless workplace now entraps employees far from the confines of the workplace and with virtually no compensating benefits.").

14 *See* Selmi, *supra* note 10, at 1036–37 ("[T]he issues surrounding privacy are representative of the broader transformation that has occurred in the workplace over the last three decades—one where the individual has triumphed over the collective, where solemnity of privacy has displaced the power of speech and collective action as a paramount workplace value . . . .").

15 *See* Bernstein, *supra* note 12, at 935 (discussing power and unions).

16 *See* Kim, *supra* note 12, at 1026 ("Although privacy has traditionally been characterized as a personal right, a number of considerations suggest that workplace privacy raises collective concerns."); Bernstein, *supra* note 12, at 934–35.

rights and an individual lawsuit approach.[17] None, however, have recently surveyed the law of the shop,[18] found in labor arbitration decisions, on the issue of employees' right to privacy from their employers' technological monitoring.[19]

This Article thus aims to fill a gap in the literature on workplace privacy by reviewing labor arbitration decisions on privacy and employer monitoring of employees via new technologies. The Article examines what the arbitration decisions say about whether and how employees' privacy should be protected. It uses these decisions as a starting point to suggest a workable framework for protecting employees' privacy from employer technological monitoring in the non-union private sector. The framework provides baseline protection for on-duty actions, intermediate protection for on-duty expression of thought, such as through computer usage, and the greatest protection for off-duty conduct.

Section I describes how new technology has exacerbated the problem of employer monitoring invading employees' privacy. Section II briefly defines privacy. Section III describes the lack of adequate legal protections to insulate employees' privacy from employer technological monitoring. Section IV summarizes various academic proposals to protect employees' privacy. Section V summarizes two previous academic articles addressing privacy protections provided by collective bargaining. Section VI describes the research methods used to ascertain the law of the shop governing employees' right to privacy from technological monitoring. Section VII discusses the arbitration decisions and proposes adequate safeguards for employees' right to privacy from technological monitoring.

---

17 *See* Kim, *supra* note 12, at 1010 ("This Comment asks what difference it makes to think about workers' rights under a collective as opposed to an individual rights model in a particular context: that of protecting employee privacy.").

18 The "law of the shop" commonly refers to the law governing a workplace pursuant to a collective bargaining agreement and arbitration decisions interpreting it. As put by Justice Douglas, a collective bargaining agreement "is more than a contract; it is a generalized code to govern a myriad of cases which the draftsmen cannot wholly anticipate . . . . It calls into being a new common law—the common law of a particular industry or of a particular plant," and "[a]rbitration is the means of solving the unforeseeable by molding a system of private law for all the problems which may arise . . . ." United Steelworkers of America v. Warrior & Gulf Navigation Co., 363 U.S. 574, 578–79, 581 (1960).

19 In 1977, Professor Charles B. Craver "canvass[ed] arbitration decisions dealing with each of the major security techniques used by employers . . . ." *The Inquisitorial Process in Private Employment*, 63 CORNELL L. REV. 1, 4 (1977). The techniques canvassed were employee interrogation, lie detector tests, searches of workers and their effects, and electronic surveillance of in-plant activities. *Id.* at 2.

I. THE PROBLEM: NEW TECHNOLOGY CREATES PRIVACY ISSUES FOR EMPLOYEES

The emergence of new technology, such as GPS devices, the Internet, and blogging, creates issues regarding employees' right to privacy from intrusion by employer monitoring. These issues are different in degree, if not in kind, from those with which employers have previously dealt. Professor Finkin states that employee use of e-mail and the Internet continues "to be one of the most vexing and controversial issues in the United States . . . due in part to the growing number of employees who use the computer at work and who connect to the Internet or access e-mail."[20]

Indeed, the use of technology in the workplace and, correspondingly, technological monitoring has been steadily increasing over the past decade. For example, the Privacy Foundation reports that the number of employees "who regularly use e-mail or Internet access at work" increased "from 30.5 million in January, 2000, to 40.7 million in January, 2001."[21] And the American Management Association (AMA) reports that in 1997, 13.7% of surveyed employers monitored computer files and 14.9% monitored e-mail while by 2007, the percentages rose to 43% for both types of monitoring.[22]

Professor Selmi discusses the role of technology in pushing privacy to become of greater importance to employees and a greater threat to employers:

> Added to the mix, technology unquestionably changed the nature of the workplace for many . . . . [W]hen e-mail replaced the telephone (or fax) as a common means of communication, it became easier for employees to feel a sense of privacy . . . . Technological advances have also enabled employers to act on their suspicions by providing them with more far-reaching means to snoop on their employees.[23]

Selmi emphasizes the hidden nature of surveillance: "[E]mployees today are often unaware of their employer's spying. Cameras can be hidden just about anywhere, technology can monitor keystrokes and

---

20 MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 115 (2d ed. Supp. 2007).

21 Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002).

22 *Id.* at 474; AMA/ePolicy Institute Research, *2007 Electronic Monitoring & Surveillance Survey*, http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.pdf (2007).

23 Selmi, *supra* note 10, at 1042.

movements throughout the workplace, and tracking devices can be implanted without easy detection."[24]

The scope of the problem, as illustrated by the scope of employer monitoring of employees, is widespread. The AMA's 2001 data indicated that 77.7% of surveyed employers recorded and reviewed "employee communications (or other activities) on the job by monitoring phone calls [or] voice mail, video recording . . . job performance, [or] monitoring . . . e-mail messages and . . . computer files."[25] The AMA's 2007 data indicate that 66% of employers monitor Internet connections, "12% monitor the blogosphere to see what is being written about the company," 10% monitor social networking sites, and 8% "use GPS to track company vehicles."[26] The Privacy Foundation reports that, of those employees "who regularly use e-mail or Internet access at work," fourteen million "are under 'continuous' surveillance . . . for their Internet access or e-mail usage."[27] This number does not include those who are spot-checked or investigated due to "reasonable suspicion" of some wrong-doing.[28]

And a substantial minority of employers appears to monitor their employees without notifying them of the monitoring. "Though more exact data are not available, a fair reading is that at least 12% of large or well financed employers (and perhaps a larger number of others) do not inform employees of their policies or practices regarding electronic monitoring."[29] Another survey reports that two out of every three "corporate workplaces have no policy requiring their employees to manifest consent to electronic monitoring or acknowledging their workplace monitoring activities."[30]

Selmi lists various legitimate employer interests "that often conflict with employees' desire for workplace privacy."[31] Employers assert "[c]oncerns about trade secrets, possible harassment suits, employee

---

24 *Id.*

25 Finkin, *supra* note 21, at 474 (surveying companies that employ about a fourth of the U.S. workforce).

26 AMA/ePolicy Institute Research, *supra* note 22.

27 Finkin, *supra* note 21, at 474.

28 *Id.*

29 *Id.* at 477; *see also* AMA/ePolicy Institute Research, *supra* note 22 (indicating that, of those monitoring computer activity, 10% don't know if employees are informed and 6% do not inform employees and, of those monitoring e-mail, 11% do not inform employees and 18% don't know if employees are informed).

30 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, 830 (2005) (citing *Survey: Most Employers Monitor E-mail, Internet Use*, SACREMENTO BUS. J., Oct. 8, 2003, *available at* http://www.bizjournals.com/sacramento/stories/2003/10/06/daily20.html.).

31 Selmi, *supra* note 10, at 1042-43.

theft, [and] efficiency in the workplace," to "justify keeping a watch on employees in a way that might infringe upon their privacy interests."[32]

In fact, the American Bar Association (ABA) has recently published two articles voicing concern about "big brother in the workplace."[33] One article begins with an example of an employer who requires those holding positions with access to a secure data center to have identification chips implanted in their arms.[34] The author concludes that "[a]lthough few companies go so far as to implant RFID [radio frequency identification] devices in employees, many institutions and individuals are using biometrics such as facial or iris recognition, fingerprint scans and satellite navigation technology to keep track of employees, children and even the elderly."[35]

The second article notes that "[i]t's becoming increasingly common for smart cards, fobs and other work-issued devices to be embedded with Global Positioning System chips, radio frequency identification and other technologies that allow employers to track every movement of their employees—both at work and away from it."[36] The article asserts that the longstanding "barrier between the workplace and the private lives of employees" is "starting to crumble."[37] Employers have more capability "to engage in" monitoring, and "more employee access to communications technology" complicates the issue.[38]

The issue of employees' workplace privacy has also received international attention. Europe includes the United States on its list of countries whose workplace privacy protections are inadequate to meet European privacy laws that include the fundamental right of respect for an employee's "private and family life," "home," "correspondence," and "communications."[39] Indeed, the types of situations implicating employees' privacy raised by the new technologies are myriad. Taxi-cab drivers protest GPS installation,[40] employees view pornography on computers at

---

32 *Id.* at 1043.

33 Jill Schachner Chanen, *The Boss is Watching*, A.B.A. J., Jan. 2008, at 48, 49; Margaret Graham Tebo, *Who's Watching the Watchers?*, A.B.A. J., June 2006 at 36.

34 *See* Tebo, *supra* note 33, at 36.

35 *Id.*

36 Chanen, *supra* note 33, at 49.

37 *Id.*

38 *Id.* at 51.

39 *See* 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.

40 *See* Colin Moynihan, *Rival Drivers' Groups Disagree on Likelihood of Taxi Strike Over New Technology*, N.Y. TIMES, Aug. 24, 2007, at B6; Alan Feuer, *Manhattan: Cabbies' Group Sues City*, N.Y. TIMES, Sep. 20, 2007, at B7; *cf.* Selmi, *supra* note 10, at 1044–45 (discussing how the introduction of GPS systems "has often proved controversial with many claiming that they infringe on employee privacy interests while demonstrating a lack of respect for employees").

work,[41] young teachers post "risqué" material on their Facebook pages,[42] and workers post statements about their employers on publicly-available blogs.[43]

II. A BASIC AND BRIEF EXPLANATION OF PRIVACY

Professor Summers provides a definition of privacy, based on Warren and Brandeis's seminal article, which serves as a good starting point for understanding privacy's precise nature.[44] According to Summers, privacy is a protection of an individual's "'inviolate personality,'" which includes "'the right to be let alone,'" "'seclusion of thoughts and sentiments,'" and the rights "to be free from 'spying into the privacy of domestic life,'" and "from revealing of 'facts relating to [one's] private life which [one] has seen fit to keep private.'"[45]

One important aspect of privacy is that of selective disclosure. Selective disclosure, or group privacy, is the concept "'that individuals want to keep things private from some people but not others.'"[46] "'Individuals typically tailor their behavior to the expected audience,'"[47] and when their behavior is exposed to "'a completely different audience'" than the one intended or expected, their "'expectations of anonymity and their autonomy in selecting to whom they will reveal parts of themselves'" are violated.[48]

---

41 *See* Finkin, *supra* note 21, at 483-84 (citing Garrity v. John Hancock Mut. Life Ins. Co., 18 IER Cases 981, *2 (D. Mass. 2002) (despite employer instructing employees "on how to create passwords and personal e-mail files," an employee had no reasonable expectation of privacy in the content of sexual e-mail messages and could be terminated)); Chanen, *supra* note 33, at 51 (employee terminated because a friend "regularly sent him e-mails containing pornographic images" despite the fact that the employee had "set his e-mail program to automatically delete the friend's e-mails").

42 *See* Ian Shapira, *When Young Teachers Go Wild on the Web*, WASH. POST, Apr. 28, 2008, at A01; *cf.* Chanen, *supra* note 33, at 50 (teacher fired after partner posted topless picture on photo-sharing website).

43 *Cf.* MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 290 (2d ed. 2003) (discussing instances where employers fired or sued employees for posts to homepages or chat boards).

44 *See* Clyde W. Summers, *Individualism, Collectivism and Autonomy in American Labor Law*, 5 EMPLOYEE RTS. & EMP. POL'Y J. 453, 467–68 (2001) (citing Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890)). For a comparative historical study of the meaning of privacy in Western law, see Finkin, *supra* note 1.

45 Summers, *supra* note 44, at 467–68 (quoting Warren & Brandeis, *supra* note 44 at 195–96.).

46 Daniel P. O'Gorman, *Looking Out For Your Employees: Employer's Surreptitious Physical Surveillance of Employees and the Tort of Invasion of Privacy*, 85 NEB. L. REV. 212, 243 (2006) (quoting Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1108 (2002)).

47 *Id.* at 243 (quoting Lyrissa B. Lidsky, *Prying, Spying, and Lying: Intrusive Newsgathering and What the Law Should Do About It*, 73 TUL. L. REV. 173, 237 (1998)).

48 *Id.* (quoting Lidsky, *supra* note 47, at 237).

III. IN THE UNITED STATES, EMPLOYEES HAVE VERY LIMITED PROTECTION OF THEIR RIGHT TO PRIVACY

Although most people "think they enjoy certain privacy protections when they are at work," they in fact do not.[49] Finkin, in his comprehensive survey of laws governing an employee's right to privacy in the United States, concludes:

> The United States has no comprehensive, coherent conception of how employer and employee interests in the collection, collation, use, and dissemination of personal data are best balanced. Rather, it is a skein of discrete pockets of legislation woven against the background of a common law that fails to fill in the gaps.[50]

Such limited protection means that an employee is entitled to virtually no expectation of privacy in the workplace. An employer can photograph an employee in compromising positions, track the quick stop an employee makes at home or at a significant other's,[51] and read an employee's e-mail, including messages containing personal information from family members. Such limited protection also generally means that an employer can pry into an employee's off-duty conduct such as smoking cigarettes or dating someone of a different race. Indeed, an employer can record an employee urinating in his secluded yard.[52]

A. Common Law Provides Only Limited Protection for the Privacy of Employees Whose Employers Conduct Surveillance of Their Behavior

Common law's limited protection of employee privacy has been well-documented.[53] The tort of intrusion upon seclusion requires that the complainant have a reasonable expectation of privacy and that any viola-

---

49 Craver, *supra* note 12, at 1069 (citing Richard S. Rosenberg, *The Technological Assault on Ethics in the Modern Workplace, in* THE ETHICS OF HUMAN RESOURCES AND INDUSTRIAL RELATIONS 141, 148 (John W. Budd & James G. Scoville eds., 2005)).

50 FINKIN, *supra* note 43, at 346. While most commentators agree that the laws in the United States do not adequately provide for employee privacy in the face of emerging technology, not all do. *See, e.g.*, O'Gorman, *supra* note 46, at 275 (arguing that the limited protection for invasion of privacy provided by the courts is appropriate in light of company's needs to surreptitiously monitor employees and to avoid litigation).

51 In some states, employers would be prohibited from taking disciplinary action based on the discovery that an empoyee's significant other is of the same sex, but in many they would not. *See* FINKIN, *supra* note 43, at 402-03.

52 *See* O'Gorman, *supra* note 46, at 248–49.

53 *Cf.* Rafael Gely & Leonard Bierman, *Social Isolation and American Workers: Employee Blogging and Legal Reform*, 20 HARV. J.L. & TECH. 287, 315–19 (2007) (discussing the limited ability of public policy exceptions to protect against termination of at-will employees for off-duty conduct).

tion of that expectation be highly offensive.[54] Typically, courts find that employees meet neither requirement. The reasonable expectation "can be dispelled by an employer's announcement that no such expectation exists." And "systemic measures taken in what business believes to be in its economic or administrative interest [are] rarely held to be capable of giving offense, at least by judges."[55]

Summers outlines a host of cases suggesting that "[m]ost courts . . . in balancing the employer's interest against the degree of intrusion place a heavy hand on the employers' side."[56] Two cases raise interesting issues of modern technology. One is the *Smyth* case mentioned in the Introduction. In the other, *Saldana v. Kelsey-Hayes Co.*, an employer investigated an employee collecting compensation for a work injury.[57] The employer, among other things, used a telephoto camera to take pictures through an open window of activity inside the employee's home.[58] "The court, without weighing the degree of intrusion against the employer's need, found no unreasonable intrusion of privacy because 'privacy is subject to the legitimate interests of the employer.'"[59]

Summers concludes:

> There is, of course, room for disagreement as to how much weight should be given to each of these interests, but for the courts, the employee's right of privacy is a hollow shell against the lead weight of the employer's claim to run his business as he pleases. The employee's sanctity of his home can be invaded by a telephoto camera or a fraudulent entry to simplify the employer's determining whether an employee is only pretending to be sick. An employer's desire to discover dissatisfied employees justifies intercepting an employee's private e-mail messages even when he has been repeatedly assured of privacy.[60]

B. Additional Statutory Protection for Employees' Right to Privacy is Generally Piecemeal

No comprehensive statutory scheme supplements the common law to provide protection for employees' privacy or even simply from em-

---

54 FINKIN, *supra* note 43, at 346.

55 *Id.*

56 Summers, *supra* note 44, at 469.

57 *See* Saldana v. Kelsey-Hayes Co., 443 N.W.2d 382, 383–84 (Mich. App. 1989).

58 *Id.*

59 Summers, *supra* note 44, at 469 (quoting *Saldana*, 443 N.W.2d at 384).

60 *Id.* at 475.

ployer monitoring.[61] Instead, a variety of federal and state laws offer only targeted and limited protections.[62] The statutes summarized herein are illustrative.

One federal statute, the Employee Polygraph Protection Act, protects employees from a specific type of privacy intrusion—intrusion by polygraph test.[63] The statute generally prohibits employers from requiring employees to take a polygraph test, and employees may not waive their right to this protection.[64]

Some states provide privacy protections from employer drug testing. These range from states that prohibit random drug testing to states that limit testing to safety-sensitive jobs to states that provide confidentiality protections for such testing.[65]

---

61 Finkin, *supra* note 21, at 473.

62 *See* Matthew W. Finkin, *Employee Privacy, American Values, and the Law*, 72 CHI-KENT L. REV. 221, 224 (1996) ("[T]he legislative response has varied from the occasional and piecemeal . . . to the non-existent. The latter may be explained for the most part by the politics of privacy, which pits organized business interests against a largely unorganized mass of individual workers."); Gely & Bierman, *supra* note 53, at 291 ("Over the past three decades, a majority of states have enacted statutes protecting a few specific employee off-duty activities."); O'Gorman, *supra* note 46, at 216 n.25 (describing state legislation "prohibiting certain surveillance of employees by employers"); Summers, *supra* note 44, at 478 ("Federal and state statutes, at best, give only freckled protection to employees who are unjustly discharged, they give no general recognition to the right of individual autonomy of workers.").

63 *See* 29 U.S.C. §§ 2001–09 (2000). A federal bill that would have protected employee's privacy, the Privacy for Consumers and Workers Act, S. 984, 103d Cong. (1993), never passed. The purpose was to prevent abuses of electronic monitoring through safeguards such as notice to employees about what activity will be monitored, restrictions on the ways employers use information obtained through electronic monitoring, and prohibition of certain types of monitoring. More recently, another bill, the Notice of Electronic Monitoring Act, H.R. 4908, 106th Cong. (2000), also failed to pass. It would have required employers to provide notice before monitoring e-mail and Internet use. The Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510–21, 2701–11 (2000), generally regulates electronic communications. But there are definitions and exceptions in both parts of the ECPA, the Wiretap Act, and the Stored Communications Act that might apply to employer monitoring of employees that generally exempt such monitoring. *See* Finkin, *supra* note 21, at 479–82, 484–89. One notable potential protection provided by the ECPA, however, is protection from disclosure of an employee's name to an employer from an entity providing electronic communications service to the public. *See id.* at 487–88.

64 *See* 29 U.S.C. §§ 2001–09 (2000); Summers, *supra* note 44, at 475–76 (citing 29 U.S.C. §§ 2001-09 (2000)); *see also* Selmi, *supra* note 10, at 1042 ("Other than the curious Polygraph Protection Act of 1988, which might be seen as affording some privacy by generally banning the use of polygraphs, there are few federal statutory protections . . . ."). But in public sector labor arbitrations, arbitrators apparently continue to discuss the appropriateness of relying on polygraph test results as evidence. *See* Jefferson County Sheriff's Office v. Fraternal Order of Police, Ohio Labor Council, Inc., 114 Lab. Arb. Rep. (BNA) 1508, 1515 (2000) (Klein, Arb.). Thus, while Professor Craver's 1970s position regarding polygraph exams has not generally been adopted, his observations may still be relevant in the arbitral context. Craver, *supra* note 19, at 40–43.

65 Summers, *supra* note 44, at 476.

Approximately thirty states protect against discipline for smoking off-duty and away from the employer's premises.[66] Some extend this protection to "off-duty use of lawful products."[67] "Two states, Connecticut and Delaware, have legislated to require notice of [electronic] monitoring."[68] New York prohibits employers from using a two-way mirror to surreptitiously observe employees in restrooms.[69] New York also prohibits employers from video recording in employee restrooms, locker rooms, and changing rooms.[70] Rhode Island prohibits both video and audio recording in restrooms.[71]

Two states, Illinois and Michigan, prohibit employers "from gathering or keeping a record of an employee's associations, political activities, publications, or communications of non-employment activities, unless authorized by the employee in writing or unless the activity occurs on the employer's premises or during working hours and interferes in the performance of the employee's or other employees' duties."[72]

In four states, California, New York, Colorado, and North Dakota, statutes protect against discharge or adverse action because of any lawful off-duty conduct.[73] The level of protection varies, with North Dakota protecting any activity "not in direct conflict with the essential business-related interests of the employer," and Colorado protecting only that activity which does not present "the appearance of . . . a conflict of interest."[74] The enforcement mechanisms also vary considerably.[75] In only one state, Montana, are employers required to show just cause for discharge.[76]

Finally, the National Labor Relations Act (NLRA) and collective-bargaining provide some privacy protections in the unionized workforce.[77] It is to the latter that this Article looks for guidance in

---

66 *See* Gely & Bierman, *supra* note 53, at 320; *see also* Selmi *supra* note 10, at 1052 ("A number of states have sought to protect off-work activities legislatively, often at the behest of the tobacco lobby which has sought to protect off-work smoking.").

67 Gely & Bierman, *supra* note 53, at 320.

68 Finkin, *supra* note 21, at 477–78, nn. 36–37 (citing CONN. GEN. STAT. § 31-48(d) (1999); DEL. CODE ANN., tit. 19, § 705(b) (2002 Supp.)).

69 *See* N.Y. GEN. BUS. LAW §§ 395–96 (2004 Supp.).

70 *Id.*

71 *See* R.I. GEN. LAWS § 28-6.12-1 (2005 Supp.).

72 Finkin, *supra* note 21, at 491, & n.112 (citing ILL. COMP. STAT. ANN. Ch. 820, § 40/9 (1999); MICH. COMP. L. ANN. § 423.508 (1995)).

73 *See* Gely & Bierman, *supra* note 53, at 320.

74 Gely & Bierman, *supra* note 53, at 321, nn.250–51 (citing N.D. CENT. CODE § 14-02.4-03 (2002); COLO. REV. STAT. § 24-34-403.(1)(b) (2008)).

75 *Id.* at 326.

76 *See* Summers, *supra* note 44, at 478; Gely & Bierman, *supra* note 53, at 315 (citing Montana Wrongful Discharge from Employment Act, MONT. CODE ANN. COMP. §§ (2) 39-2-901–915 (2005)).

77 *See* Finkin, *supra* note 21, at 498–501 (discussing NLRA protection against monitoring, including electronic monitoring, of protected activity). *But see* Register-Guard, 351

fashioning appropriate comprehensive protection for employee privacy from employer monitoring.

IV. PROPOSALS TO ADDRESS THE PRIVACY ISSUES RESULTING FROM EMERGING TECHNOLOGY

A number of academic proposals address the types of workplace privacy issues raised by newly emergent technology, and several include proposals related to employer monitoring of employees. This section briefly discusses three proposals that well-illustrate the spectrum of protections proposed. Professor Selmi proposes a dualistic system providing an extensive right to privacy while off-duty and a limited right while on-duty.[78] Professors Gely and Bierman propose activity-specific legislation to protect blogging.[79] And Professor Rustad and Sandra Paulsson propose federal legislation, modeled on European privacy protections, to protect employees' Internet and e-mail use at work.[80]

A. Professor Selmi Proposes a Dualistic System of Protection with a Nearly Absolute Right to Privacy While Off-Duty and Almost No Right to Privacy in the Workplace

Selmi proposes extensive, almost absolute protection of an employee's right to privacy when not at work.[81] He recommends that even if an employer requires an employee to complete work at home on company-provided equipment, the employer should not have "the right to look into that home."[82] He reasons that employees should not have to open their entire life to employer view because that would violate a central value of privacy—"the right to determine how much of one's self

---

NLRB No. 70 (Dec. 16, 2007) (employers can prohibit use of computers for "non-job-related solicitations," including union solicitations, unless the employer discriminates by banning only some "organizational notices").

78 *See* Selmi, *supra* note 10, at 1056.

79 *See* Gely & Bierman, *supra* note 53, at 303–14; *see also* 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 (2005) (proposing specific legislation to address monitoring via GPS).

80 *See* Rustad & Paulsson, *supra* note 30, at 895; *see also* Gail Lasprogata, Nancy J. King & Sukanya Pillay, *Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada*, 2004 STAN. TECH. L. REV. 4, 5 (proposing employers voluntarily honor fundamental privacy principles).

81 *See* Selmi, *supra* note 10, at 1046, 1052–53 ("It is one thing to give an employer broad dominion over its own workplace but quite another to extend that dominion wherever the employee goes.") ("The public policy tort should be extended to include all off-work activity, and require the employer to substantiate a legitimate business interest that outweighs the employee's interests in order to uphold a termination for off-work activity.").

82 *Id.* at 1046-47.

one wants to reveal to the world . . . ."[83] He proposes that not even a legitimate interest should entitle an employer to invade an employee's privacy outside of the workplace.[84]

Selmi additionally proposes that "any time an employer terminates an employee for lawful off-work activity, the employer must provide a compelling justification for its actions sufficient to override the employee's substantial interest in off-work autonomy."[85] He reasons that an employer could prevail by showing that an employee's conduct attributable to the employer "might bring public opprobrium" and damage the employer's reputation.[86]

But Selmi does not propose protecting an employee's right to privacy at work beyond that to be free of bodily invasion (or that obtained through contract).[87] He reasons that "an employee has been hired to work, and has no right to send private e-mails, view pornography, shop, blog, instant message, or talk on the telephone."[88] He concludes that when an employer tolerates such conduct, toleration does not give rise to a right to privacy, although it may give rise to an implied contract.[89]

He proposes this dualistic framework as most compatible with employment-at-will.[90] He reasons that to provide employees better workplaces would require "overhauling the entire system," whereas keeping employers "out of employee homes, out of city council meetings, [and] out of their employee's private lives" is fully possible.[91]

The proposal is a practical one in that the bright-line between on-duty activity and off-duty activity makes it relatively straightforward for employers to follow. As Selmi claims, the proposal is also congruent with employment-at-will to the extent that it permits the employer almost unlimited ability to monitor employees and their work and to discipline as the employer sees fit based on any information discovered. Such leeway enables management to efficiently manage.

---

83 *Id.* at 1046.

84 *See id.* at 1047. But he does include an exception that might in many instances swallow the rule. If an employee chooses to work at home, then the employee will have no privacy interest in the contents of any employer issued equipment used at home. *See id.* at 1048.

85 *Id.* at 1053.

86 *Id.*

87 *See id.* at 1043, 1045; *cf.* CYNTHIA ESTLUND, WORKING TOGETHER: HOW WORKPLACE BONDS STRENGTHEN A DIVERSE DEMOCRACY 158 (2003) ("It is no answer to say—as defenders of harassment law sometimes do—that 'the workplace is for work.' As we have seen, the workplace is for much more than work, both in the lives of individual workers and in the society as a whole. The law should not adopt as its motto a proposition that would so impoverish social life.").

88 Selmi, *supra* note 10, at 1043.

89 *See id.*

90 *See id.* at 1055 ("[T]his sharp distinction is most consistent with the employment-at-will rule . . . .").

91 Selmi, *supra* note 10, at 1056.

But the proposal is not congruent with employment-at-will to the extent it forbids employers from monitoring off-work activity and to the extent it places a heavy burden on employers to show a compelling justification for terminating an employee for off-duty conduct. These off-duty protections undermine the assertion that the proposal is consistent with employment-at-will. Instead, the proposal is grounded in the argument that pushing for such a dualistic approach is realistic. In other words, the underlying rationale is that it is easier to challenge the governing framework of employment-at-will when dealing with conduct outside the workplace than within.

Because workable privacy protections will, however, at least to some extent challenge the employment-at-will system, there is no practical reason to limit protections to outside the workplace. Rather, a privacy framework can satisfy employers' interests in monitoring and protect employees' privacy rights without providing the employer an absolute right to monitor in the workplace.[92]

Furthermore, privacy protections should be guaranteed in the workplace, even if doing so challenges the employment-at-will system. The workplace has become, as a practical matter, a place for more than work and should be, as an aspirational goal, a place for more than work. Expecting employees to do nothing at work, except work, and to give up their privacy when they do otherwise, is unrealistic. The American workplace has become "boundaryless."[93] Given the relentless American drive for efficiency, the internationalization of work, advances in technology, and the recognition that flexible work enables many to enjoy a more satisfactory work-life balance, the overlap between work and life is unlikely to cease. Many people work two, or even three jobs,[94] while others work much of the time on one.[95] Many people work at home and

92 *See* discussion *infra* Section VII suggesting possible frameworks based on a review of the arbitration decisions.

93 Selmi, *supra* note 10, at 1037.

94 *See* Belinda M. Smith, *Time Norms in the Workplace: Their Exclusionary Effect and Potential for Change*, 11 COLUM. J. GENDER & L. 271, 278 (2002) ("Between six and thirteen percent of all employees report having two or more jobs.").

95 *Id.* at 277 ("The United States is one of only two industrialized countries that has more than twenty percent of its workforce working fifty hours or more per week.").

conduct personal life at work.[96] And many employees use technology at work.[97]

Selmi recognizes that an employee's right to keep off-duty actions private from an employer is a fundamental value. But the proposal largely fails to recognize any view of an employee as a human in the workplace.[98] The proposal takes the position that "work-is-for-working," that employment at-will leaves little room for human dignity in the workplace, and that privacy is not a significant workplace value.[99] Selmi argues that blue-collar workers value family above work and likely place little value on workplace privacy.[100] Selmi himself concedes that "allowing employers such broad dominion over the workplace may functionally turn that workplace into the equivalent of a prison, where employee rights parallel the limited rights of prisoners."[101]

Yet humans do not cease being human in the workplace. Simply because certain groups of people, such as the working class or Gen X, purport to work in order to provide for themselves and their families or to enjoy time away from work,[102] does not mean that the workplace is not an appropriate place to protect privacy. These groups might place more value on work if employers treated them more humanely, including protecting their privacy. Additionally, many groups, such as professionals and older cohorts, do view the workplace as a venue for personal fulfillment.[103] While the debate over the purposes of work will doubtless rage eternally, in a democratic society, work should be for more than work. It should be a place for personal growth, a means to contribute to

---

96 Robert Sprague, *From Taylorisim to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace*, 25 J. MARSHALL J. COMPUTER & INFO. L. 1, 27 & n.219 (2007); Gely & Bierman, *supra* note 53, at 297 ("As Professor Patrick Schlitz has noted in the context of large law firms, current work-hour requirements may result in employees having little time for anything other than work.") (citing Patrick J. Schlitz, *On Being a Happy, Healthy, and Ethical Member of an Unhappy, Unhealthy, and Unethical Profession*, 52 VAND. L. REV. 871, 888–95 (1999)).

97 *See* Jeffrey M. Hirsch, *The Silicon Bullet: Will the Internet Kill the NLRA?*, 76 GEO. WASH. L. REV. 262, 274 (2008) ("A 2003 survey estimated that forty percent of all workers used the Internet or e-mail at work.") (citing *BLS Finds 55 Percent of Employees Used Computers at Work in October 2003*, Daily Lab. Rep. (BNA) No. 148, at D-24 (Aug. 3, 2005)).

98 *See* Selmi, *supra* note 10, at 1045.

99 *See id.* at 1045–46.

100 *See id.* at 1046 (citing MICHELE LAMONT, THE DIGNITY OF WORKING MEN: MORALITY AND THE BOUNDARIES OF RACE, CLASS AND IMAGINATION 30 (Harvard University Press 2000)).

101 *Id.* at 1056.

102 *See* Kathleen Brady, *From Law Student to Lawyer*, 36 STUDENT LAWYER 20, 22 (2008) ("For Gen Xers, work is seen as a means to an end. While they also enjoy the personal fulfillment that comes with a job well done, they expect to be paid for their efforts. Their reward is the freedom that money buys them to pursue outside interests.").

103 *See id.* ("For the Veterans, work fulfills a sense of duty and the only reward needed is knowing you've done your job well . . . . Boomers work for a sense of personal fulfillment and find their reward in the status that comes with hard work.").

society, and possibly a way to help the young. Providing privacy protections at work can help further these goals.[104]

Selmi bases his dualistic proposal on his understanding of the "nostalgic workplace"—that of the 1940's through 70's, where union density was at thirty percent, and other companies mimicked the union workplace because of the threat of unionization.[105] At work, "there was frequently no place to hide, no place for meaningful privacy."[106] But away from work, to the extent an employee's conduct "did not interfere with her employment, there might be a protectable privacy interest because that behavior was none of the employer's business."[107]

Yet a review of more recent labor arbitration decisions suggests a more nuanced approach that can serve as a starting point for a workable framework for protecting employees' rights to privacy both on and off the job.[108]

B. Professors Gely and Bierman Propose Modifying State Legislation to Protect Blogging

Professors Gely and Bierman view blogs as "virtual union halls where employees can connect, building social ties and reducing the isolation inherent in present-day American life."[109] While they do not frame the issue as one of privacy, they decry employers' ability to terminate employees for off-duty blogging.[110] They recommend amending state statutes that currently provide protection for specific off-duty activities, such as smoking, to incorporate protection for off-duty blogging.[111]

Gely and Bierman discuss how over the last century "monitoring and control of employee speech has increased considerably,"[112] "job se-

---

104 For instance, privacy protections may contribute to an employee's feelings of worth, enabling the employee to focus better on the work and to contribute to the employee's full capacity. Adequate privacy protections would likely include notice of related infractions, which would enable employees to avoid conduct harmful to the employer, or at a minimum, to learn from their mistakes and mature into more useful contributors. Of course, one employee is unlikely to be able to engage in personal growth, contribute to society, and help the young all at the same job. Many will be able to fulfill none of these goals on the job because a job is ultimately limited by the tasks that must be performed in order to produce the service or product. This is one reason that there should also be protection for off-duty conduct.

105 *See* Selmi, *supra* note 10, at 1039.

106 *Id.*

107 *Id.* at 1039–40.

108 *See infra* Section VII.

109 Gely & Bierman, *supra* note 53, at 288. Blogs are not truly analogous to a union hall, a space where not only members, but union officials and employees, conduct the affairs of a representative that has legal authority in the workplace.

110 *See id.* at 290–91.

111 *See id.* at 291.

112 *Id.* at 299.

curity has declined in tandem with falling levels of unionization,"[113] and harassment laws have created incentives for employers to censor speech and limit social interactions between employees.[114] They propose protection for off-duty blogging as an antidote to the social isolation resulting from these trends.[115] Protection would not, however, extend to blogs that disclose confidential information, to harassing speech directed toward a co-worker or supervisor, or to certain other kinds of abusive blogging.[116]

Gely and Bierman assert that the policy underlying some of the state statutes is that employees should be able to smoke "off-duty in return for their compliance with any employer rules prohibiting smoking while on the job."[117] They analogize: in return for the broad discretion "employers should have" to regulate computer usage at work, employees' use of their computers when off work should be protected.[118]

Their proposal would "address an important social concern in a limited and targeted manner."[119] It would also "involve easily administrable bright line rules."[120] Gely and Bierman's piecemeal approach is pragmatic, and likely to succeed in providing protection for a limited employee right to blog, a right that the law would not otherwise protect.

On the other hand, their proposal does not address an employee's right to privacy in the workplace; it does not protect against invasion of privacy through similar technology, such as Facebook or MySpace, a Google Doc, a wiki, or a yet-to-be-invented technology; and it does not provide protection from different types of technological monitoring of off-duty conduct.

For reasons discussed in response to Selmi's proposal, failing to protect against violations of privacy while on-duty is not a tenable path towards privacy protection.[121] Workers spend too much time at work to lightly give up such rights in return for off-duty protection. Additionally, a piecemeal approach, while pragmatic, is unlikely to adapt to changes in technology. Each time a new technology replaces an old one, further statutory amendment will need to be sought. On the other hand, a privacy policy that protects systemically, based on the nature of the inva-

---

113 *Id.* at 300.

114 *Id.* at 301.

115 *See id.* at 302–03.

116 *See id.* at 330.

117 *Id.* at 327.

118 *See id.*

119 *Id.*

120 *Id.*

121 *See supra* notes 87–104 and accompanying text.

sion rather than the specific technology, is likely to remain effective for a longer period of time.[122]

C. *Professor Rustad and Sandra Paulsson Propose a Federal Law Governing Monitoring of Computer Use Based on European Insights*

Professor Rustad and Sandra Paulsson survey European privacy laws, particularly those of England[123] and France,[124] governing the monitoring of employee e-mail and Internet usage. They note a "divergence in the value placed upon informational privacy" in the United States and Europe.[125]

Based on the insights from European law, Rustad and Paulsson propose a federal electronic monitoring act. The act would require employers to "formulate clear e-mail and Internet guidelines."[126] Employers would then be required to provide written notice of the program to employees before implementing a monitoring program. The act would also require that employees consent to the monitoring. Then the employer would have to provide electronic notice of monitoring each time an employee accesses a company computer system. "Finally, all employers . . . would be required to articulate legitimate business reasons for instituting a monitoring program," and would be entitled to monitor only for that reason.[127] Violations of these requirements would subject employers to "criminal as well as civil penalties, including compensatory as well as punitive damages," and employees in some cases would receive attorneys' fees and costs.[128]

One advantage of this system is that United States companies "would have, in effect, a safe harbor in cross-border communications with their European trading partners."[129] The authors also believe the measure would be a "first step in preventing U.S. companies from devolving into electronic sweatshops."[130]

The proposal includes some appropriate safeguards for employee privacy when using an employer's computer. Furthermore, the bright-line nature of the proposal—requiring notice and a legitimate business reason in all instances—should render it relatively easy for employers to

---

122 *See* discussion *infra* Section VII.C.
123 *See* Rustad & Paulsson, *supra* note 30, at 884–90.
124 *See id.* at 890–95.
125 *Id.* at 831.
126 *Id.* at 862.
127 *Id.* at 900.
128 *Id.*
129 *Id.* at 832.
130 *Id.*

comply with. Additionally, because the proposal is based on European laws, it has been shown to work in other regions.

Nevertheless, some will object that differences between the European legal system and traditions and those of the United States make implementation of any such system difficult, or even inappropriate. As the authors note, "Americans reflexively dismiss Europe as a clapped-out old continent—a wonderful place to visit but hardly the anvil of the future."[131] Indeed, it may be possible, as a review of the labor arbitration decisions below indicates, to develop a more nuanced and flexible approach to protecting employee privacy.[132] Such an approach might respond more adequately to employer concerns, while at the same time providing adequate safeguards for employees' privacy.

Moreover, Rustad and Paulsson's proposal addresses only computer usage but does not deal with other aspects of employer monitoring or informational privacy. As the authors recognize, it is designed as a starting point and not an end point "in developing a labor law that truly respects the dignity of the person."[133]

V. THE BACKDROP OF PRIOR PRECEDENT: LABOR ARBITRATION DECISIONS PROVIDE A LONG-STANDING, UNIQUELY AMERICAN PRECEDENT FOR ADDRESSING WORKPLACE PRIVACY ISSUES

One starting point for thinking about how to address employees' concerns is to look at how they are addressed in the union setting, where there is a long history of dealing with workplace disputes.[134] In 1960, the Supreme Court decided three cases, known as the *Steelworkers' Trilogy*, and established arbitration as the preferred dispute resolution mechanism in the unionized sector.[135] Since then, labor arbitrators have grappled with issues of emerging technology and potential resultant invasions of employees' privacy, whether couched in those terms or not.[136]

---

131 *Id.* (quoting *Old America v. New Europe*, ECONOMIST, Feb. 22, 2003, at 32.).

132 *See* discussion *infra* Section VII.

133 Rustad & Paulsson, *supra* note 30, at 904.

134 *See* Craver, *supra* note 19, at 7 ("[T]he arbitration process has provided the only major forum for weighing employer and employee interests in the security area, and has developed an analytical framework—adaptable in almost every employment context—for dealing with each of the major security techniques in use today.").

135 *See* Katherine V. W. Stone, *The Steelworkers' Trilogy: The Evolution of Labor Arbitration*, 180, 185, *in* LABOR LAW STORIES (Cooper & Fisk, eds. 2005) (discussing United Steelworkers of America v. American Mfg. Co., 363 U.S. 564 (1960); United Steelworkers of America v. Enterprise Wheel & Car. Corp., 363 U.S. 593 (1960); United Steelworkers of America v. Warrior & Gulf Nav. Co., 363 U.S. 574 (1960); and their impact on arbitration in the United States).

136 *See* Craver, *supra* note 19, at 4 (discussing how "[a] substantial body of arbitration case law has resulted" from challenges to "the reasonableness of particular searches or interro-

Academics have written about the privacy protections afforded to employees in the unionized setting, including protections from polygraph testing, searches, surveillance, discipline for off-duty activity, drug testing, and appearance codes.[137] Indeed, arbitrators have previously dealt with changes in technology and its impact on employees' privacy rights. Labor arbitrators make decisions about today's emerging technologies, such as GPS, e-mail, and Internet use against the backdrop of these long-standing precedents. Thus, some background on previous studies of privacy rights in the unionized setting is appropriate before discussing the specific findings of the decisions addressing today's emerging technologies.

This section will discuss the conclusions of Professors Craver and Summers about the types and level of protections afforded for employee privacy in the unionized workplace. These conclusions are representative of the general understanding of the protections provided; an understanding this Article aims to enhance by providing a detailed review of the concepts found in decisions addressing more recent technologies.

A. Professor Craver's 1970's Review of Arbitration Decisions Addressing Employer Monitoring of Employees and His Proposals for Adequate On-Duty Privacy Protections Serve as Background for Developing Workable Privacy Protections Based on Present Day Arbitration Decisions

Craver envisions arbitration over employer security techniques that raise privacy issues as "the balancing of employer interests in industrial efficiency against employee interests in privacy and personal dignity."[138] He states:

> It is generally recognized that employers are 'permitted by law and by contract to make such rules and regulations as are not inconsistent with the parties' collective bargaining agreement, and which are reasonably necessary for the smooth, efficient conduct of the business—even though at times they may impinge on the employee's personal privacy.' Nevertheless, some manage-

gations" and "there are now general areas of agreement among arbitrators as to the propriety of various security measures").

137 *See, e.g.*, Marion Crain, *Expanded Employee Drug-Detection Programs and the Public Good: Big Brother at the Bargaining Table*, 64 N.Y.U. L. REV. 1286 (1989); Pauline T. Kim, *supra* note 12; Michael J. Yelnosky, *What Do Unions Do About Appearance Codes*, 14 DUKE J. GENDER L. & POL'Y 521 (2007).

138 Craver, *supra* note 19, at 5.

> ment practices inevitably become so intrusive as to offend contemporary standards.[139]

Craver discusses how the right balance might consider factors outside the facts of the case. He points out that a solitary invasion of privacy might not appear overly intrusive, but, in certain cases, in conjunction with a course of conduct on the employer's part, it might be unreasonable.[140] He also mentions that employee conduct causes approximately one-third of all business closures, and that overly restricting an employer's ability to check for misconduct can lead to job loss for innocent employees.[141]

Craver discusses the application of these principles in three contexts: polygraph exams, searches, and surveillance.

1. Polygraph Exams

Craver makes a proposal regarding polygraph exams that bears on the issue of when e-mail surveillance should be permitted because both technologies monitor the thoughts of the employee. He suggests that three baseline considerations must be shown: serious employee misconduct is suspected; other investigative techniques have been attempted or are unworkable; and the employer has a reasonable suspicion that the employee has relevant information.[142] Furthermore, the scope of the inquiry should be as narrow as possible, and none of the responses to personal questions should be disclosed to management officials.[143] In addition, only the relevant answers should be disclosed, and only to appropriate persons.[144]

Four of the safeguards that Craver suggests—using a confidential reviewer, limiting the scope of information collection, monitoring based on reasonable suspicion, and using alternative methods prior to resorting to monitoring—are suggested by recent arbitration cases. The fifth protection that Craver suggests—monitoring only when serious misconduct is suspected—offers another protection that could be appropriately used as part of the range of protections when the conduct is off-duty or when monitoring of on-duty speech is surreptitious.

---

139 *Id.* at 5 (quoting Scheiber, *Tests and Questionnaires in the Labor-Management Relationship*, 20 LAB. L.J. 695, 697 (1969)).

140 *See id.* at 6.

141 *See id.*

142 *See id.* at 41.

143 *See id.*

144 *See id.* at 41–42.

2. Searches

Craver also summarizes his understanding of the arbitral authority governing searches.[145] This framework also bears on the issue of adequate protections from computer monitoring and on monitoring addressed to employees' on-duty actions, such as by GPS.

As to entrance and exit searches, and searches of specified personal property, such as large purses, Craver summarizes as follows:[146]

> Generally speaking, the security procedure must be one that is clearly established, fairly administered, and understood by all workers. If an arbitrator determines that an inspection rule has been arbitrarily applied, or has been promulgated in a manner which has not sufficiently apprised the workers of their obligations thereunder, he may order the rescission or modification of any disciplinary action taken against the employees who failed to cooperate in the search.[147]

Additionally, an employer may condition access to semi-private spaces, such as a locker, on the right to inspect the contents at any time.[148] Even without a rule, employers can examine an employee's personal property that is contained within employer property, such as a locker, when the employer has a reasonable suspicion that contraband or misappropriated company property is also therein. Craver points out that, "If no such presupposition exists, however, the immediate proprietary interest of the worker in his personal belongings should take precedence over the employer's ownership right, and a search should not be permitted."[149]

On the other hand, an employer does not have the right to "examine a worker's belongings that are not situated in a company container."[150] Mere presence of the employee's belongings on company property does not suffice to permit a search. An employer may only search the employee's belongings when the employer has probable cause to believe discovery of serious misconduct will result and other means of discovery have failed.[151]

---

145 *See id.* at 46.

146 Craver specifically states that as to personal property, as opposed to entrance and exit searches, that if there is a "carefully defined management rule" requiring inspection of personal property, such as large purses, compliance with the rule is a condition of employment. *Id.* at 47.

147 *Id.* at 46.

148 *See id.*

149 *Id.* at 47.

150 *Id.* at 49.

151 *Id.*

Craver's ultimate proposal for protecting employees from employer searches is that "arbitrators should recognize an implied covenant in collective bargaining agreements acknowledging the fundamental right of employees to be free from unreasonable management encroachments."[152] Breach of the covenant would result in monetary damages and, in some cases, modification of the imposed discipline. Interestingly, however, he proposes that when an employer "acts in good faith on a mistaken belief in its authority to conduct the search," the evidence discovered should be admitted and termination for gross misconduct should be upheld.[153]

Four additional safeguards, beyond the five discussed in relation to polygraphs, are suggested by Craver's discussion of searches: an affirmative right to refuse to be searched, notice of monitoring, notice of the particulars of the monitoring, and enforcement of the noticed policy. Craver's proposal for an implied covenant suggests two additional protections: compensation for violations of privacy and restrictions on discipline based on inappropriately gathered information.

Use of such safeguards is likely more workable than conditioning imposition of discipline on the sometimes nebulous "good faith" standard. Thus, the availability of privacy protection should turn on the degree of the monitoring's invasiveness, whether satisfactory privacy safeguards were utilized, and the severity of the offense. For instance, if an employee has committed gross misconduct, such as sharing trade secrets, then the employee could be terminated if other mandatory safeguards were afforded, regardless of whether the employer acted in good faith when monitoring the employee's e-mail.

3. Surveillance

Craver also discusses surveillance, through photographic and eavesdropping equipment, among other means.[154] The safeguards discussed, or lack thereof, might bear on monitoring of employee's actions through other means, such as GPS, or even potentially on monitoring of employees' electronic communications.

Craver concludes that employers generally have the right to conduct surveillance, surreptitious or not, of an employee based on "previously developed suspicions."[155] The use of surveillance techniques "in production areas, stockrooms, loading zones, and similar locations" is appropriate.[156] Craver discusses one arbitration decision where the arbitrator explained that, "'[i]t should be evident that an employee's ac-

152 *Id.* at 50.
153 *See id.*
154 *See id.* at 51.
155 *Id.*
156 *Id.* at 55–56.

tions during working hours are *not private* actions.'"[157] The arbitrator reasoned that a camera is simply a difference in the degree of observation, but not a difference in kind.[158]

However, in areas where employees are "entitled to privacy," such as lavatories and lounges, surveillance should be limited.[159] Craver suggests that "Congress should . . . prohibit all surreptitious visual monitoring of employees under circumstances entitling them to a reasonable expectation of privacy."[160]

Neither the arbitral authority as summarized by Craver nor his proposal provides significant protection for employees' right to privacy from employer monitoring of their actions while working. While a minimal level of protection is appropriate for such monitoring, some combination of safeguards should still apply to guarantee that employers do not abuse quickly evolving technology.

B. Professor Summers's Discussion of the Privacy Protections Provided for Off-Duty Behavior Provide Further Background for Developing Workable Privacy Protections Based on Labor Arbitration Decisions

Summers discusses the union framework protecting individual autonomy, of which he considers the right to privacy a subset.[161] He asserts that, "Collective contracts, unlike individual employment contracts, provide substantial protection of individual autonomy of employees."[162] He views the just cause provisions included in "almost all collective agreements" as contributing to such protection.[163] He discusses how the emphasis is on an employee's interest in her job which grows with seniority rather than on an employee's interest in privacy or autonomy per se.[164] He writes, "But the result is that personal autonomy obtains substantial implicit, if not explicit, protection."[165] Summers concludes: "The collective agreement gives substantial protection to the employee's

---

157 *Id.* at 62 (quoting FMC Corp., 46 Lab. Arb. Rep. (BNA) 335, 338 (1966) (Mittenthal, Arb.)) (emphasis in original).

158 *See id.*

159 *See id.* at 56.

160 *Id.* at 60.

161 *See* Summers, *supra* note 44, at 478.

162 *Id*; *cf.* Yelnosky, *supra* note 137, at 526. Professor Yelnosky promotes collective bargaining as a means to protect employees against employers overreaching in imposing appearance codes. He states that one arbitrator found a no-beard policy in violation of the CBA "using language that makes clear that a culture of employee autonomy exists in some union workplaces that is virtually unheard of in the non-union workplace." *Id.* (discussing Fairmont-Zarda Dairy, 106 Lab. Arb. Rep. (BNA) 583 (1995) (Rolhik, Arb.)).

163 *See* Summers, *supra* note 44, at 478.

164 *See id.* at 483.

165 *Id.*

right of privacy. Arbitrators weigh the employer's business interests against the employee's privacy interests but require the employer to show some substantial business need."[166]

He also notes that one of the most widely accepted principles among arbitrators is that "'what an employee does on his own time is none of the employer's business.'"[167] He implies that there may be an exception where there is a "concrete showing of a direct effect on the employer's business."[168]

Yet Summers recognizes that "invasions by employer action other than discipline or discharge go largely uncurbed."[169] For example, "intrusion into an employee's home by telephoto camera" or "intercepting e-mail are seldom prohibited by collective agreements."[170] Arbitration is unlikely to provide a satisfactory remedy for such invasions of privacy because arbitrators typically do not award monetary damages other than backpay.[171]

Thus, Summers's thesis supports the idea that the privacy protections provided by arbitration decisions, whether explicitly framed as such or not, provide a starting point for developing an adequate system of protection for employees' privacy rights.[172] One aspect of such a system should be significant protection for off-duty activities. Summers's suggestion that a "concrete showing of a direct effect" is necessary in order to impose discipline is supported by many of the decisions reviewed. Indeed, a review of the recent decisions addressing emerging technology such as GPS, e-mail, and Internet monitoring can serve as a basis for fleshing out the types of activities that have such a concrete harmful effect on an employer.

Summers's explanation also indicates that arbitration decisions merely serve as a starting point for an adequate framework of protection because they inadequately compensate employees for privacy invasions

---

166 *Id.* at 481.

167 *Id.* at 478–79 (quoting MARVIN F. HILL & MARK L. KAHN, DISCIPLINE AND DISCHARGE FOR OFF-DUTY MISCONDUCT: WHAT ARE THE ARBITRAL STANDARDS' IN ARBITRATION 1986: CURRENT AND EXPANDING ROLES 121 (Proceed., 39th Ann. Meet., Nat'l Acad. of Arb. Gladys Gershenfeld ed., 1986)).

168 *Id.* at 479.

169 *Id.* at 483.

170 *Id.*

171 *Id.*; *see also* Kim, *supra* note 12, at 1022. Professor Kim's article focuses on protecting employee privacy in the context of employer drug testing. Kim posits that, "individual grievances processed under collective bargaining agreements focused on protecting job security, rather than redressing any dignitary harm resulting from invasive testing practices." *Id.* Kim's explanation is that "lack of attention to workers' privacy is consistent with the fact that arbitrators rarely award money damages to workers except to compensate for lost wages." *Id.*

172 *Cf.* Kim, *supra* note 12, at 1027. Kim concludes that "unions appear to offer at least the possibility of mobilizing a collective response to threats of employee privacy." *Id.*

which do not result in discipline.[173] Indeed, while a review of the recent cases suggests that compensation and other types of protections from privacy invasions, such as an affirmative right to refuse to submit to privacy invasions, are conceptually recognized by arbitrators, they are not in widespread use. Nevertheless, an adequate system of protection for employees' privacy rights would draw upon these concepts to integrate such safeguards into an effective system to protect employees' privacy rights.

VI. RESEARCH METHODS

In order to discern the law of the shop regarding employee privacy in the face of emerging technology, searches were performed in the Bureau of National Affairs' (BNA) labor arbitration decisions database for decisions that addressed privacy and for decisions that addressed four recent technologies: GPS, e-mail, blogging, and the Internet.

Initially, a search was performed for the word "privacy." This search disclosed 417 documents, indicating that privacy was indeed addressed in the labor arbitration decisions. A review of the cases dating back to 1999 disclosed seventy cases potentially relevant to the issue of employee privacy from technological monitoring. Thereafter, searches were performed targeting specific technologies. Cases not explicitly framed in terms of privacy but that dealt with emergent technologies might also provide insight as to how to address privacy issues arising out of such technologies.

GPS was chosen as an emerging technology that monitors employees' actions while on duty. Searches for the terms "GPS," "global positioning system," "tracking system," or "computer communications system" brought up twenty-three cases. Some dated to as early as 1985. Six cases used the first term, and the earliest of those cases was in 2002, while the only year with multiple cases was 2007. This suggests that GPS is beginning to be addressed as a new technology in the workplace over the past decade.

E-mail was chosen as a relatively new technology that prompts monitoring of employees' communications in the workplace. A search for "email," "e-mail," or "electronic mail" revealed 281 documents, all of which were reviewed. The initial case mentioning e-mail was decided in 1990. In 1994 there were only three cases, and in 1995 four. By 1998 there were ten cases and by 2000 there were nineteen cases. These find-

---

173 *Cf. id.* at 1011. Kim discusses how the early cases brought by unions did focus on concerns about privacy and human dignity but later cases did not. Kim writes that, "Workers who felt aggrieved because of the manner in which a test was administered, or by the intrusiveness of the test itself, could not recover damages for dignitary harms, and those who suffered no tangible job loss were essentially remediless under the collective bargaining system." *Id.* at 1029.

ings suggest that there is significant arbitral precedent involving e-mail which can serve as a starting point for developing adequate protection of privacy for employees' personal communications while on-duty.

Blogging was selected as an emerging technology that implicates employer monitoring of off-duty conduct. But a search for the terms "blog!" or "blawg!" revealed only one decision.[174] While the case does deal with off-duty conduct, the case does not deal with a blog, as the term is typically conceived, but rather with posts to MySpace. Additionally, the case is somewhat unusual because the off-duty information about the employee was not posted by the employee but rather by his estranged wife. Thus, decisions about blogging are insufficient in number to serve as a starting point for developing adequate protections from off-duty monitoring.

In order to locate additional cases potentially dealing with off-duty monitoring, a search for the terms "internet" or "intranet" was performed and a search for the terms "web," "webpage," "web page," "website," "web site," "homepage," or "home page" was conducted as well. The former search revealed 104 decisions, which were reviewed back to those decided in 1999. The latter search retrieved 145 documents, which also were reviewed back to those decided in 1999. This search located several cases that dealt with off-duty conduct that can serve as a starting point, in conjunction with other types of off-duty cases, for developing adequate protections from off-duty monitoring. This search also located a large number of cases dealing with on-duty conduct, further supplementing the cases that address the use of e-mail.

Finally, a supplemental search aimed at discovering other cases dealing with decisions addressing privacy in off-duty conduct was conducted for the terms "private" or "privately." This search revealed an overwhelming number of cases—1,790—and those dating back to 2003 were reviewed.

Only a fraction of arbitration decisions are published. Thus, this inquiry is not reflective of the universe of arbitration decisions. Nor does the inquiry look specifically at collective bargaining agreements (CBA), employer policies, or court decisions, all of which would provide further insight as to the law of the shop on privacy.

The BNA-published arbitration decisions, however, reflect the law of the shop and are relied upon by other arbitrators making later decisions. They thus serve as a good starting point for discerning the law of the shop. Additionally, the concepts used by the arbitrators could be successfully adapted to the non-union workplace in order to regulate em-

174 *See* Warren City Bd. of Educ., 124 Lab. Arb. Rep. (BNA) 532, 535 (2007) (Skulina, Arb.).

ployers' use of technology to monitor employees and to protect employees' right to privacy.

Of these reviewed cases, eighty-three were more closely reviewed, sixty-eight of which are cited herein. Fifty-nine are cases challenging discipline under a just cause provision. In thirty-six of those cases, the discipline was overturned or reduced. Eight are cases alleging other types of violations of contractual provisions or past-practice. The grievance was upheld, at least in part, in six of those cases. One is an interest arbitration decision rejecting a proposal that employees perform routine maintenance on their assigned computers. Twenty-two of these sixty-eight cases explicitly frame a relevant issue as one addressing employees' privacy concerns.[175]

VII. FINDINGS AND CONCLUSIONS: THE LAW OF THE SHOP RECOGNIZES THAT EMPLOYEES HAVE A RIGHT TO PRIVACY

Arbitral authority recognizes employees' right to privacy.[176] For instance, in one case the arbitrator states, "There is a common law of the shop which holds that when an employee is being disciplined the supervisor should honor the employee's privacy."[177]

Indeed, arbitrators have recognized that, at times, limits must be placed on the technology that an employer can use in order to protect employees' privacy concerns. In one case, for example, an arbitrator concluded that an employer could not unilaterally implement a direct deposit pay system, in part because of privacy considerations.[178] While these cases deal with maintaining information private from co-workers and third parties rather than from employers, they suggest that limits are possible and, in certain instances, appropriate.[179] They also suggest that any policies dealing with maintaining employees' privacy from employer monitoring and conduct might best be integrated into larger policies ad-

---

175 These findings coincide with those of Kim, who concludes that, when addressing drug testing, unions do assert privacy rights but tend to focus on job security. *See* Kim, *supra* note 12, at 1011.

176 *See, e.g.*, City of Kalamazoo, 116 Lab. Arb. Rep. (BNA) 815, 818-19 (2001) (Daniel, Arb.) (addressing whether a policy extending benefits to same-sex couples was appropriate and stating "[a]pplicants need not be homosexual and certainly the city would not inquire as to any employee's sexual activities—that would be an egregious violation of privacy").

177 Rhodia, Inc., 118 Lab. Arb. Rep. (BNA) 455, 464 (2003) (Neas, Arb.).

178 *See* Fremont Plastic Prods., 122 Lab. Arb. Rep. (BNA) 149, 154 (2005) (Franckiewicz, Arb.). *But see* City of Bedford, 121 Lab. Arb. Rep. 1214 (2005) (Skulina, Arb.) (upholding mandatory direct deposit).

179 *See* Wackenhut Corrs. Corp., 118 Lab. Arb. Rep. (BNA) 63 (2003) (O'Conner, Arb.) (addressing the privacy of medical information).

dressed toward maintaining privacy of employee information more generally.[180]

The arbitration decisions also indicate that privacy is situational. In this context, situational privacy means that employees desire to selectively disclose certain information only to certain people and maintain the information private from others. One arbitrator found an employer's investigation is inadequate where the employer did not speak to each employee witness in private.[181] The arbitrator reasoned that an employee would need privacy before implicating a co-worker.[182] Thus, employees have some thoughts they should be asked to share only with certain people. This idea extends to keeping certain conduct and thoughts private from their employers.[183]

The cases dealing with privacy and the impact of new technology on employer monitoring of employees suggest twelve safeguards for employee privacy from employer monitoring: 1) the right to affirmatively refuse monitoring; 2) notice of monitoring; 3) notice of the particulars of the 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.

Nevertheless, the protection of employees' privacy is not as systematic or robust as would be ideal to provide consistent protection of employees' rights to privacy.[184] Through systematically grouping these

---

180 To the extent possible, the protections from employer technological monitoring discussed in this Article should be integrated or coordinated with overall policies governing workplace privacy. These would include regulations about gathering information from employees or about employees by means other than technological monitoring and regulations governing to whom collected information can be disclosed, including regulations regarding privacy of medical information.

181 *See* ESAB Welding & Cutting Prods., 115 Lab. Arb. Rep. (BNA) 79, 83 (2000) (Wolkinson, Arb.).

182 *See id.* ("One does not have to be a trained investigator to understand that only when afforded appropriate privacy might employees provide sensitive information incriminating other co-workers.").

183 *See* discussion *infra* Section VII. C.

184 It is interesting, and ironic, that in one case involving a discharge of an employee for taking a picture on his phone of a sunset while at work in violation of a rule forbidding recording devices in the plant, the employer asserted that an underlying reason for the rule was to protect employees who are "generally very, very sensitive of being recorded." Trane Co., 124 Lab. Arb. Rep. (BNA) 673, 674 (2007) (Heekin, Arb.). In another case, an employer asserted termination of an employee was appropriate in part because he had invaded his super-

twelve safeguards into potential protection packages depending on the level of intrusion of the employees' privacy, satisfactory policies protecting employee privacy can be developed. These safeguards, used in varying combinations, can serve as a starting point for thinking about workable privacy protections in the American context.

This section mentions the role of collective bargaining in protecting privacy and suggests potential means for mimicking that protection in the non-union sector. The section then surveys general arbitral principles that might be useful in developing protections for employee privacy. Next, the section describes cases dealing with employees' right to privacy and right to be free from technological monitoring. It proposes that the safeguards suggested by these cases can serve as a starting point for developing an adequate framework for protecting employees' privacy from technological monitoring. Finally, the section proposes potential remedies for violations of the proposed privacy protections and discusses the issue of whether employees should be permitted to waive the proposed protections in return for compensation.

A. Creative Yet Practical Means, Such as Minimal "Floors"[185] of Privacy Protection or Safe-Harbor Policies, Can Be Used to Mimic Forbidding Employers from Unilaterally Imposing Policies that Invade Privacy Without Bargaining with the Union[186]

Some arbitrators require bargaining with the union before installing monitoring devices or otherwise invading an employee's privacy,[187]

---

visor's privacy by reading e-mails on his supervisor's work computer. *See* Monterey County, 117 Lab. Arb. Rep. (BNA) 897, 900 (2002) (Levy, Arb.). These cases support Craver's suggestion that employers will assert the privacy interests of their employees to further management prerogative but deny that employees have any right to privacy for the same end. *See* Craver, *supra* note 12, at 1059.

185 Matthew Finkin, Book Review, 21 COMP. LAB. L. & POL'Y J. 813, 814 (2000) (discussing "gap between the French 'floor of rights'" and employer "control of employee privacy" in the United States).

186 The word "mimic" indicates that, for many reasons, it is not possible to replicate, or even nearly replicate, the protections provided by the requirement that employer's bargain with exclusive representatives over working conditions. The level of equality in bargaining position and the likelihood of enforcement are likely greater in a collective scheme than one based on individual rights.

187 *See, e.g.*, Lyondell Citgo Ref., 120 Lab. Arb. Rep. (BNA) 360, 363 (2004) (Moreland, IV, Arb.); St. Louis Post-Dispatch, 117 Lab. Arb. Rep. (BNA) 1274, 1279 (2002) (Daly, Arb.) (requiring bargaining to implement restraints on the "fundamental freedom" of a person to "work where" the person "can and hold a job") (quoting Lowell Sun Publ'g Co., 43 Lab. Arb. Rep. 273 (BNA) (1964) (Hogan, Arb.)); *cf.* Berkley Sch. Dist., 122 Lab. Arb. Rep. 356 (2005) (Daniel, Arb.) (employer could not install closed circuit televisions in instructional areas because contract forbid their use, as well as use of any similar surveillance device).

while others do not.[188] During mandated bargaining, unions bargain for safeguards such as notice, verification of accuracy of the photos or other reports from the monitoring system, or particularized suspicion to monitor.

In the non-union sector there is, of course, no union with which to bargain. One possible mechanism for ensuring equivalent types of safeguards for non-union situations is to legislate minimum employee privacy rights. These rights might be enforced through private court action, an administrative proceeding, mediation and conciliation, or private arbitration.

Promulgation of safe-harbor policies could also provide such protection. Similar to the privacy policies that United States companies now adopt to comply with European privacy laws,[189] the state or federal government, whether through the legislature or a designated agency, could develop a set of privacy policies. Providing a range of policies offers employers with different management policies and cultures the flexibility of adopting different policies based on needs and fit. If an employer implemented and complied with one of the promulgated policies, that would serve as a safe-harbor from any type of invasion of privacy claim covered by the safe-harbor policies.[190] In other words, an employee would be unable to bring a privacy claim of the kind addressed by the policy against an employer who complied with an adopted policy.

---

188 *See, e.g.*, City of Okmulgee, 124 Lab. Arb. Rep. (BNA) 423, 430 (2007) (Walker, Arb.) (new policy on use of computers and internet is not contrary to CBA and does not materially, substantially, and significantly affect the terms and conditions of employment); Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) 257, 262 (2006) (Nicholas, Arb.). *But see* California Newspaper Partnerships, 350 N.L.R.B. No. 89 (Sept. 10, 2007) (employer must bargain with union over policy forbidding use of e-mail accounts to send messages about union affairs).

189 Because the United States provides an inadequate level of privacy protection, no data can be transferred from the European Union to the United States unless the involved company has pursued a safe-harbor option. The company can either certify annually to the U.S. Department of Commerce that it "agree[s] to adhere to comparable notice, choice, access and enforcement requirements" or can sign "onto standard contractual clauses adopted by the European Commission to ensure adequate safeguards for personal data transfer." Moldof, *supra* note 39, at 10.

190 Another possibility to encourage acceptable privacy practices might be to condition some privilege, such as access to free high speed internet provided by the community, on adopting such a policy. This would not recognize employees' right to privacy but would, at least, tend to encourage recognition of privacy concerns.

B. Some Limits on Employer Conduct Generally Recognized by Arbitrators Might Serve as a Starting Point for Developing Minimal Privacy Protections or Safe-Harbor Policies[191]

This Article will focus on recommending policies derived from the concepts specifically addressing privacy concerns discussed below in Sub-Section C. Nevertheless, some legislatures, courts, administrators, or even employers may wish to consider incorporating some of the more generally-recognized arbitral principles as part of a system regulating employee privacy.[192] Additionally, these principles serve as useful background for the more detailed discussion of the safeguards protecting privacy discussed thereafter.[193] Thus, this section briefly discusses some of the standard principles recognized by arbitrators: reasonable rules, notice, thorough investigation, disparate treatment, progressive discipline, mitigating circumstances, and the fit between the severity of the infraction and the resulting discipline.

1. Reasonable Rules

Arbitrators generally conclude that a rule must be "reasonably" related "to the orderly, efficient and safe operation of the employer's business."[194]

---

191 Some of these concepts are part of the oft-cited seven questions posed by Professor Dougherty in Enterprise Wire Co., 46 Lab. Arb. Rep. (BNA) 359 (1966), to determine whether there is just cause. *See* Sycamore Bd. of Educ., 123 Lab. Arb. Rep. (BNA) 1588, 1596 n.1 (2007) (Van Pelt, Arb.).

192 For instance, one decision involves a non-union employer who voluntarily adopted progressive discipline. *See* Alliedsignal Engines, 106 Lab. Arb Rep. (BNA) 614 (1996) (Rivera, Arb.).

193 While the lead text on labor arbitration, ELKOURI & ELKOURI, HOW ARBITRATION WORKS (Alan M. Ruben ed., 6th ed. 2003), does not contain a section specifically dedicated to employees' right to privacy from technological monitoring, it does contain relevant information in various sections. *See, e.g.*, Privacy, Dignity, and Peace of Mind, 1076; Use of Grievance Procedure Versus Self-Help, 283; "Moonlighting" and Outside Business Interest, 1043; Personal Appearance: Hair and Clothes, 1046; Fraternization, Intermarriage of Employees, Employment of Relatives, Married Employees, 1073; Use of Personal Radios, 1085. DISCIPLINE AND DISCHARGE IN ARBITRATION (Norman Brand ed., 1998), is also a good source for information about general principles applied in that context.

194 United Ass'n of Plumbers & Steamfitters, 116 Lab. Arb. Rep. (BNA) 710, 712 (2001) (Wolfson, Arb.); *see also e.g.*, Embarq, 123 Lab. Arb. Rep. (BNA) 923, 928 (2007) (Armendariz, Arb.); Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) 1388, 1391 (2005) (Fagan, Arb.); JBM, 120 Lab. Arb. Rep. (BNA) 1688, 1699 (2005) (Rosen, Arb.); Georgia Power Co., 123 Lab. Arb. Rep. 936, 946 (2006) (Nolan, Arb.); Albertson's Inc., 115 Lab. Arb. Rep. (BNA) 886, 891 (2000) (Gangle, Arb.).

2. Notice

Arbitrators commonly endorse the idea of notice, be it notice of rules,[195] notice of monitoring,[196] notice of potential level of discipline,[197] or notice within a limited time period that an employee has committed an infraction.[198] Typically, to provide reasonable notice of monitoring or prohibited conduct, a rule must be clear.[199]

3. Thorough Investigation

Arbitrators generally consider whether any investigation of an employee's misconduct that led to discipline was adequately thorough.[200]

4. Disparate Treatment

Arbitrators commonly consider whether other employees who have committed the same types of infractions received lesser penalties.[201]

5. Progressive Discipline

Arbitrators commonly endorse the idea of progressive discipline.[202] Progressive discipline punishes an initial infraction less severely than a

---

195 *See, e.g.*, Trane Co., 124 Lab. Arb. Rep. (BNA) 673, 674 (2007) (Heekin, Arb.); Sycamore Bd. of Educ., 123 Lab. Arb. Rep. (BNA) at 1597; Georgia Power Co., 123 Lab. Arb. Rep. (BNA) at 947; Cingular Wireless, 121 Lab. Arb. Rep. (BNA) 438, 441 (2005) (Nolan, Arb.); Saint Gobain Norpro, 116 Lab. Arb. Rep. (BNA) 960, 967 (2001) (Fullmer, Arb.); Conneaut Sch. Dist., 104 Lab. Arb. Rep. (BNA) 909, 914 (1995) (Talarico, Arb.).

196 *See, e.g.*, Georgia Power Co., 123 Lab. Arb. Rep. (BNA) at 944 (arbitrators concluded that policy "expressly warned" that the company would monitor electronic communications despite fact that only quoted policy language simply "reserved the right" to monitor).

197 *See, e.g.*, *id.*; Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) at 1391; Penn Window Co., 120 Lab. Arb. Rep. (BNA) 298, 304 (2004) (Dissen, Arb.) ("If an employee is not informed of rules and the consequences for their violation, his due process rights are significantly compromised."); Univ. of Mich., 114 Lab. Arb. Rep. (BNA) 1394, 1399 (2000) (Sugerman, Arb.) (termination inappropriate when employer failed to notify grievant that failing to terminate personal calls would lead to termination).

198 *See, e.g.*, City of El Paso, 123 Lab. Arb. Rep. (BNA) 691, 693 (2006) (Greer, Arb.) (180-day period for disciplinary action for non-criminal violations); Union-Scioto Local Bd. of Educ., 119 Lab. Arb. Rep. (BNA) 1071, 1078 (2004) (Cohen, Arb.) (notice inadequate to inform grievant of nature of infraction).

199 *See, e.g.*, Xcel Energy, 119 Lab. Arb. Rep. (BNA) 26, 34 (2003) (Daly, Arb.).

200 *See, e.g.*, Embarq, 123 Lab. Arb. Rep. (BNA) 923, 928 (2007) (Armendariz, Arb.); Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) at 1391; ESAB Welding & Cutting Prods., 115 Lab. Arb. Rep. (BNA) at 83.

201 *See, e.g.*, Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) at 262; Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) at 1391; Xcel Energy, 119 Lab. Arb. Rep. (BNA) at 35 (reasoning that downloading child pornography is more serious than downloading other pornography); Monterey County, 117 Lab. Arb. Rep. 897, 900 (2002) (Levy, Arb.) (disparate treatment where those who sent inappropriate and sexually explicit e-mails to employee were not disciplined); Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) 271, 276–77, 279 (2001) (Goodstein, Arb.); PPG Indus., 113 Lab. Arb. Rep. 833, 844 (1999) (Dichter, Arb).

202 *See, e.g.,* Orange County, Fla., 123 Lab. Arb. Rep. (BNA) 460, 465 (2007) (Smith, Arb.) ("The credibility of the whole grievance and arbitration system hinges on review of the

later infraction of the same type.[203] It "affords an employee the opportunity to correct his or her behavior before more severe discipline, up to and including termination, is imposed."[204] Many arbitrators endorse progressive discipline for misuse of company equipment, including computer systems.[205] They also endorse progressive discipline for infractions discovered by monitoring devices such as GPS.[206]

6. Mitigating Circumstances, Including Seniority

Arbitrators commonly consider aggravating and mitigating factors to determine whether the level of discipline is appropriate. Common mitigators include honesty and acceptance of responsibility for infractions,[207] long-time service,[208] a record that is clear of previous discipline,[209] and any awards or commendations.[210]

While some employers may protest reliance on seniority as opposed to merit, seniority does indicate an ability to conduct oneself in the workplace in a manner that complies with the employer's work rules.[211] Moreover, while employers may be concerned that employees are hiding

---

penalty to assure that it is in conformity with the guiding precept of progressive or corrective, rather than punitive, discipline."); Sycamore Bd. of Educ., 123 Lab. Arb. Rep. (BNA) 1588, 1598 (2007) (Van Pelt, Arb.); Kuhlman Elec. Corp., 123 Lab. Arb Rep. (BNA) at 262; Mont. Child & Family Servs., 122 Lab. Arb. Rep. (BNA) 656, 662 (2006) (Reeves, Arb.); Cingular Wireless, 121 Lab. Arb. Rep. (BNA) 438, 441 (2005) (Nolan, Arb.).

203 *See* Orange County, Fla., 123 Lab. Arb. Rep. (BNA) at 465; JBM, Inc., 120 Lab. Arb. Rep. (BNA) 1688, 1698 (2005) (Rosen, Arb.) (discussing progressive discipline).

204 JBM, Inc., 120 Lab. Arb. Rep. (BNA) at 1698.

205 *See, e.g.,* Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) at 262; Ga. Power Co., 123 Lab. Arb. Rep. 936, 947 (2006); County of Sacramento, 118 Lab. Arb. Rep. (BNA) 699, 702 (2003) (Riker, Arb.); Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) at 271; Snohomish County, 115 Lab. Arb. Rep. 1, 7 (2000) (Levak, Arb.); *see also* Nw. Publ'ns, 114 Lab. Arb. Rep. (BNA) 761, 765 (2000) (Bognanno, Arb.) (reducing five day suspension for working on photo of nude wife on computer and showing image to co-workers, including one who was offended, to warning/counseling).

206 *See, e.g.*, Orange County, Fla., 123 Lab. Arb. Rep. (BNA) at 465.

207 *See, e.g.*, Monterey County, 117 Lab. Arb. Rep. (BNA) 897, 900 (2002) (Levy, Arb.); Shawnee County, 123 Lab. Arb. Rep. (BNA) 1659, 1663 (2007) (Daly, Arb.).

208 *See, e.g.*, Mont. Child and Family Servs., 122 Lab. Arb. Rep. (BNA) at 662; Ga. Power Co., 123 Lab. Arb. Rep. (BNA) at 947; Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) at 1391; King Soopers, Inc., 120 Lab. Arb. Rep. (BNA) 501, 505-06 (2004) (Sass, Arb.); Monterey County, 117 Lab. Arb. Rep. (BNA) at 900 ; Quaker Oats Co., 116 Lab. Arb. Rep. (BNA) 211, 215 (2001) (Marino, Arb.); Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) at 274; PPG Indus. Inc., 113 Lab. Arb. Rep. (BNA) at 844.

209 *See, e.g.*, Ga. Power Co., 123 Lab. Arb. Rep. (BNA) at 947; Mont. Child and Family Servs., 122 Lab. Arb. Rep. (BNA) at 662; King Soopers, Inc., 120 Lab. Arb. Rep. (BNA) at 505–06; Monterey County, 117 Lab. Arb. Rep. (BNA) at 900; Quaker Oats Co., 116 Lab. Arb. Rep. (BNA) at 215; Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) at 274; PPG Indus. Inc., 113 Lab. Arb. Rep. (BNA) at 842.

210 *See, e.g.*, Kuhlman Elec. Corp., 123 Lab. Arb Rep. (BNA) at 262.

211 *See* Ga. Power Co., 123 Lab. Arb. Rep. (BNA) at 947 ("[L]ong service without previous discipline strongly suggests that the employee can learn from his mistakes."); King Soopers, Inc., 120 Lab. Arb. Rep. (BNA) at 506 ("[Y]ears of good service show that an em-

behaviors that harm the employer, the performance of long-term employees likely would have suffered over time had they been hiding poor behavior all along. Thus, it seems fair to consider longevity of employment in cases where a violation of the employees' privacy leads to discipline.

7. Severity of Discipline Fits Infraction

Arbitrators often consider whether the level of discipline is appropriate in light of the seriousness of the infraction.[212]

C. Arbitral Concepts Particular to Protecting Employees' Right to Privacy and to be Free of Technological Monitoring Can Serve as a Starting Framework for Regulation or Safe-Harbor Policies

Arbitration decisions serve as a good starting point for developing a spectrum of protection from monitoring based on the intrusiveness of the invasion. The least protection is afforded from technologies that monitor on-duty actions, such as GPS or video cameras, albeit systematically, completely, and in a recorded manner.[213] Intermediate protection is afforded from those that record information that implicates other human rights, such as the right to speak or to associate,[214] and the greatest protection is afforded from those that monitor off-duty behavior. Indeed, arbitration decisions address technologies, such as GPS and video surveillance, that monitor an employee's outward actions with only incidental recording of conversations or images. Arbitration decisions also address monitoring of employees' computer usage, which focuses on the content of employees' thoughts and communications. Additionally, arbitration decisions address employees' behavior in their private lives outside of the workplace.

Arbitration decisions address both surreptitious and open monitoring of these different types of employee behavior, and some decisions even recognize an affirmative right to privacy. The sub-sections below survey the decisions addressing the spectrum of privacy intrusions, comment on the decisions and tease out the various safeguards for employee

---

ployee can conform to the rules and that whatever they did to warrant discipline was something of an aberration rather than their normal way of behaving.").

212 *See, e.g.,* Embarq, 123 Lab. Arb. Rep. (BNA) 923, 928 (2007) (Armendariz, Arb.).

213 *See* Bernstein, *supra* note 12, at 925 ("One might argue . . . that observation via closed-circuit television camera is worse than the human-on-human snooping to which Selmi compared it if only because a video image of a face can be re-wound and replayed, edited, enlarged into grotesque nostril-boring expansion, whereas the human snoop gets nothing to exploit beyond his glance.").

214 *See* Craver, *supra* note 12, at 1076 (suggesting that monitoring activities is less intrusive than monitoring communications where employees "have the right to expect their appropriate exchanges with coworkers and outside person will remain confidential" and proposing a monitoring system where confidentiality from managers is maintained).

privacy proposed by arbitrators, suggest extensions of the safeguards, and then suggest various frameworks combining those safeguards that would adequately protect an employee's privacy right from each level of intrusion.

The first sub-section discusses the concept of a negative or affirmative right to privacy and proposes an affirmative right to privacy as an appropriate safeguard for protecting an employee's privacy. The second sub-section discusses monitoring, both open and surreptitious, of employees' actions while on-duty. The third sub-section addresses monitoring of employees' computer use as an example of monitoring of employees' thoughts and communications on-duty. Finally, the last subsection addresses monitoring of and discipline for off-duty behavior.

1. Affirmative or Negative Right to Privacy

Some arbitration decisions suggest that an employee has an affirmative right to refuse to permit an employer from invading the employee's privacy. These include decisions shielding off-duty behavior from employer mandate or inquiry,[215] and a decision recognizing an employee's right to assert privacy as an exception to the rule that an employee, when working, must obey an employer's directive.[216]

a. Affirmative Right to Privacy For Off-Duty Behavior

Two decisions suggest that there is an affirmative right to privacy in one's off-duty behavior. In one case, the arbitrator rather fully embraced the thesis underlying Selmi's proposal that off-duty behavior should be private from the employer.[217] The arbitrator held that the Collective Bargaining Agreement prohibited an employer from implementing a system under which all maintenance employees must wear pagers, respond within fifteen minutes of being called, and report to work within one hour.[218] The arbitrator concluded:

> It must be recognized, that the imposition of wearing a pager while off-duty infringes upon an employee's right to their [sic.] peaceable enjoyment of life and privacy during self-governed hours beyond the scrutiny and control of the employer, particularly when the employee is not volunteering for the inconvenience nor being compensated for the intrusion. These are the issues to be

---

215 *See, e.g.*, Shawnee County, 123 Lab. Arb. Rep. (BNA) 1659, 1663 (2007) (Daly, Arb.); Lyondell Citgo Ref., 120 Lab. Arb. Rep. (BNA) 360, 364 (2004) (Moreland, Arb.).

216 *See* Albertson's Inc., 115 Lab. Arb. Rep. (BNA) 886 (2000) (Gangle, Arb.).

217 *See* Lyondell Citgo Ref., 120 Lab. Arb. Rep. (BNA) at 364.

218 *See id.* at 365.

> appropriately addressed and conceded only after good faith collective bargaining, which did not occur.[219]

The arbitrator ordered the employer to rescind the policy and any resulting discipline.[220] He ordered that "said disciplined employee(s) shall be made whole in all respects, including wage loss, back pay, job demotion, blemished work record, promotion denial, seniority, or any other employment related benefit(s) loss directly attributable to any disciplinary action stemming from the violation of the on call pager policy."[221] Thus, the arbitrator recognized that employees have a right to privacy from employer monitoring while off-duty. The opinion appears to endorse an affirmative right to refuse to wear monitoring devices while off-duty.[222] It erases discipline and any other negative action resulting from affirmatively refusing to comply with the policy.

Furthermore, while the decision does not provide compensation for the invasion of privacy itself as one of the remedies, it suggests that, as a general proposition, employees should be compensated for invasions of privacy, at least pertaining to off-duty conduct.[223] Compensation for an invasion of privacy is, thus, another recognized safeguard, and this could easily extend to providing a remedy for violations of privacy.

Another case implies that there is an affirmative right to privacy for off-duty conduct, even where that conduct is documented on a publicly-available web page.[224] The grievant, a sheriff's deputy, attended a dance bar, and the bar posted a photo of many people dancing, including the grievant, on its website.[225] The grievant called in late to work the next day, and management asked her about her reasons for being late.[226] When she was terminated for lying about the reasons why she was tardy, the arbitrator reasoned that no rule prohibited the grievant from attending

---

219 *Id.* at 364.

220 *See id.* at 365.

221 *Id.*

222 *See id.; see also* Lake Wash. Sch. Dist., 120 Lab. Arb. Rep. (BNA) 1081, 1087 (2004) (Henner, Arb.) (suggesting that if a teacher who was subject to limitations on spending time with children outside of work hours had sought permission to spend time with the children of the woman he was dating and the employer had refused permission, "he might even have been entitled to refuse to comply with an unreasonable denial").

223 *See id.* at 361.

224 *See* Shawnee County, 123 Lab. Arb. Rep. (BNA) 1659, 1661 (2007) (Daly, Arb.). This is a public sector case, but, like all other public sector cases cited in this Article (unless explicitly mentioned otherwise), it does not involve constitutional or other issues that would differentiate it from private sector cases. As discussed below, there are, however, many other cases which find it appropriate to monitor an employee's off-duty conduct in certain circumstances. *See* discussion *infra* Section VII C.4.b.

225 *See* Shawnee County, 123 Lab. Arb. Rep. (BNA) 1659, 1661 (2007) (Daly, Arb.).

226 *See id.* at 1662.

the bar and that officers were not required to report reasons for tardiness.[227]

The undercurrent of the decision suggests that the arbitrator believed it was inappropriate for the employer to inquire about the grievant's off-duty conduct, even if her photo was publicly available. The decision suggests that the employee's right to refuse to divulge personal reasons for tardiness extends so far as to excuse any lies about her off-duty life.[228] Thus, the opinion suggests an affirmative right to refuse to disclose personal information, such as off-duty behavior, to an employer. Such a right might be extended to provide a safeguard from violation of privacy protections whether involving off-duty behavior or not.

b. Affirmative Right to Privacy for On-Duty Behavior

There is an interesting discussion about whether employees must, when on duty, submit to privacy invasions and grieve later.[229] In one case, for instance, the arbitrator found it appropriate for an employee to refuse to stick out her tongue.[230] The supervisor desired to determine whether she was wearing a tongue ring in violation of company rules.[231] The arbitrator reasoned that the principle "obey now, grieve later" is subject to certain exceptions.[232] These exceptions include refusing to "perform an illegal, immoral or dangerously unsafe act" or an act that would humiliate or violate the privacy right of the employee.[233] The arbitrator reasoned that arbitrators recognized the latter justification in drug testing cases.[234] The arbitrator further reasoned that "[i]t was unreasonably intrusive, therefore, to require that she open her mouth and extend her tongue, so that [the supervisor] could check her private, personal space."[235]

Thus, the decision recognizes an affirmative right to privacy in the right of an on-duty employee to refuse to submit to privacy invasions by her employer. And while bodily integrity is certainly an important aspect of privacy, it is arguably equally invasive to monitor someone's private thoughts or the images the person chooses to view as it is to view some-

---

227 *See id.* at 1663.

228 *See id.* at 1664.

229 *See* DISCIPLINE AND DISCHARGE IN ARBITRATION 165 (Norman Brand ed. 1998) ("There is a line of cases finding discipline to have been improperly imposed in circumstances where the employer's action conflicts with the individual's right to privacy.").

230 *See* Albertson's Inc., 115 Lab. Arb. Rep. (BNA) 886, 893 (2000) (Gangle, Arb.).

231 *See id.* at 889.

232 *See id.* at 892.

233 *Id.*; *see* Yelnosky, *supra* note 137, at 527–28 (discussing *Albertson's* as an example of a case protecting unreasonable application of a reasonable rule regulating employee appearance).

234 *See* Albertson's Inc., 115 Lab. Arb. Rep. (BNA) at 893.

235 *See id.*

one's tongue. Certainly an employee could suffer more emotionally from an employer gaining access to information that disclosed an unwanted pregnancy, a same-sex relationship, or a child out-of-wedlock than from simply being required to stick out a tongue. Thus, extending this safeguard as part of a framework to address employer monitoring of employees, at a minimum to protect on-duty communications, would be appropriate.

Many arbitrators, however, would probably take the position that an employee must obey an order that threatens the employee's privacy and grieve the violation later.[236] For instance, one decision exempts only safety threats that would result in physical injury to the employee from the rule to grieve later.[237] The arbitrator upheld the employee's discharge for refusal to share photos on his private phone with his employer.[238] The only other misconduct the grievant engaged in was using his private property during his break period while in a smoking area to photograph a sunset.[239] He thereby violated a rule prohibiting using recording devices on plant property.[240] The arbitrator did intimate that if the employee had testified as to the harm that would have resulted from sharing the photos with management, the outcome may have been different.[241]

Such a position indicates that employees have no affirmative right to privacy. They cannot assert their privacy and keep it inviolate from employers. Rather, employees only have negative privacy rights. They can assert that employers have violated their privacy after-the-fact and can thus seek a remedy for the invasion.

Yet it is difficult to believe that taking a picture of a sunset while on company property grants an employer permission to view an employee's private photographs. The obvious harm is that employers are forcing employees to disclose private personal information. A means of proving harm beyond that is difficult to conceive. Certainly an employee should not have more of a privacy right because the photographs would disclose sexual or other generally frowned-upon photographs. Additionally, an employer who has no reasonable suspicion that there are pictures of company property or employees has no grounds upon which to trample an employee's privacy rights.[242]

---

236 *See* Trane Co., 124 Lab. Arb. Rep. (BNA) 673, 677 (2007) (Heekin, Arb.).

237 *See id.* at 676.

238 *See id.* at 677.

239 *See id.* at 674.

240 *See id.*

241 *See id.* at 677.

242 Moreover, it is difficult to believe that termination is the appropriate discipline for such a refusal. Privacy seems like a significant mitigating circumstance with respect to the finding of insubordination. Under principles of progressive discipline, discussed above, less

Instead of recognizing only a negative right to privacy, an employer can adequately protect employees' rights by recognizing an affirmative right of privacy as one safeguard appropriately used in conjunction with others. This is particularly true in a non-union setting where there is no union-representative or grievance process to challenge a privacy invasion after-the-fact.

For instance, an employee with photos on a phone might have an affirmative right to refuse disclosure unless other safeguards are met. These safeguards might include using a designated non-management employee who will review the contents, keep the information confidential, and, if possible, review only information time-dated as being collected during times the employee was at work. Disclosure from that employee to management should result only if the photographs reviewed indicate that the particular, significant, and concrete work-related misconduct for which the employee performed the search had taken place.

2. Monitoring of Employees' Actions While on Duty

This section discusses the monitoring of employees' actions while on duty. First, it discusses open monitoring of employees' on-duty conduct. Next, it discusses surreptitious monitoring. Each sub-section sets out the range of arbitrators' views on the appropriateness of such monitoring and suggests frameworks that would provide the adequate minimal protection needed for such monitoring. Finally, the section discusses insuring the accuracy and reliability of gathered information.

a. Open Monitoring of Employees' On-Duty Conduct

Two arbitration decisions suggest two appropriate safeguards for violation of employee privacy from employer technological monitoring of the employee's actions during work-time. These safeguards are notice of monitoring and notice of the infractions that the monitoring is designed to prevent.

In one decision, a GPS disclosed that an employee had driven an employer-owned vehicle to his home for lunch.[243] There was no challenge to the use of the GPS, of which the employees were well-aware, on privacy or any other grounds. Significantly, however, the arbitrator did not uphold the discipline because, among other reasons, no policy provided the employee notice that driving home was prohibited.[244] In another decision, a GPS disclosed that an employee had misrepresented the

---

discipline would certainly seem sufficient to prevent the employee from taking photographs in the future while on plant property. *See supra* Section VII.B.5.

243 *See* Orange County, Fla., 123 Lab. Arb. Rep. (BNA) at 463.

244 *See id.* at 465.

time spent working at customer sites.[245] Again, there was no challenge to the use of the GPS, of which the employees were well-aware.[246] The discipline in this case was, however, upheld, in part because the grievant had been warned about his behavior and falsifying time records.[247]

Indeed, notice of monitoring provides an important safeguard for employees' right to privacy. Notice does not interfere with an employer's ability to ensure that the employees are performing their duties, even when they work off-site or when assessing the employee's output is difficult (such as when the employee self-reports completion of work at a customer location).[248] Moroever, employees understand that their movements are monitored and, consistent with the theory of selective disclosure, employees will not take action to disclose private information to the employer.[249]

Equally important, notice must be provided with respect to the types of actions that, if discovered via the monitoring, will result in discipline.[250] The purpose of the monitoring is not to catch the employees in bad acts of which the employer has no suspicion. Rather, in this context, it is simply to ensure efficiency and quality work-product.[251] Thus, employees should be on notice not only of the quantity and quality of work expected but also of other actions which might result in discipline, such as traveling to their homes.

Assuming that the monitoring is only during work-time, if these minimal protections are satisfied, only one further safeguard will be necessary: some assurance of the accuracy and reliability of the records of monitoring.[252] While the permanence of GPS records makes it simpler for an employer to "check-in" on an employee, and the constant record-keeping of every movement may be somewhat oppressive, the monitoring of on-duty conduct is not so intrusive as to necessitate further safeguards.

Additionally, periodic management check-ups of reports, even without a reasonable suspicion of particularized wrongdoing, is permissive because employees are unlikely to be engaged in conduct that they legitimately wish to keep private from their employer that would be captured by GPS monitoring of on-duty actions. An employee might stop some-

---

245 *See* Embarq, 123 Lab. Arb. Rep. (BNA) at 923, 930, 931 (2007) (Armendariz, Arb.).

246 *See id.* at 924.

247 *See id.* at 931–32.

248 *See id.* at 924 (explaining that employee worked at customers' premises without supervision and also self-reported time worked).

249 There must be evidence of actual notice or employee acknowledgment of receipt of a written policy. *See* Orange County, Fla., 123 Lab. Arb. Rep. (BNA) at 465.

250 *See id.*

251 *See id.* at 460.

252 *See infra* Section VII.C.2.c.

where private, such as to pick up medication, but this type of privacy invasion is less likely to occur than when an employer is monitoring personal communications.[253] And while employees may be lulled into a false suspicion that employers are not checking on their actions, periodically checking an employees' records is unlikely to seriously intrude on private conduct.[254]

On the other hand, some would take the position that noticed technological monitoring of on-duty conduct is an invasion of privacy, even with the minimal safeguards suggested.[255] New York City taxi-cab drivers vigorously resisted installation of a GPS in their cabs, and Bernstein suggests that she wishes others would have pushed more for privacy rights with respect to monitoring of on-duty activities.[256] Employers may not need to monitor employees' actions, even when working off-site, because they should be able to tell from the employee's work product whether he or she is performing job duties adequately.[257] Even when an employee is self-reporting, telephone calls to clients or customers to ascertain their level of satisfaction would be equally effective and less invasive in terms of the employees' right to privacy. One might even protest that using such monitoring devices is equivalent to scientific management, or Taylorism; it may increase efficiency but does so at too significant a human cost.[258] These concerns would provide an adequate basis for including some additional safeguards in protective legislation or policies.[259]

---

253 *See* Embarq, 123 Lab. Arb. Rep. (BNA) at 930, 932. In this case, a new supervisor was conducting a routine review of GPS reports which led her to investigate prior GPS reports. *See id.* at 930.

254 Although GPS can in some ways be more intrusive than video surveillance because its mobility enables it to record every action, in some ways it is less invasive because it does not photograph the person's actions for posterity.

255 *See* Finkin, *supra* note 21, at 503–04 (asserting that "the additional features of technology that make it more pervasive, all-seeing and all-knowing, never forgetting (or forgiving), become legally irrelevant" despite the fact that a "company could scarcely have assigned a supervisor to each employee to observe (and record) his or her every motor movement . . . at every moment throughout the work day").

256 *See* Bernstein, *supra* note 12, at 925 ("One might argue . . . that observation via closed-circuit television camera is worse than the human-on-human snooping to which Selmi compared it if only because a video image of a face can be re-wound and replayed, edited, enlarged into grotesque nostril-boring expansion, whereas the human snoop gets nothing to exploit beyond his glance.").

257 For instance, many lawyers prefer to be judged on output rather than a log of "billable hours."

258 *See* Sprague, *supra* note 96, at 1.

259 For instance, a policy could reasonably require consistent enforcement of the monitoring and rules governing infractions, reasonable suspicion of a particularized wrongdoing before monitoring, trying other methods of enforcing rules before implementing GPS monitoring, or compensation for an invasion of privacy.

b. Surreptitious Surveillance of On-Duty Conduct

One decision suggests that surreptitious use of a GPS is generally unwarranted.[260] The company suspected the employee, who worked off-site, of not being at work during work hours because when a manager discovered the employee was absent, the employee reported being in his car using his cell phone.[261] The company thus installed a GPS system into the company vehicles of employees who worked off-site.[262] The arbitrator reasoned that the company failed to fulfill its obligations to the grievant when it used the GPS without notifying employees of the system and of "the consequences of abuse of company time."[263] The decision implies that notice of the GPS system would not detract from the purposes of tracking employees and improving productivity.[264]

Indeed, one reasonable framework of privacy protection would be to require that all surveillance of on-duty activity be performed pursuant to the safeguards discussed above in Sub-Section VII.C.2.a. While, as discussed below, this framework might limit employers' ability in certain instances to verify wrongdoing or discover who committed an infraction, it would generally enable them to monitor employees and to thereby prevent infractions from occurring.

However, another arbitrator did not object to surreptitious surveillance of an employee's conduct while on duty, even when the surveillance captured content that the employee was viewing.[265] The arbitrator implied that "testimonial or documentary evidence obtained through a nonconsensual search" is appropriate " 'so long as the methods employed are not excessively shocking to the conscience of a reasonable person . . . .' "[266] The employer had printouts evidencing that an employee had used a computer for personal reasons without authorization in violation of a company rule. Thus, the employer set up a camera to capture photos of the computer misuse. The arbitrator admitted the photos that were intended to capture the misuse of the computer but ultimately captured other conduct, including viewing of what appeared to be pornographic digital versatile/video disks (DVDs), which violated company policy.

Another case suggests that surreptitious monitoring is appropriate when there is a known violation but no knowledge of who has engaged

260 *See* Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) at 1391.

261 *See id.* at 1389.

262 *See id.*

263 *Id.* at 1391.

264 *See id.* at 1388.

265 *See* Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) at 262.

266 *Id.* at 260 n.2 (quoting DISCIPLINE AND DISCHARGE IN ARBITRATION 337 (Norman Brand ed., 1998)).

in the violation.[267] The arbitrator upheld discipline of an employee who had been captured smoking, in violation of the hospital employer's rules, by a web-cam video device.[268] The arbitrator did not address the lack of notice to employees of the hidden camera.[269]

The "excessively shocking to the conscience standard," when coupled with a non-particularized search, would condone almost unlimited surreptitious surveillance of employees at the workplace. Yet, if the goal of surveillance is to monitor productivity, there is no necessity that it be secret from the employees.

If, on the other hand, the goal is to verify wrongdoing, then surreptitious monitoring would be unnecessary when sufficient proof of wrongdoing already exists. In the former case, for instance, the employer already possessed print-outs indicating an infraction on the employee's part. Employees should not live in fear that they will be singled out for surreptitious surveillance because of a workplace infraction.

If on the other hand, the employer's goal is to verify a reasonable suspicion of wrongdoing,[270] such as in a case where a co-worker made an allegation,[271] or to determine who has engaged in a known infraction, such as when a manager smells cigarette smoke, then surreptitious surveillance of on-duty conduct might be appropriate. In such instances, a number of other safeguards, in addition to the requirement of a reasonable suspicion, can be used to ensure adequate protection of an employee's privacy. Additionally, the quality of the evidence, discussed below in Sub-Section VII.C.2.c, is an important safeguard.

For instance, an employer might provide notice that it will monitor when it has a reasonable suspicion to do so. The notice should explain what constitutes a reasonable suspicion, such as a statement from a co-worker or evidence of an infraction that is not attributable to a specific individual. An employer should also notify employees of the types of

---

267 *See* Montgomery Gen. Hosp., 122 Lab. Arb. Rep. (BNA) 949 (2006) (Coyne, Arb.). This is a public sector case and to some extent the public nature of the employer did contribute to the decision.

268 *See id.* at 953.

269 *See id.*

270 *Cf.* Albertson's Inc., 115 Lab. Arb. Rep. (BNA) at 886 (holding that there was no reasonable suspicion proved where supervisors relied on rumors that employee was wearing her tongue ring but did not see "silver or gold-colored flashing in her mouth" or observe her putting her hand across her mouth when speaking to them; direction to stick out tongue inappropriate).

271 *See* Xcel Energy, 119 Lab. Arb. Rep. (BNA) at 26 (explaining that employer audited grievant's computer usage for approximately twenty-day period when co-worker anonymously complained that grievant was viewing child pornography). Arguably an anonymous complaint would not rise to the level of creating a reasonable suspicion. *Cf.* Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) at 278 (implicitly questioning appropriateness of relying on complaints of inappropriate e-mail to launch investigation of employee's e-mail and terminate him based upon findings when those complaining are not identified).

infractions that will be monitored. Employers should consistently enforce such a policy so that employees know that periodic surreptitious monitoring takes place.

Alternatively, an employer might be permitted to monitor when it has a reasonable suspicion of wrongdoing and has exhausted other methods of verification or discovery, such as visual observation or inquiries of employees, before resorting to surreptitious surveillance.[272] In such an instance, providing a compensatory remedy to the employee for the invasion of her privacy would be an additional appropriate safeguard because of the surreptitious nature of the monitoring.[273]

c. The Quality of the Evidence

Arbitrators recognize that documentary evidence of surveillance must be assessed according to the quality of the photograph or report and in light of other circumstantial evidence.[274] In one case, for instance, the arbitrator found that a photograph did not prove the grievant was masturbating, as asserted by management, when considered in the light of the grievant's credible testimony to the contrary.[275] In another case, the arbitrator concluded that "grainy" black-and-white photos were not enough, standing on their own, to prove the misconduct.[276] But, in light of management's credible testimony, the photos were sufficient proof.[277]

GPS reports are treated similarly. In one case, the reports did not establish a time-line of the grievant's work day.[278] But they did sufficiently establish a conflict between the time logged by the grievant as spent at customers' premises and the time actually spent at the customers' premises.[279]

One potential way to ensure the accuracy and reliability of the information collected, upon which discipline is based, is to provide employees the right to review and contest the information.[280] In fact, general arbitral principles providing an employee the opportunity to respond to alle-

---

272 Each of these has considerable drawbacks as they are unlikely to catch the violation and may notify the violator to switch to a different area or method. Then again, it may put the violator on notice to stop, which is the desired result.

273 To the extent the surveillance includes an auditory component—capturing conversations—it is more appropriately governed by the frameworks discussed in the next section.

274 *See* Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) at 262.

275 *See id.* (explaining that the grievant asserted he was cleaning a boil).

276 *See* Montgomery Gen. Hosp., 122 Lab. Arb. Rep. (BNA) at 951.

277 *See id.*

278 *See* Embarq, 123 Lab. Arb. Rep. (BNA) at 930.

279 *See id.* at 930, 931.

280 European law requires that employees be provided a copy of the information gathered by monitoring. *See, e.g.*, Council and European Parliament Directive 95/46/EC, Recitals 2, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice_home/fsj/privacy/law/index_en.htm.

gations of misdeeds support such a solution.[281] Indeed, in one case, an arbitrator found that the employer's failure to review video surveillance of the employee and provide the employee an opportunity to respond provided one reason for overturning the employee's dismissal.[282]

3. Monitoring of Employees' Computer Usage

This sub-section addresses monitoring of employees' computer usage, as an example of monitoring of employees' thoughts and communications on-duty. Monitoring of the content of employees' e-mail most obviously falls in the category of monitoring employees' thoughts and communications.

Monitoring the types of websites visited by particular employees also relatively clearly monitors employees' thoughts. In some ways, such monitoring is similar to monitoring an on-duty off-site employee's travel because it captures instances when the person stops at a "place" that is not work-related. But monitoring website use is much more likely than monitoring actions to disclose personal non-business related thoughts or conduct. There is wide discretion in the number and types of websites an employee might visit while working. For this reason, monitoring of website usage is addressed by the framework proposed in this section. Additionally, one unitary policy governing computer usage is more readily understandable for employees than two different ones.[283]

This section discusses personal use of company computers, employees' right to privacy when using a company computer for personal reasons, types of employee uses that are appropriately prohibited by employers, open monitoring of employee computer usage, surreptitious monitoring of employee computer usage, and discipline for computer usage. While it finds that arbitrators sometimes uphold rules prohibiting personal use of company computers, it proposes that the better default position is that employees should not be prohibited from using computers for personal reasons. It then outlines types of personal use which an

---

281 *See* Bud Indus. Inc., 124 Lab. Arb. Rep. 908, 914 (BNA) (2007) (Miles, Arb.) ("It is generally recognized in the arbitral arena that in order to satisfy industrial due process, an employee 'must be given an adequate opportunity to present his or her side of the case' before being disciplined.") (quoting ELKOURI & ELKOURI, *supra* note 193, at 967, 969); Penn Window Co., 120 Lab. Arb. Rep. (BNA) at 303 ("[J]ust cause requires that employees against whom management is considering discipline first be allowed a meaningful opportunity to refute the allegations made against him (sic.), or explain or excuse his conduct.").

282 *See* Bud Indus. Inc., 124 Lab. Arb. Rep. (BNA) at 914.

283 Monitoring of only the number of e-mails or websites viewed would have less of a tendency to reveal personal thoughts, communications, or conduct. To the extent the technology is available and employers are interested in that type of monitoring, it could be appropriately governed by the frameworks discussed in the former section. Because it is most expedient, however, to treat all monitoring of computer use in one section, all such monitoring is addressed herein.

employer might legitimately prohibit and suggests certain safeguards for monitoring solicitation and messages disrespectful of management. Next it addresses excessive computer use. Finally, the section proposes a framework to adequately protect employees' privacy from both open monitoring and surreptitious monitoring, including the safeguard of mitigating discipline due to the private nature of behavior.

a. Personal Use of Company Computers

Some arbitrators uphold employer rules forbidding personal use of company computers so long as progressive discipline is followed.[284] For instance, in one case, an arbitrator upheld a termination when the employee's own conduct of printing personal e-mails led to the discipline.[285]

Yet in today's typical workplace, forbidding personal use of company computers appears out of sync with modern workplace reality. Many workplaces are computerized and many employees, whether professional or not, have access to computers, including one specifically designated for their use.[286] Additionally, many employees spend more time at work than before.[287] This necessitates occasional performance of personal tasks on work time, such as answering an e-mail. Employees also increasingly spend time at home working.[288] Thus it seems only fair that employees, especially when salaried, should spend a minimum amount of time at work performing personal tasks.[289] Moreover, many employees have "down-time" at work, such as a receptionist who has

---

284 *See, e.g.*, Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) at 262; A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371, 1375 (2004) (Nathan, Arb.) (upholding termination where employees were "repeatedly advised against using the computer for personal business and especially not to use it to download or transmit pornography"); Alliedsignal Engines, 106 Lab. Arb. Rep. (BNA) 614 (1996) (Rivera, Arb.) (upholding rule at non-union employer prohibiting distributing written material via e-mail system but reducing termination, for this violation and others, to last-chance agreement); City of El Paso, 123 Lab. Arb. Rep. (BNA) 691, 695, 696 (2006) (Greer, Arb.); Conneaut Sch. Dist., 104 Lab. Arb. Rep. (BNA) at 914 (where rule is enforced, employer may appropriately preclude employees from using the computer and e-mail system for personal reasons, including exchanging recipes with co-workers). *See also* related discussion on limiting computer use to non-work time, *infra* Section VII.C.3.d.

285 *See* Kuhlman Elec. Corp., 123 Lab. Arb. Rep. (BNA) at 262.

286 *See* A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) at 1373 (describing production process where "[m]uch, if not most, of the production process involves the use of computers" and maintenance shop containing two information terminals used by maintenance employees); Hirsch, *supra* note 97, at 274 ("A 2003 survey estimated that forty percent of all workers used the Internet or e-mail at work."); Finkin, *supra* note 21, at 474 & n.17 ("A 1999 survey indicated that a third of employees spend time surfing the Net while at work").

287 *See* Sprague, *supra* note 96, at 27 & n.219; Gely & Bierman, *supra* note 53, at 76.

288 *See* Sprague, *supra* note 96, at 27 & n.219.

289 *Cf.* Rustad & Paulsson, *supra* note 30, at 891 (discussing how the French legal institution, Le Forum des droits sur l'Internet, concludes that "it is only fair" to permit employees to use the Internet at work for personal use because the "employer benefits from having his

completed the filing and is waiting for the next call, or a parking attendant waiting for the next vehicle to drive in.[290] Using a computer during down-time does not detract from the employee's work any more than reading a book would.

Preventing employees from using a computer on the logic that it takes away from work-time does not withstand scrutiny.[291] Most people can spend a short time at work doing personal business without any impact on their work performance. If an employee is spending excessive time on a computer, an employer should be able to tell by a decrease in work performance. At a minimum, the employer with a reasonable suspicion of excessive employee computer use could appropriately launch an investigation, including monitoring of personal usage. As reasoned by one arbitrator, occasional performance of personal tasks does not necessarily impact an employee's job performance.[292] The grievant, a law enforcement officer, had met on more than one occasion with his girlfriend, had his picture taken with acquaintances, permitted acquaintances to sit in his cruiser, and made "a bogus traffic stop" of his soon-to-be girlfriend.[293] The arbitrator concluded that personal actions during work-time did not constitute neglect or inattentiveness to duty when there was no "affirmative evidence of factual instances of neglect or inattention to duty."[294] He so reasoned even in the law enforcement context where the arbitrator believed personnel are held to a higher standard in "the performance of their duties than employees in the private sector."[295] Moreover, a rule that prohibits all personal use opens the door to simply utilizing an employee's personal use discriminatorily to "get rid" of an employee for other reasons.

Likewise, to assert that concerns about work-time use justify an outright ban on personal use is overreaching. Providing for limited personal use should not overburden the computer system. If the system shows an unacceptable overall level of use, then employees can be directed to minimize use in order to maintain a working system.[296]

---

employees connected and available via the Internet at all times" including sometimes through portable computers and cell phones).

290 *See, e.g.*, Georgia Power Co., 123 Lab. Arb. Rep. (BNA) at 939 (noting that grievant spent much time "in a relatively private location" waiting for assignments and employees frequently spent "a lot of time" on the computer when there was no work).

291 *See* Franklin County Sheriff's Office, 124 Lab. Arb. Rep. (BNA) 654 (2007) (Bell, Arb.).

292 *See id.*

293 *See id.* at 660.

294 *Id.* at 662.

295 *Id.* at 661.

296 Technology is available that would permit an employer to block the downloading of MP3's, streaming video, or other large files if the bandwith of the system is insufficient to support such usage. Alternatively, an employer could monitor for downloading of such mate-

Thus, the default rule should be that employees are not prohibited from using computers for personal reasons.[297] If the employer can show that the nature of the work requires a workplace where "work is for work," and that employees work every minute on the clock and that no one uses company computers for personal reasons, then the employer might reasonably institute such a rule. If the employer can show some other reason that justifies such circumstances, such as an extremely limited computer capacity, then that too could be considered. But the burden should be on the employer to demonstrate a business necessity for a rule banning personal use because it is incongruent with the modern workplace to assert such a rule simply on the basis of property rights.[298]

b. Right to Privacy When Using Computer for Personal Reasons

One arbitrator has implied that employees do have a right to privacy in their computer usage. In the case, the arbitrator overturned the termination of an employee who had accessed computer files of another employee.[299] The arbitrator reasoned that "management has, by contract (seniority clauses, etc.), given the employees rights to their jobs under decent working conditions."[300] The arbitrator found that the grievant's supervisor had created indecent working conditions, causing union membership in his department to increase from three members, which was about twenty-five percent, to thirteen, which was one hundred percent. One of the indecent working conditions cited was the monitoring of the employees' computer usage. One employee testified, "We were scrutinized completely . . . . Our group was being held to a higher standard than anybody else as far as computer usage . . . [O]ur group was being investigated . . . . We referred to it as the Gestapo."[301]

---

rial consistent with the protections for employee privacy discussed in this section if the system bandwith is insufficient to support such usage.

297 Indeed, some companies have policies permitting personal use. *See, e.g.*, Tesoro Ref. & Mktg. Co., 120 Lab. Arb. Rep. (BNA) 1299, 1301 (2005) (Suntrup, Arb.) (Communications policy permits "[l]imited, occasional or incidental personal, non-business use.").

298 Employers may wish to prohibit employees from using personal e-mail accounts while at work. For example, one policy, states, "Employees should only set up personal Internet access through their home computer for non-work related Internet activities. These accounts should not be accessed using Company equipment." Xcel Energy, 119 Lab. Arb. Rep. (BNA) 26, 29 (2003) (Daly, Arb.). The rationale behind such a prohibition is unclear. Perhaps the employer does not want the employee engaged in personal work on the company computer. That unrealistic goal is discussed above. To the extent use of a personal account is justified by some type of business necessity, the proposals for safeguards discussed below would appropriately apply to monitoring to ensure employees are not using personal e-mail accounts.

299 *See* Boeing-Irving Co., 113 Lab. Arb. Rep. (BNA) 699, 704 (1999) (Bankston, Arb.) (quoting ELKOURI & ELKOURI, HOW ARBITRATION WORKS 803 (5th ed. 1997)).

300 *Id.*

301 *Id.* at 702.

But other arbitrators have assumed that e-mails are not private unless employer policy explicitly affords such protection.[302] For example, one decision involved an employee who opened his supervisor's e-mails while seated at his supervisor's computer.[303] The arbitrator assumed that the supervisor had no right to privacy in his e-mail.[304]

Not only do many employees use company computers for personal use, but they often believe that their communications will remain private when they do so.[305] They may reason that everyone is using the computer for personal reasons and no one has ever had their e-mail monitored or been punished for so doing.[306] Additionally, they may believe

---

302 *See, e.g.*, Monterey County, 117 Lab. Arb. Rep. (BNA) 897, 900 (2002) (Levy, Arb.); PPG Indus., 113 Lab. Arb. Rep. (BNA) at 840 (indicating that arbitrator might find a privacy right if management had told the grievant the e-mail was private). Even one union agreed that certain uses of company e-mail system, such as by the union for representational purposes, are not private. *See, e.g.*, Sycamore Bd. of Educ., 123 Lab. Arb. Rep. (BNA) at 1589, 1589 (finding an e-mail sent by an employee collecting information for a grievance was clearly not private where CBA provided "The Association and/or its members may use e-mail with no prior approval rights, but no expectation of privacy or security.").

303 *See* Monterey County, 117 Lab. Arb. Rep. (BNA) at 900.

304 *See id.* This arbitrator fairly nearly adopted the dualistic framework proposed by Selmi because he also concluded that an affair with a co-worker was permissible, in part because it occurred during non-working time. *But see* Hoosier Energy Rural Elec. Coop., 116 Lab. Arb. Rep. (BNA) 1049, 1050 (2001) (Cohen, Arb.) (reasoning that a supervisor has a right to privacy in his office, desk, letter files, and computer files).

305 *See* Jonathan D. Glater, *A Company Computer and Questions About E-Mail Privacy*, N.Y. TIMES, June 27, 2008, at C1 ("People disclose all manner of personal information in e-mail messages, in the expectation—perhaps unfounded—that what they type will remain confidential. Companies often adopt policies explicitly stating that everything an employee does on a computer provided by the employer is subject to monitoring. But even so, and especially in the absence of such a policy, employees may have a reasonable expectation of privacy . . . ."); Rustad & Paulsson, *supra* note 30, at 830 (noting "widespread misconception" that e-mail is as private as postal mail). One case raises an interesting question of whether an employee can install a password on his computer which prohibits management from using the computer. *See* Saint Gobain Norpro, 116 Lab. Arb. Rep. (BNA) 960 (2001) (Fullmer, Arb.). The arbitrator concluded that the company owned the computers and had a management right to forbid installation of passwords. *See id.* at 967. Indeed, while protection for employees' privacy in personal use of their employer's computer is appropriate, allowing an employee to prohibit the employer any access to the computer is not. At a minimum, the employer may need such access to maintain its equipment. Further there are instances where the employer needs to access the computer to perform work. Additionally, even if only the assigned employee performs work on the computer, the employer may have a need to access work-product, as opposed to personal e-mail or folders, on the computer. Adequate privacy protections need not interfere with these legitimate employer interests. *Cf.* Arkansas Educ. Ass'n., 118 Lab. Arb. Rep. (BNA) 1540 (2003) (Moore, Arb.) (interest arbitration rejecting proposal that employees perform routine maintenance on assigned computers and supporting proposal where computers are sent to appropriate location for employer to make changes).

306 *See, e.g.*, Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) 271, 275 (2001) (Goodstein, Arb.) (finding that past practice of permitting use of e-mail for non-business related activity "completely negated" its written policy to the contrary); *cf.* Alliedsignal Engines, 106 Lab. Arb. Rep. (BNA) 614, 624 (1996) (Rivera, Arb.) (noting that where grievant in non-union setting sent his newsletter via e-mail "the past practice of the Employer that allowed, over a

that while the employer might for some reason decide to view a personal e-mail, they would not be disciplined for its content.[307]

Statements that an employee has "no expectation of privacy regarding personal information they have stored on or sent from Company equipment"[308] or that management "reserves the right" to monitor computer usage are unlikely to dispel employees' beliefs in the privacy of their electronic communications when no conduct of the employer evidences otherwise. Instead, more effective protections for the privacy of employees' personal computer use are necessary.

c. Prohibited Types of Personal Use of Company Computers

While there is generally no justification for monitoring to ensure that employees are not utilizing computers for personal use, monitoring to ensure that employees are not utilizing computers for certain prohibited uses can be appropriate. An employer has a legitimate business interest in prohibiting certain computer uses that are likely to negatively impact the business or workplace. When such monitoring takes place, it should, however, be subject to a framework of safeguards that provides suitable protection for an employee's right to privacy.[309]

The arbitration decisions disclose several types of computer use that are likely to negatively impact the business or workplace. Employers might reasonably prohibit use that is likely illegal,[310] such as downloading images of child pornography.[311] An employer should not have to tolerate use of its equipment for illegal purposes or risk responsibility for its employees' illegal conduct.[312] Employers might also reasonably prohibit computer use that would be unlawful, such as a defamatory communication.[313]

---

ten year period, the publication of the offending newsletter lulled the Grievant into a false sense of security.").

307 The belief of an employee who made a racist remark in the privacy of the backroom, or of a woman who sent a racist e-mail, she believed to be anonymous, to a chat room are examples of similar beliefs. *See* MT Detroit, 118 Lab. Arb. Rep. (BNA) 1777 (2003) (Allen, Arb.); King Soopers, Inc., 120 Lab. Arb. Rep. (BNA) 501 (2004) (Sass, Arb.).

308 Xcel Energy, 119 Lab. Arb. Rep. (BNA) 26, 28 (2003) (Daly, Arb.).

309 *See* discussion *infra* Parts C.3.e– f.

310 *See, e.g.*, Sycamore Bd. of Educ., 123 Lab. Arb. Rep. 1588, 1599 (BNA) (2007) (discussing how although the employer may not generally interfere with the union's right, once employer grants the right to use the computer system, employer may restrict the use of the e-mail for unlawful purposes).

311 *See, e.g.*, Xcel Energy, 119 Lab. Arb. Rep. at 34.

312 *But see* Doe v. XYC Corp., 887 A.2d 1156, 1167 (N.J. Super. 2005) (holding that employer may be held liable for child pornography if it has reason to know the employee is using the computer to disseminate pornography).

313 *See, e.g.*, Tesoro Ref. & Mktg. Co., 120 Lab. Arb. Rep. (BNA) 1299, 1301 (2005) (noting policy that forbids electronic communications that are defamatory).

Employers might reasonably prohibit images of a racial or sexual nature that might offend co-workers. While there is far-ranging debate on the appropriateness of restricting people's right to free speech in order to promote the equality of women and racial minorities, it is well-established within the workplace that certain speech and conduct must be prohibited or else racial or sexual harassment might result. Prohibiting this category of racial or sexual images protects employers from liability.[314]

It is also fairly commonplace to prohibit statements and images that are racially or sexually offensive but do not rise to a legally-forbidden level.[315] And for purposes of a workable privacy policy, it is reasonable to permit employers to prohibit the entire category of images when appropriate safeguards to protect employees' privacy are in place. Racist statements and sexual pictures that are, inadvertently or purposefully, exposed to co-workers do have the potential to offend co-workers.[316] Such images can also contribute to a workplace that is inhospitable to women or minorities, despite not rising to the level of legally "hostile."[317] Additionally, society generally disapproves of these types of materials at work.[318] Moreover, it is likely easier and less expensive to monitor for

---

314 *See, e.g.*, Sycamore Bd. of Educ., 123 Lab. Arb. Rep. (BNA) at 1588 (discussing how although the employer may not generally interfere with the union's right, once the employer grants the right to use the computer system, the employer may prohibit the use of the e-mail to racially or sexually harass other employees).

315 *See* Tesoro Ref. & Mktg. Co., 120 Lab. Arb. Rep. (BNA) at 1301 (stating that employees must not "store or retrieve any communication of a discriminatory or offensive nature which are derogatory to any individual or group or which are obscene or defamatory. The viewing of Internet sites containing sexual material is strictly prohibited."); A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371, 1373 (2004) (Nathan, Arb.) (stating in its policy that e-mail and the Internet "may not be used to send or receive pornography or other inappropriate messages and/or materials."); MT Detroit, 118 Lab. Arb. Rep. (BNA) 1777, 1782 (2003) (Allen, Arb.) (upholding termination of employee who sent message with offensive racial language to a "chat room"); County of Sacramento, 118 Lab. Arb. Rep. (BNA) 699, 699 (2003) (Riker, Arb.) (prohibiting "sexually-related banter, jokes, propositions, and/or activities"); U.S. Dept. of Agric., 118 Lab. Arb. Rep. (BNA) 1212, 1216 (2003) (Cook, Arb.) (upholding five day suspension for viewing sexually explicit web pages on employer's computer while off-duty); State of Minn., 117 Lab. Arb. Rep. (BNA) 1569, 1573 (2002) (Neigh, Arb.) (upholding termination because viewed more violent and disturbing pornography than other employees); S. Cal. Edison, 117 Lab. Arb. Rep. (BNA) 1066, 1072 (2002) (Prayzich, Arb.) (upholding suspension for e-mailing calendar that was offensive and where certain pictures violated the employer's equal opportunity policies, which were more prohibitive than required by law); PPG Indus., 113 Lab. Arb. Rep. (BNA) 833, 842 (1999) (Dichter, Arb) (concluding that sexual jokes sent to employees who did not take offense violated employer's sexual harassment policy).

316 *See, e.g.*, King Soopers, Inc., 120 Lab. Arb. Rep. (BNA) 501, 505 (2004) (Sass, Arb.) (the co-worker who reported the statement was offended by it even though the offending party did not mean to offend).

317 *See* Harris v. Forklift Sys., Inc., 114 S. Ct 367, 370 (1993).

318 *See* PPG Indus., 113 Lab. Arb. Rep. (BNA) at 844 ("[A]ll employers in today's day and age must insure that the work environment is free from the type of material that was in grievant's mailbox. It cannot close its eyes to what grievant did. Failure to act is unfair to

all types of sexual and racial images rather than having to develop a monitoring system that aims to monitor only those that amount to unlawful sexual or racial harassment.

On the other hand, there are reasons that a privacy policy may limit prohibited computer usage to unlawful harassment.[319] To the extent e-mails or Internet views are completely private, they do not have the potential to offend anyone.[320] And it is certainly debatable whether prohibitions of this type lead to inhospitable workplaces for employees,[321] or unnecessarily deprive them of rights of speech and privacy. Employer expense should not easily outweigh privacy. Nor does general social disapproval translate to the reality of many workplaces where the viewing of pornography is fairly common.[322] Furthermore, such private viewing is generally no more disruptive of the workplace than any other type of private conduct. If, for instance, an employee is permitted to read during work, it would appear unnecessary and overbearing to prohibit reading lewd books that contain no pictures.[323] One arbitrator concluded, for instance, that receipt by a computer systems manager of inappropriate and sexually explicit e-mails did not provide a basis for discipline.[324] The arbitrator found that "conclusionary remarks about

---

other employees and subjects the Employer to potential liability. An employer that fails to strongly address conduct like the grievant's is buying itself a lawsuit.").

319 Finkin, for instance, discounts an employer's need to monitor for racially or sexually offensive material. "[T]he speech involved must be so pervasive as to alter working conditions: A single display of a pornographic picture on a video terminal or the transmission of an ethnic or sexual joke to a limited number of people would not be actionable. And, as the Supreme Court of New Jersey was at pains to emphasize, there is no *duty* to monitor to assure that offensive remarks are not transmitted." FINKIN, *supra* note 43, at 281.

320 *See* Georgia Power Co., 123 Lab. Arb. Rep. 936, 946-47 (2006) (Nolan, Arb.) (holding that private viewing of pornography when no one else was present was not threatening or harassing and did not violate laws or create liability, but viewing such pornography did violate reasonable work rules).

321 *See* CYNTHIA ESTLUND, WORKING TOGETHER: HOW WORKPLACE BONDS STRENGTHEN A DIVERSE DEMOCRACY 158 (Oxford 2003) ("It is no answer to say—as defenders of harassment law sometimes do—that 'the workplace is for work.' As we have seen, the workplace is for much more than work, both in the lives of individual workers and in the society as a whole. The law should not adopt as its motto a proposition that would so impoverish social life.").

322 *See, e.g.*, A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371, 1376 (2004) (Nathan, Arb.) (union argued that "commonplace nature" of sexually explicit materials means that viewing pornography is not a "capital workplace offense").

323 Another interesting hypothetical to consider is whether an employer would prohibit an employee from storing pornographic magazines in his locker.

324 Monterey County, 117 Lab. Arb. Rep. (BNA) 897, 899-900 (2002) (Levy, Arb.). Another case indicates that personal use, including receipt of "earthy, candid, and disgusting" e-mails, does not constitute inappropriate use of the computer system. *See* City of Fort Worth, 123 Lab. Arb. Rep. (BNA) 1125, 1129-30 (2007) (Moore, Arb.). The applicable electronic communications use policy forbid certain specified uses, such as for harassment, and uses creating "the appearance of inappropriate use." *See id.* The arbitrator reasoned that "[w]hat may be one individual's art may be another's pornography." *Id.* He reasoned that the grievant did not generate the pictures, implying company time and resources were not used, and she did

breach of trust, abuse of position, and harm to public service are not established and are not substitutes for required just cause."[325]

An employer might reasonably prohibit the use for personal reasons of proprietary company information located on databases. For example, in one case, an arbitrator decided a one-day suspension would be appropriate when a deputy sheriff ran acquaintances' names through a law enforcement database containing motor vehicle and warrant information.[326] In another, an arbitrator imposed a suspension when an employee checked a social services database to verify that a complaint of child neglect had been filed against her.[327]

An employer might also reasonably prohibit solicitation.[328] While prohibiting certain solicitation is barred by federal law,[329] generally prohibiting employees from asking co-workers for money or support for non-work activities is justified. Co-workers might otherwise feel pressure to support a cause they do not believe in or to give money they would prefer to spend elsewhere. Additionally, employers might prohibit messages disrespectful of management.[330]

Any penalty imposed for violation of these latter two prohibitions should be mitigated by the private nature of any such message whether or not the monitoring is with notice to employees.[331] Employees are bound to privately make statements critical of management or their employers and bound to ask friendly co-workers to buy Girl Scout cookies. And the

---

not disseminate them, implying no co-workers were affected by them. *See id.* Thus, the grievant was reinstated and granted backpay. *See id.*

325 Monterey County, 117 Lab. Arb. Rep. (BNA) 897, 899-900 (2002) (Levy, Arb.).

326 *See* Franklin County Sheriff's Office, 124 Lab. Arb. Rep. (BNA) 654, 660-63 (2007) (Bell, Arb.).

327 *See* Montana Child and Family Servs., 122 Lab. Arb. Rep. (BNA) 656, 662 (2006) (Reeves, Arb.).

328 *See* Xcel Energy, 119 Lab. Arb. Rep. (BNA) 26, 29 (2003) (Daly, Arb.).

329 *See* Register Guard, 351 N.L.R.B. No. 70 (Dec. 16, 2007), 2007 NLRB Lexis 499, 12 (holding that employer may not prohibit only union-related e-mail messages of a certain type while permitting other messages of the same type, such as personal messages).

330 *See* Marine Corps Air Ground Command Ctr., 111 Lab. Arb. Rep. (BNA) 161, 162 (1998) (Gentile, Arb.) (concluding that disrespectful e-mail, stating grievant had "continued to tolerate the abuse and micro management of the Comptroller's shop," provided grounds for termination in conjunction with the more serious conduct of verbal threats against management).

331 The NLRA may prohibit employers from conducting surveillance for the purpose of finding certain messages that are concerted activity regarding terms and conditions of work. Finkin, *supra* 21, at 499. *But see* Register-Guard, 351 NLRB No. 70 (Dec. 16, 2007) (stating employers can prohibit use of computers for "non-job-related solicitations," including union solicitations, unless the employer discriminates by banning only some "organizational notices").

harm from such statements or requests is not as significant as that from the other types of prohibited computer usage.[332]

This list is not intended to be exhaustive on the topic of communications that an employer has a legitimate business interest in prohibiting because they are likely to negatively impact the workplace. For instance, using computers to copy trade secrets would fall within this category. Rather, this list provides a starting point, based on the arbitration decisions, for legislators, courts, and others to use in framing appropriate protections for employees' right to privacy.

d. Limiting Personal Use of Computer

Arbitration decisions suggest that employers have a legitimate business interest in ensuring that excessive personal computer use does not result in interference with successful job performance.[333] For instance, in one case, a campus police officer self-reported his work time, yet computer records revealed that he had been using another employee's computer during the time he was self-reporting the completion of checking the premise of one facility.[334] The amount of time spent on the computer indicated that it would have been impossible for him to have completed the necessary premise check, thus leaving the premise unchecked and unsecured.[335] The arbitrator upheld his termination.[336]

In fact, in one decision, there was no evidence that the quality of the grievant's work suffered, but an arbitrator upheld a twenty-four-hour suspension for "occasional to frequent" use of his work computer for "his personal metal fabrication business."[337] This misuse was proved not through records of monitoring, but through testimony of co-workers who observed the grievant using the computer for personal reasons.[338]

Additionally, several decisions suggest that personal use of computers can be limited to break time. For instance, in one case, the arbitrator found that it was appropriate to admonish a union representative for

---

332 *See*, *e.g.*, Sycamore Bd. of Educ., 123 Lab. Arb. Rep. (BNA) 1588, 1590–91 (2007) (discussing an e-mail which ridiculed a rule governing the number of posters a teacher could hang on the classroom walls).

333 *See, e.g.*, Univ. of Mich., 114 Lab. Arb. Rep. (BNA) at 1401 (when an employee has a history of abusing phone call privilege to make numerous personal phone calls during and after working hours, to the extent it negatively impacted his work, the employer could direct the employee not to make or receive personal calls while on break after discussing and attempting to resolve the issue with the union).

334 *See* Univ. of Chi., 120 Lab. Arb. Rep. (BNA) 88, 95, 96 (2004) (Briggs, Arb.).

335 *See id.*

336 *See id.*

337 City of El Paso, 123 Lab. Arb. Rep. (BNA) 691, 695 (2006) (Greer, Arb.).

338 *See id.* at 694; *see also* Hoosier Energy Rural Elec. Coop., 116 Lab. Arb. Rep. (BNA) 1043, 1048 (2001) (upholding termination for, among other reasons, using computer for non-work reasons for six to eight hours a week during work-time).

using the e-mail system during his work time to notify other members of a union meeting without first seeking the permission of management.[339] The arbitrator reasoned that the representative could not have been on his fifteen minute break at the time of day that he sent the e-mail.[340]

Another arbitrator also upheld limiting Internet use to break time. The grievant's supervisor saw him access the Internet for what appeared to be non-business reasons several times.[341] She also saw him call over other employees to view his computer screen and announce breaking news.[342] The supervisor requested an audit of the grievant's computer usage.[343] The audit disclosed that the grievant was repeatedly using the computer during work time for non-business related purposes, such as accessing websites of Ticketmaster, weather.com, the St. Petersburg Times, and USA jobs.[344] The arbitrator found that personal use was reasonably limited to break times because intermittent viewing of websites would be "disruptive and inefficient as to productivity."[345] As a result, it would likely adversely affect the employee's work performance, as the arbitrator found it had in the case.[346]

Generally, however, employees should not be limited to using the computer for personal reasons during break time. Sending a brief e-mail, such as the one at issue in the case regarding the union representative, is no more disruptive than saying hello to a passing co-worker or stopping to look around and give one's eyes a rest. If the level of personal use is significant, this should manifest itself in a reduction in the quantity or quality of an employee's work, as was apparent to the supervisor in the latter case.

Moreover, as some of these cases suggest, before conducting surreptitious monitoring of an employee for the purpose of discovering excessive computer use, the employer should have a reasonable suspicion that the employee is using the computer in a way that is likely to detrimentally impact his work. If there is no reasonable suspicion, there are no grounds to surreptitiously monitor the e-mail. And if there is already adequate proof of excessive use (such as in the case where co-workers testified about the metal fabrication business), no further monitoring is necessary. Additional safeguards for surreptitious monitoring of com-

339 *See* Dep't of Veterans Affairs, 118 Lab. Arb. Rep. (BNA) 1543, 1546 (2003) (Oberdank, Arb.). It is unclear by what method the e-mail was discovered by management, so whether it was open or hidden surveillance cannot be ascertained from the decision.

340 *See id.*

341 *See* Dep't of Veterans Affairs, 122 Lab. Arb. Rep. (BNA) 106, 108 (2006) (Hoffman, Arb.).

342 *See id.*

343 *See id.*

344 *See id.*

345 *Id.*

346 *See id.* at 111–12.

puter use are discussed below in Sub-Section VII.C.3.f. But in order to appropriately protect employees' privacy, the safeguard of requiring employers to use other means of verifying wrong-doing, such as assessing the quality or quantity of the employee's work, should be instituted when the purpose of the monitoring is to prove that use of work time for personal reasons is negatively impacting an employee's job performance.

e. Open Monitoring of Computer Use

One important safeguard suggested by the decisions is notice that employees are being monitored and notice of which types of content or actions are prohibited and being searched for.[347] Notice alone, however, is insufficient to protect employees' right to privacy in their personal computer use. Rather, the monitoring system must be used consistently and violations consistently disciplined so that a culture of engaging in prohibited conduct that is contrary to the written policy does not develop.[348] Several cases illustrate this safeguard.

For instance, one arbitrator found that because employees, including supervisors, routinely used the computer system to send e-mail for non-business related activities, including sending sexually-related jokes, a company's policy forbidding such use was "completely negated."[349] The arbitrator reasoned that failing to monitor for prohibited use and instead relying only on complaints of inappropriate use meant that employees "had a right to believe that what they are doing has been condoned by the Company."[350] The arbitrator suggested that "by spot checking the e-mail messages sent over the Company computers, from time to time, the Company could determine whether anyone was violating the Company's e-mail Policy."[351] The grievant's termination was reduced to a three-day suspension.[352]

Another arbitrator similarly decided that when supervisors "on a regular basis knowingly tolerated, condoned and joined" in sending e-mails which were inappropriate per a written policy, there was no just

---

347 *See* S. Cal. Edison, 117 Lab. Arb. Rep. (BNA) 1066, 1071 (2002) (upholding suspension for circulating offensive calendar via e-mail where employee was on notice of detailed and comprehensive equal opportunity policy that prohibited derogatory pictures and suggestive calendar displays).

348 *See* Xcel Energy, 119 Lab. Arb. Rep. (BNA) 26, 30–34 (2003) (Daly, Arb.) The complaint that ''pornography was one thing, but child pornography was something else," suggests that employees might commonly be viewing pornography without being "caught." Employees are not likely to come forward to testify to this because they are reluctant to identify themselves or their co-workers knowing that termination will result. *See* Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) 271 (2001) (Goodstein, Arb.).

349 *Id.* at 272.

350 *Id.*

351 *Id.* at 279.

352 *See id.* at 281.

cause for the grievant's termination.[353] The arbitrator reasoned that lax enforcement lulls employees into "a false sense of security."[354] Another case suggests that while some level of discipline might be appropriate when enforcement of a computer usage policy is not consistent, the resulting invasion of privacy must mitigate any discipline imposed.[355] The employer permitted an internal, non-Internet, communication system designed for use in emergencies to be utilized to notify employees when "muffins were being delivered to the office."[356] The arbitrator held that the non-emergency use mitigated the discipline of an employee who used the system to send sexually-explicit messages to a co-worker.[357]

In another decision, arbitrators recognized that the private nature of viewing prohibited content must mitigate the level of discipline imposed for the infraction.[358] The arbitrators concluded this was so despite the following facts: the employees knew that the company would monitor electronic communications, the grievant knew that viewing the content was prohibited, the grievant knew that he could be disciplined and possibly discharged, and the company had a consistent enforcement policy of monitoring for attempts to access inappropriate sites and instituting an investigation of all computer usage for all employees who attempted to access twenty or more inappropriate sites in one month.[359]

The union did not challenge the monitoring system on privacy grounds. The union did, however, contend that the company had not warned employees that it "was keeping a record of the number" of inappropriately accessed pages or that attempting to access twenty "might lead to investigation or discipline."[360] The arbitrators did not directly address the contention but did conclude that the company had warned employees that it would monitor electronic communications.[361]

The result of the case is a reasonable starting point for developing workable protections for employee privacy from monitoring of computer usage. It permits a type of generalized monitoring where certain employee conduct triggers scrutiny of the actual content of webpages

---

353 Snohomish County, 115 Lab. Arb. Rep. (BNA) 1, 7 (2000) (Levak, Arb.).

354 *Id.* (quoting DISCIPLINE AND DISCHARGE IN ARBITRATION 81 (Norman Brand ed., 1998)).

355 *See* County of Sacramento, 118 Lab. Arb. Rep. (BNA) 699, 701 (2003) (Riker, Arb.).

356 *Id.*

357 *See id.*

358 *See* Georgia Power Co., 123 Lab. Arb. Rep. (BNA) 936, 947 (2006) (Nolan, Arb.).

359 *See id.* The company used an outside vendor who provided a list of banned sites based on employees' internet usage. The company's monitoring system blocked access to these sites. *See id.*

360 *Id.* at 944.

361 *See id.* at 947 (the information on the policies provided is not sufficient to assess this conclusion; it only states that the company reserves the right to monitor, which is different than stating that the company will or is monitoring).

viewed and downloaded. Employees are notified that the monitoring is taking place and notified of which conduct constitutes infractions, and the monitoring is consistent (as presumably is imposition of discipline for infractions). And while employees are not notified of the specifics of the monitoring program, the private nature of the conduct serves to mitigate any discipline that can be imposed because the specific type of monitoring is not clear.[362] To ensure protection of the employees' privacy, the additional safeguards of having a confidential reviewer or limiting collection to that connected to the purpose of monitoring should also be implemented. For instance, in this situation, a confidential person would pull all websites that appeared related to pornography and would not report other personal matters, for instance paying an electric bill or checking library hours, to management.[363]

An alternative would be a policy where the employees were notified of the monitoring, notified of the particulars of the monitoring (such as the number of prohibited sites accessed and number of attempts that lead to greater scrutiny), and notified of the infractions (but not necessarily the level of resulting discipline). If such a policy was consistently enforced, so that employees were not lulled into a false sense of privacy, then there would be no mitigation of discipline due to the private nature of the conduct. The employees would be well-aware that they were being monitored and would be disciplined for prohibited conduct. Additional provisions would include confidential review so as to ensure that personal non-prohibited conduct was not reported to management or restricted monitoring to gather only the type of communication or information prohibited.

f. Surreptitious Monitoring of Computer Use

Several cases suggest that surreptitious review of computer usage is appropriate when there is a reasonable suspicion that a violation of com-

---

362 Some arbitrators have, however, considered the private nature of the conduct to be an aggravating, rather than a mitigating factor. In a case where an employee sent pornographic e-mails to co-workers and others "at night or other times when only one supervisor was in the plant," the arbitrator considered this to support upholding termination. *See* A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371, 1375 (2004) (Nathan, Arb.).

363 The confidential reviewer could disclose other violations that were incidentally discovered to management. In one case an employer promised an employee confidentiality when interviewing her as part of a sexual-harassment investigation. The employee disclosed that she had used an internal computer system to send sexually explicit messages to a co-worker. The interviewer stated that the information she provided would not "be reported to her supervisor or co-workers, unless there was a need to know." The arbitrator reasoned that the one-day-suspension of the employee should be reduced to a written reprimand, in part because it was based on her confidential disclosures. *See* County of Sacramento, 118 Lab. Arb. Rep. (BNA) 699, 702 (2003) (Riker, Arb.).

pany policy has taken place.[364] In one case, the policy permitted "limited, occasional or incidental personal, non-business use."[365] It prohibited storing or retrieving discriminatory, offensive, derogatory, obscene, sexual, or defamatory communications.[366] The policy also indicated that the company did not intend to strictly monitor the computer system, but that it reserved the right to do so.[367] In particular, the company might do so to ensure an employee's usage complied with the law and company policies or when the company had a business need to monitor.[368] The policy warned that abuse of the policy would subject an employee "to disciplinary action without further warning, up to and including discharge . . . ."[369] In the particular case, a co-worker had e-mailed members of the bargaining unit, including the grievant, warning them not to access pornographic sites because he had been disciplined for doing so.[370] The grievant was, thus, arguably provided notice that infractions were being disciplined. Human resources instigated an investigation of the grievant's computer usage when he posted a hate group's poster, with a Uniform Resource Locator (URL) address indicated, on the company bulletin board. Human resources discovered that the grievant had accessed hate sites and pornographic sites "innumerable times."[371] The arbitrator upheld his termination based on the misuse of the computer system and additional misconduct.

---

364 *See, e.g.*, Dep't of Veterans Affairs, 122 Lab. Arb. Rep. (BNA) 106, 108 (2006) (Hoffman, Arb.) (supervisor observed grievant repeatedly using computer for non-work related matters and calling other employees over to view his computer or announcing news to them and so requested a review of his internet usage); Dep't of Veterans Affairs, 122 Lab. Arb. Rep. (BNA) 300 (2005) (Petersen, Arb.) (e-mails evidencing a slowdown were discovered when someone alleged harassment and defamation; the arbitrator reduced the discharge to a written reprimand because that was the penalty for a slowdown under the employer's progressive discipline policy); Tesoro Ref. & Mktg. Co., 120 Lab. Arb. Rep. (BNA) 1299, 1303 (2005) (investigation where employee posted hate group poster with listed URL); A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371 (2004) (Nathan, Arb.); MT Detroit, 118 Lab. Arb. Rep. (BNA) 1777 (2003) (Allen, Arb.) ("chat room" operator informed company that an employee had posted a message containing offensive racial language); State of Minn., 117 Lab. Arb. Rep. (BNA) 1569 (2002) (Neigh, Arb.) (extensive investigation of chain of pornographic e-mails and related computer use based on complaint from one employee that she viewed a naked woman on co-worker's computer screen); *cf.* Union-Scioto Local Bd. of Educ., 119 Lab. Arb. Rep. (BNA) 1071,1075–76 (2004) (concluding that grievant had diminished expectation of privacy when engaging in conversation on employer property during work-time but that, nevertheless, discipline was inappropriate where employer surreptitiously and selectively videotaped conversation without any evidence of misconduct by grievant).

365 Tesoro Ref. & Mktg. Co., 120 Lab. Arb. Rep. (BNA) 1299, 1301 (2005) (Suntrup, Arb.).

366 *See id.*

367 *See id.* at 1302.

368 *See id.*

369 *Id.* at 1302.

370 *See id.* at 1306.

371 *Id.*

Another arbitrator explicitly found no privacy violation of an employee's rights in a case involving similar facts.[372] The arbitrator concluded that employees have no expectation of privacy, even when using an individualized e-mail password, because an employer has a right to see "material that would be confidential to others" and the company provides the computer access to the employee.[373] The arbitrator also concluded, however, that the grievant could not be disciplined for bypassing a firewall because the employer provided insufficient notice that a purpose of the firewall was to exclude pornographic material.[374]

In addition to requiring a reasonable suspicion of an infraction, these cases suggest several other potential safeguards. They suggest that notice of the type of conduct that will constitute an infraction and the potential level of resulting discipline for an infraction is important. They also suggest that notice that monitoring will take place when the employer has a reasonable suspicion of an infraction can be an appropriate safeguard. Finally, they suggest that notice of the particulars of the monitoring system also serves as an important safeguard.

Indeed, while surreptitious review of e-mail may be appropriate when an employer has a reasonable suspicion of an infraction, additional safeguards should be mandated to protect an employee's privacy. Employees should be notified of potential infractions and the discipline that might result from engaging in any infraction. As discussed with open monitoring, the collection should be performed by a confidential employee or limited to review of usage that appears to relate to the infraction suspected because the review is likely to disclose personal information and an employee's private thoughts.[375]

Additional safeguards might work in combination. For example, the employer should first try other avenues of confirming the supposed infraction, such as via interviews of co-workers. The employer should compensate the employee for the invasion of privacy, because the employee was not on notice that her thoughts might be reviewed. Addition-

---

372 *See* PPG Indus. Inc., 113 Lab. Arb. Rep. (BNA) 833, 840 (1999) (Dichter, Arb.). The employer investigated the employee's e-mail based on a co-worker's complaint. *See id.* The investigation of the chain of e-mails led the employer to change the grievant's password in order to access his e-mail. *See id.* Therein, the employer discovered hard-core material which had been e-mailed from grievant's home computer, and to other employees and an employee of an independent contractor. *See id.* The arbitrator did not uphold the discharge, however, instead providing reinstatement (after nine months leave) with no back-pay. *See id.* The privacy challenge was purportedly launched under the Electronic Communications Privacy Act. *See id.*

373 *Id.*

374 *See id.* at 842.

375 The confidential employee could also report violations that were not the focus of the investigation, so under that type of review, the initial case where discipline was imposed for a slow-down based on review for defamation would be possible.

ally, the private nature of the conduct should mitigate any discipline imposed.[376]

Alternatively, the employer could notify employees that it will monitor e-mails and computer usage when it has a reasonable suspicion of an infraction and clearly notify the employees of the particulars of the monitoring system that will be used, as well as resulting infractions.[377] Notice that it "reserves the right" to monitor, or may monitor, should not suffice. An employer should enforce the policy in order to notify employees that such monitoring is taking place. The notice would indicate that the invasion of privacy was not as severe, suggesting that either mitigation of the discipline or compensation for the injury would suffice as an appropriate safeguard.

Another case erroneously suggests that reasonable suspicion, without other safeguards except notice that the conduct is prohibited, provides an adequate basis to monitor employees, at least in circumstances involving "hard core" pornography.[378] In the case, a company was investigating an employee and discovered that employees were e-mailing pornography.[379] The grievant was terminated for sending "hard core" images to other employees and people outside the plant, and sometimes introducing them to the company system by e-mailing them from his home computer. The arbitrator upheld the discharge, reasoning that the conduct was "so discredited in the workplace" that the grievant need not have been told it could lead to discharge.[380]

The arbitrator in this case so ruled despite widespread pornographic communication through the system and the lack of warning that such communication could result in discharge.[381] While the number of employees in the plant was not specified, the employer had already "uncovered" twenty-five employees sending pornographic messages in a plant with one hundred and forty computers.[382] The arbitrator conceded that there was "some merit" to the argument that "the conduct had been going

---

376 An exception could be provided that the private nature of the conduct would not mitigate discipline when the monitoring was based on a reasonable suspicion of excessive personal use.

377 All the safeguards discussed in the paragraph before the preceding one would equally apply.

378 *See* A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371, 1374 (2004) (Nathan, Arb.).

379 *See id.*

380 *See id.* at 1375; *cf.* PPG Indus., 113 Lab. Arb. Rep. (BNA) 833, 843 (1999) (Dichter, Arb.) ("There can be no doubt that even apart from any Rule violations what grievant did exceeds the bounds of propriety and warrants discipline."); State of Minn. Dept. of Admin., 117 Lab. Arb. Rep. (BNA) 1569 (2002) (Neigh, Arb.) (upholding termination because the grievant viewed more violent and disturbing pornography than other employees).

381 *See* A.E. Staley Mfg. Co., 119 Lab. Arb. Rep. (BNA) 1371, 1374 (2004) (Nathan, Arb.).

382 *See id.* at 1374.

on for so long that the employees were impliedly led to believe that it would not give rise to grave discipline."[383]

Nevertheless, the arbitrator believed the company had been damaged in four respects: misuse of equipment, wasting "time for which [the grievant] was being paid," disrupting "the efficiency of other employees," and exposing the company "to risks of liability and disruption of its overall system."[384] He concluded, "The grievant was potentially exposing the Company's email system to the purveyors of pornography who might have gained access to the larger system and infected the network with their filth."[385]

Misuse of equipment does not, however, standing on its own, damage an employer. For instance, if a person needs to stop a leak in the ceiling from dripping on the floor and the only receptacle around is a waste paper basket, then the basket's misuse as a rain catcher would not damage the company. Likewise, if an employee needs to send a personal letter and takes an envelope, but replaces it with one from home the next day, the envelope has been misused but the harm is minimal, if any.

Wasting time or disrupting co-workers' efficiency does harm the employer but is generally evidenced in a lack of quantity or quality of production.[386] Limited computer use does not waste any more time than many other personal activities prevalent in the workplace, such as chatting with co-workers or listening to the radio. Even if the conduct did waste a significant amount of time, the violation of privacy would outweigh that waste if the monitoring was not conducted with appropriate safeguards.

It is unclear what is meant technologically by "disruption of the system" and "purveyors of pornography who might have gained access to the larger system and infected the network with their filth." It might indicate spammers, spy-ware, or even viruses. One might surmise, however, that spammers are no more likely to invade a system based on e-mailing employees, a home e-mail address, or friends than they are based on business related e-mail.[387] And any time one accesses the web for business or other reasons, one risks infection by virus or spy-ware. Most systems have protection from all of these potential "invaders," and it is doubtful that the risk of personal e-mail, even if pornographic in nature, poses such a risk that discharge is appropriate despite a lack of appropriate safeguards for employees' privacy.

---

383 *Id.* at 1376.

384 *Id.* at 1375.

385 *Id.* at 1376.

386 *See supra* Section VII.C.3.d.

387 Downloading from pornographic sites that will sell user information may lead to spammers.

This leaves "risk of liability" as the only potentially reasonable grounds for the discharge. It is unclear what the risk of liability is, except perhaps for sexual harassment. Yet while a reasonable suspicion that an employee is utilizing a computer to forward pornography is an appropriate grounds for monitoring personal usage of the employee's computer, it hardly justifies discharge when other safeguards for protection of employees' privacy are not in place.

A standard for what constitutes reasonable suspicion should be developed. As mentioned above, one case suggests that when there is a particularized suspicion of wrongdoing, but no proof beyond the accusation of a co-worker, a limited exception for surreptitious monitoring of a limited duration is appropriate in order to verify the accusation.[388] This thesis is supported in the context of monitoring of computer usage as well.[389]

g. Discipline for Computer Use

A number of decisions suggest that the degree to which prohibited information was kept private should be considered, and the level of discipline imposed adjusted accordingly.[390] Many decisions suggest that disciplining employees because of prohibited behavior that was only private and exposed to no one else should considerably mitigate any discipline imposed.[391] Moreover, even when the material has been shared with others, if the number of recipients was few or if the recipients were

---

388 *See* Xcel Energy, 119 Lab. Arb. Rep. (BNA) 26 (2003) (Daly, Arb.).

389 *See* City of Fort Worth, Tex., 123 Lab. Arb. Rep. 1125 (2007) (Moore, Arb.) (search of e-mail conducted when one employee reported grievant was assisting another employee in theft of saw-blades); S. Cal. Edison, 117 Lab. Arb. Rep. (BNA) 1066, 1069 (2002) (Prayzich, Arb.) (implying search of grievant's e-mail was performed when co-worker complained about receiving offensive calendar).

390 *Cf.* MT Detroit, Inc., 118 Lab. Arb. Rep. (BNA) 1777 (2003) (Allen, Arb.) (when an employee sent a message with offensive racial language that she believed to be anonymous but was actually traceable back to the employer, the employee's belief that the message was anonymous did not mitigate the termination).

391 *See, e.g.*, City of Fort Worth, Tex., 123 Lab. Arb. Rep. 1125 (2007) (Moore, Arb.) (considering that employee did not disseminate e-mails as important in decision to reinstate employee with back-pay); Snohomish County Wash. Pub. County Dist. No. 1, 115 Lab. Arb. Rep. (BNA) 1, 8 (2000) (Levak, Arb.) ("penalty of discharge was far too severe" when employee sent inappropriate e-mails only to his own home e-mail address); *cf.* Xcel Energy Co., 123 Lab. Arb. Rep. (BNA) at 603 (discharge for keeping a private joke file in desk that was "never shared with other employees" is inappropriate; appropriate discipline is suspension); Wackenhut Corr. Corp., 118 Lab. Arb. Rep. (BNA) 63 (2003) (O'Connor, Arb.) (suggesting that grievant's understandable embarrassment when supervisor shared private phone message from abortion clinic with a co-worker would mitigate the imposition of discharge for insubordinately yelling at supervisor upon learning of the disclosure).

friends of the employee, this also should mitigate any imposed discipline.[392]

As discussed above, the suggested proposals adopt this safeguard, except in some situations where the employee is on notice of the particulars of monitoring.[393] Unlike a situation where an employee is told conduct is prohibited but does not have notice that the particular private area will be monitored, when an employer provides notice to an employee of the prohibited conduct and of the fact that monitoring through a specified system is ongoing, the employee knows not to engage in the conduct, even in private. Thus, the privacy interest of the employee weighs less when such a policy is in effect.

4. Off-Duty Behavior

As stated by one arbitrator, "As a general rule, once an employee is off duty and away from the workplace, there is a presumption that the employee's private life is beyond the employer's control."[394] This section first discusses the safeguard of limiting employers' ability to discipline for off-duty conduct and then describes different combinations of rules that would adequately protect employees from employer monitoring of off-duty conduct.

a. Disciplining for Off-Duty Conduct

Many arbitration decisions limit discipline for off-duty conduct. Such limitations provide a safeguard for employees' right to privacy in their personal off-duty activities. The arbitral authority regarding this

---

392 *See* Chevron Prods. Co., 116 Lab. Arb. Rep. (BNA) 271, 274, 280, 281 (emphasizing that grievant sent arguably sexually explicit and offensive e-mails to only three close friends none of whom would be offended, in reasoning termination should be reduced to suspension); *cf.* Cingular Wireless, 121 Lab. Arb. Rep. (BNA) 438, 441 (2005) (Nolan, Arb.) (The arbitrator reasoned that "[a]n employee's one-time use of an offensive term [when speaking to supervisor about a customer] hardly rises" to the level justifying termination.); JBM, Inc., 120 Lab. Arb. Rep. (BNA) 1688, 1699 (2005) (Rosen, Arb.) (termination is not appropriate where grievant swore two times in private conversations with supervisors that did not disrupt the workplace); King Soopers, Inc., 120 Lab. Arb. Rep. (BNA) 501, 506 (2004) (Sass, Arb.) (circumstances surrounding grievant's racist statement including the fact that "[t]his was an isolated comment made in the privacy of the back room by one employee to another . . ." must be considered).

393 *See supra* Section VII.C.3.e– f.

394 Dept. of Corr. Servs., 114 Lab. Arb. Rep. (BNA) 1533, 1536 (1997) (Simmelkjaer, Arb.). *See also* ELKOURI & ELKOURI, *supra* note 193, at 1111 ("It is well established that the time of an employee outside his regular hours of work and outside the overtime sometimes incidental thereto belongs to him and may be used for recreation and work, provided the employee does not engage in practices or occupations that are detrimental or clearly prejudicial to the business and interests with which his duties in the service of his regular employee are connected.") (quoting Janitorial Serv., 33 Lab. Arb. Rep. (BNA) 902, 907–08 (1959) (Whelan, Arb.)).

safeguard serves as a good starting point for devising adequate privacy protections for employees' off-duty conduct.

A review of the cases suggests that an employer must prove some significant concrete harm to the employer in order to discipline an employee for off-duty conduct, because off-duty conduct is subject to a high level of privacy.[395] Some arbitrators use the terminology that discipline for off-duty conduct requires proof of a "direct nexus" between the misconduct and the employer's "legitimate interests."[396] The decisions recognize several categories of significant concrete harm to the employer that generally justify discipline for off-duty conduct. They also recognize several categories that do not suffice to justify discipline.

i) Examples of Significant Concrete Harms

Two relatively recent cases dealing with Internet activity suggest that one concern magnified by the new technology is that of employees competing with their employers. In one case, the arbitrator upheld a termination in part based upon an employee's e-mail soliciting business from a company that the grievant's employer was also soliciting.[397] In another, the arbitrator upheld the termination of an employee who had set up an Internet website and purchased equipment to establish a directly competing business.[398] These cases are consistent with arbitral decisions that have found direct competition with one's employer to amount to a sufficient harm to justify termination.[399]

There are, however, limits as to what constitutes direct competition. As noted by one arbitrator, "[f]or competition to be substantively significant it clearly must be more than minimal. One can arguably contend that the corner delicatessen competes with the nearby supermarket; but

---

395 *See* Quaker Oats Co., 116 Lab. Arb. Rep. (BNA) 211, 215 (2001) (Marino, Arb.) ("As a general rule, arbitrators hold that an employer may not discipline an employee for off-duty activities. Nevertheless, while agreeing that the private life of an employee is beyond the reach of his employer, it must be pointed out that the effect of the conduct on an employee's job relationship may prevail over consideration of privacy.").

396 *See id.* at 213; *see also* Dept. of Corr. Servs., 114 Lab. Arb. Rep. (BNA) at 1536 (determining that the boundary between the employer's business interest and employee's privacy interests shift only where it can be shown there is a "nexus" between the off-duty behavior and the employer's interests).

397 *See* GFC Crane Consultants Inc., 122 Lab. Arb. Rep. (BNA) 801, 804 (2006) (Abrams, Arb.).

398 *See* Fox Television Station, 118 Lab. Arb. Rep. (BNA) 641, 645 (2003) (Allen, Arb.). There is an entire body of common law governing the appropriateness of non-compete clauses, which is a topic beyond the scope of this Article.

399 *See* Penn Window Co., 120 Lab. Arb. Rep. (BNA) 298, 304 (2004) (Dissen, Arb.) (indicating that employers can have a policy forbidding employees to work for a direct competitor and can terminate employees who are aware of the policy but go against it); *cf.* ATC/Vancom of Las Vegas, L.P., 119 Lab. Arb. Rep. (BNA) 836 (2003) (Block, Arb.) (upholding termination of employees who advocated that city eliminate employer and run buses itself).

one cannot logically or accurately conclude that such competition is anything more than minimal."[400]

Indeed, a stronger position could be taken. If employees are provided no rights to privacy or autonomy in the workplace, but rather treated simply as a labor commodity, then they should be free to work even for a competitor. By providing the labor, they have provided all that the employer asks. If, however, employees are treated as participants in the success of the company, humanely, and with rights of privacy, then employers might expect loyalty from them, including the loyalty not to undermine the company by working for a competitor.[401]

One decision suggests that a concrete adverse effect on the employee's performance of his duties would also suffice whereas an impact on office morale is not a significant enough harm.[402] The grievant's affair with a subordinate whom he recommended for promotion created an appearance of impropriety and unfairness in the workplace but an investigation revealed no preferential treatment.[403]

Another decision suggests that a type of significant concrete harm is when supervisors and their families "are targeted by employees' off-duty conduct because of the supervisors' on-duty, work related actions," rendering the supervisors unable to perform their jobs effectively.[404]

Another category of recognized significant concrete harm is where a role model engages in immoral and obscene conduct, drawing attention from those in the workplace and community.[405] The grievant, a school teacher, was terminated when his estranged wife posted obscene nude photos of the grievant on MySpace, as well as two other websites, in

---

400 Copley Newspapers, 107 Lab. Arb. Rep. (BNA) 310, 313 (1996) (Stallworth, Arb.).

401 This is consistent with the rationale for rules against competition as summarized by one employer. Working for a competitor "jeapordizes both the financial well being of the Employer and the Employer's own ability to secure work for its employees . . . ." Penn Window Co., 120 Lab. Arb. Rep. (BNA) at 300. The arbitrator explained that a skilled employee who worked for a new direct competitor provided the new company "the benefit of his experience" learned at the old company and thereby "assisted" the new company "in establishing a competitive local presence, to the obvious detriment of the Employer." *Id.* at 305.

402 *See* Monterey County, 117 Lab. Arb. Rep. (BNA) 897, 900 (2002) (Levy, Arb.). *But see* Quaker Oats Co., 116 Lab. Arb. Rep. (BNA) 211 (2001) (Marino, Arb.) (suggesting in dicta that an adverse impact on employee morale is a legitimate employer interest).

403 *See* Monterey County, 117 Lab. Arb. Rep. (BNA) at 898.

404 Quaker Oats Co., 116 Lab. Arb. Rep. (BNA) 211, 215 (2001) (Marino, Arb.).

405 *See* Warren City Bd. of Educ., 124 Lab. Arb. Rep. (BNA) 532 (Skulina, Arb.) (holding that a high school teacher, who did not take reasonable steps to maintain custody and control of obscene photographs of him and his wife, which she posted on websites accessible to students, was discharged for just cause); *see also* Lake Washington Sch. Dist., 120 Lab. Arb. Rep. (BNA) 1081, 1087 (2004) (Henner, Arb.) (suggesting that an employer can appropriately require a teacher with a record of complaints against him of unwarranted contact with students to seek permission from employer before having unsupervised contact with students outside of work).

conjunction with "gross" write-ups.[406] Co-workers, children, parents, the local newspaper, and the community became aware of the photos.[407] At least one child called a teacher in tears.[408]

The analysis conducted by the arbitrator was consistent with that used in off-duty conduct cases which rely on situational privacy. The arbitrator looked at the effect of the off-duty conduct on the employee's ability to perform his job.[409] The decision recognized that, at least in such circumstances, an employee has some responsibility to keep off-duty conduct private from those in the workplace.[410] The arbitrator reasoned that the grievant had been warned that his wife would likely make the photos publicly available but had not taken measures to prevent her from so doing.[411] This category should, however, be given a restrictive application because some might categorize unobjectionable behavior like two men holding hands or kissing as immoral and obscene.

The most obvious type of significant concrete harm would be a financial harm, such as paying for Family Medical Leave Act (FMLA) leave for an employee who was not actually using such leave.[412] Indeed, the potential harm of employees taking paid leave when not truly entitled to it appears to give rise to a great amount of off-duty monitoring by employers.

Another arbitrator concludes that potential damage to the company's reputation is a significant enough harm. The arbitrator suggests that the proper factors to determine whether there is a direct relation between the off-duty conduct and the grievant's work are the following:

---

406 Warren City Bd. of Educ., 124 Lab. Arb. Rep. (BNA) at 535.

407 *See id.*

408 *See id.*

409 *See id.* at 536.

410 *See id.* at 535.

411 *See id.* The issue of a third party exposing an employee's private information to the employer and others raises a host of interesting legal issues that are beyond the scope of this paper. What level of action must an employee take to ensure private information remains private? If despite taking such action, the information is disclosed to the employer, can the employer properly act on the information?

412 One arbitrator proposes that termination for off-duty conduct is appropriate when an employee violates a rule that is "reasonably" related "to the orderly, efficient, and safe operation of the employer's business" and the infraction impedes the employer's ability to "conduct its operations profitably and in a business like manner." United Ass'n of Plumbers & Steamfitters, 116 Lab. Arb. Rep. (BNA) 710, 712 (2001) (Wolfson, Arb.). The employee failed to disclose her divorce to her employer resulting in the employer erroneously paying for benefits for her prior husband. The arbitrator concluded that her justifications including "her state of mind, her desire for privacy and her emotions surrounding being divorced after thirty years of marriage in a community where she and her ex-husband are well-known" were not the type he could consider. *Id.* at 713. The standards used by the arbitrator are quite vague and do not specifically address the concrete harm at issue in the case, a financial loss to the employer, regardless of the overall profitability of the business. Additionally, the standards fail to properly factor in the employee's privacy interest.

"the extent to which the business is affected (harm to the business); whether the affect is reasonable or inevitable; whether the harm adversely affects the employee's ability to perform his or her job; or whether the conduct will lead other employees to refuse to work with the offender."[413]

The first and second factors appear to indicate, as discussed above, that there should be a significant harm to the employer. The third and fourth factors appear to be subsets of the types of potential harms. While the third is a valid consideration, the fourth should require proof that employees have actually refused to work with the employee.[414] Otherwise an employer can simply claim that employees may refuse to work, and can, perhaps, even encourage employees to state they would refuse to work.

Apparently, relying heavily on the company's reputation as an "all-American" and "wholesome" company as well as the third factor, the arbitrator concluded that because the employee was registered as a sex offender on a state website, and would be for ten years, the public, customers, and co-workers could all be expected to object to the unsupervised delivery of products by the grievant.[415] The arbitrator concluded, "[t]he type of crime is serious enough, and its unacceptability to the public significant enough to justify the Grievant's termination."[416]

Contrary to the decision, potential damage to a company's reputation should not constitute the type of significant concrete harm necessary to discipline for off-duty conduct. Reputation is a nebulous concept, and much conduct might potentially affect any organization's perception of its image. Rather, some concrete harm such as customer complaints or refusals to work with the employee should be required.

If, on the other hand, harm to reputation does suffice, it should be narrowly limited, as this arbitrator suggests, to conviction for a crime that is extremely unacceptable to the public and notice of which is more

---

413 The Coca-Cola Bottling Co. of Ohio/Ky. Dayton Sales Ctr., 121 Lab. Arb. Rep. (BNA) 1489, 1498 (2005) (Paolucci, Arb.); *cf.* Dept. of Corr. Sers., 114 Lab. Arb. Rep. (BNA) 1533, 1537 (1997) (Simmelkjaer, Arb.) (stating exceptions to the general rule are when employer proves the conduct either harms the business; has an adverse effect on the employee's ability to perform the job; or leads other employees to refuse to work); The Admiral at the Lake, 121 Lab. Arb. Rep (BNA) 19, 25 (2005) (Petersen, Arb.) (stating exceptions to the general rule are when the employee's behavior 1) harms "the employer's reputation or product;" 2) "renders the employee unable to perform his or her duties or appear at work;" or 3) "leads to a refusal, reluctance, or inability of other employees to work with" the employee).

414 *See* Dept. of Corr. Servs., 114 Lab. Arb. Rep. (BNA) at 1536 (holding statements that co-workers were embarrassed by grievant's conduct of flying a Nazi flag were not sufficient to prove they refused to work with him).

415 *See* The Coca-Cola Bottling Co. of Ohio/Ky. Dayton Sales Ctr., 121 Lab. Arb. Rep. (BNA) at 1494, 1497.

416 *Id.* at 1498.

readily available than through court documents, such as through a registered sex offender website designed for use by the public.

ii) Examples of Insufficient Harms

In addition to harm to office morale or reputation being insufficient, other types of harm are recognized as being inadequately significant, such as being late to work.[417] In one case, an arbitrator implied that even if the grievant's off-duty conduct of attending a dance bar was the true reason for her tardiness, she could not be disciplined for the tardiness or lying about it.[418]

Another type of harm that is not concrete enough is a potential ethical conflict. In one decision, newspaper sports-writers freelanced for publications of the teams on which they reported.[419] The arbitrator decided that it was not "sufficient for the employer to offer its fears or concerns that the reading public may perceive a conflict of interest."[420] Instead, the employer would need concrete evidence that the freelancing influenced the grievants' work or that the public had complained about the grievants' lack of objectivity.[421]

b. Monitoring Off-Duty Behavior[422]

Three decisions illustrate the range of arbitral concern regarding surveillance of off-duty behavior, which does not yet appear to be a critical issue for many arbitrators.[423] Generally, arbitrators rely on the safeguard of limiting discipline for off-duty conduct to the exclusion of other

---

417 *See* Shawnee County, Kan. 123 Lab. Arb. Rep. (BNA) 1659 (2007) (Daly, Arb.).

418 *See id.*

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

420 *Id.* at 1279.

421 *See id*.

422 A related issue is whether employees should be required to report personal off-duty information to employers. *See* United Ass'n of Plumbers & Steamfitters, 116 Lab. Arb. Rep. (BNA) 710, 712 (2001) (Wolfson, Arb.). This topic is beyond the scope of the Article. But requiring employees to report any outside business activity seems overly invasive. *Cf.* Fox Television Station, 118 Lab. Arb. Rep. 641, 646 (2003) (Allen, Arb.) (upholding rule requiring employees to disclose any outside business activity). Additionally, it seems feasible to require gathering of information related to off-duty conduct be held confidential, upon an employee's request to do so, by only those who need to know the information to take necessary action. Such action is analogous to the manner in which employers honor the confidentiality of job applicants who request confidentiality from their current employers. For instance, in the case of United Ass'n of Plumbers & Steamfitters, 116 Lab. Arb. Rep. (BNA) 710 (2001) (Wolfson, Arb.), limiting the release of the information to the appropriate benefits personnel might have avoided the situation where the grievant failed to report her divorce.

423 *But see* Lyondell Citgo Ref., 120 Lab. Arb. Rep. (BNA) at 364. No case reviewed other than *Lyondell* dealt with generalized monitoring, without reasonable suspicion, of employees' off-duty conduct. Cases involving generalized monitoring of off-duty activity do not arise or are settled prior to arbitration, likely because of the clear line between private off-duty conduct and on-duty conduct in the union setting.

appropriate safeguards. Some arbitrators require reasonable suspicion to monitor, while others do not. Some consider whether the conduct is "outdoors and in the open" and others consider whether the conduct is "public," generally indicating that monitoring of activity within the private home is inappropriate.

For instance, one arbitrator believes that even surreptitious off-duty surveillance of a particular employee based on a reasonable suspicion of work-related misconduct is appropriate if the surveillance takes place "outdoors and in the open."[424] While such conduct may be a violation of privacy, it is not "untoward."[425] In the case, an employee told his supervisor he would be hunting over Thanksgiving week. When he called in to use FMLA leave Thanksgiving week with the excuse that he had to care for his sick wife, the employer hired a private investigator whose surveillance films revealed the employee loading a truck and otherwise preparing to go hunting. The arbitrator relied on the film to uphold the employee's discharge.[426]

In another case the arbitrator suggests that not all activity outside of a home is public. The arbitrator concluded that the display of a Nazi flag on a porch was not public when the house was "approximately 300 feet off the main highway" and "surrounded by numerous trees."[427] The arbitrator reasoned that to take a photo of the flag, the photographer either stood on the private property or "used a long distance lens."[428] The arbitrator overturned the grievant's discharge because the grievant's conduct was not directly related to his employment.[429]

In a third case, an arbitrator's decision suggests that monitoring without reasonable suspicion is justifiable. Because an employee used 255.33 hours of FMLA leave in less than a twelve month period, the executive vice president of the employer decided to have an investigative firm conduct surveillance of the employee's activities on a day he was off on FMLA leave.[430] The arbitrator concluded that the video of the grievant performing yard work demonstrated that the grievant "had an obvious impairment" and would have been unable to work for all but the last hour and a half of his shift.[431] The vice president had previously decided to terminate the grievant based on the private investigator's re-

---

424 *See* Interstate Brands Corp., 121 Lab. Arb. Rep. (BNA) 1580, 1582 (2005) (Skulina, Arb.).

425 *Id.*

426 *See id.* at 1581.

427 Dept. of Corr. Servs., 114 Lab. Arb. Rep. (BNA) at 1541.

428 *Id.*

429 *See id.* at 1542.

430 *See* Bud Indus. Inc., 124 Lab. Arb. Rep. (BNA) 908, 909, 912 (Miles, Arb.). The video revealed the grievant working in his yard, but he was not "limber" or "fast" and appeared to be in an altered state. He "labored to pull" a rake across the lawn. *Id.* at 914.

431 *Id.*

port without reviewing the video.[432] The arbitrator overturned the termination.[433]

These arbitration decisions do not suggest a per se ban on employer surveillance of off-duty conduct. Rather, the decisions indicate that any such surveillance policy should comply with an appropriate minimal floor. Any policy which sufficiently protects employees' right to privacy should place severe restrictions on employer monitoring of off-duty conduct. Indeed, the arbitrators' reliance on the concept of the surveillance being open and outdoors suggest that surveillance of an employee indoors, especially in the home, is inappropriate. Just as the privacy of the home has been recognized as sacrosanct for Fourth Amendment privacy inquiries, it should likewise be guaranteed a high level of privacy from employers. People have an absolute right for tasks performed in the home, such as consuming medication or undergoing medical procedures, engaging in sexual activity, or keeping personal diaries, to remain private from their employers. Employers are unlikely to need to monitor an employee's activity within the home to determine whether a violation of sick leave, disability leave, or other work-related rules has occurred. The only exception might be for monitoring an employee's use of the employer's own equipment, such as a computer, in the home.[434]

Additionally, restricting monitoring of private behavior, even if outside or in the open is equally appropriate. The employer is likely able, in most cases, to discern any violation of work rules without prying into an employee's backyard or a romantic picnic in a deserted park. In those limited cases where the employer cannot, due to the isolation of the employee and his home, it is appropriate to place the burden of potential loss on the employer rather than sacrifice the privacy of the majority of working people.

Even when monitoring is of public off-duty behavior, additional safeguards beyond limitations on discipline are appropriate. An employer should have a reasonable suspicion that the employee is engaging in conduct that would cause a significant concrete harm to the employer. Without such a rule, employers can randomly monitor employees' behavior without any basis for suspecting wrongdoing.[435] For instance, an employer could monitor every employee who went on workers' compensation leave or pry into non-work related, but potentially objectionable

---

432 *See id.* at 910.

433 *See id.* at 915.

434 *See* discussion *infra* Section VII.C.4.c.

435 This is similar to random drug testing protested by unions as an invasion of privacy.

conduct, such as visits to the doctor, volunteer work at an AIDS/HIV clinic, or a close friendship with a known convict.[436]

Additional safeguards for monitoring of off-duty conduct involve many of those discussed in the previous sections. Because off-duty conduct is the most private, the package of protection afforded should include the most stringent combination of safeguards. In all instances, other available means of verifying an infraction should be used prior to monitoring. A confidential reviewer should perform the monitoring, which should be limited to only behavior relevant to the purpose of the monitoring. Only behavior that is in violation of the stated purpose of the monitoring should be disclosed to management, even if other infractions are discovered. And that information should be disclosed only to those with a need to know. Furthermore, compensation should be provided for the violation of the employee's privacy whether or not disciplinary action actually results.

In addition, an appropriate package of safeguards could include notifying employees that the employer will monitor when it has a reasonable suspicion of an infraction that would cause harm to the employer. The notice should clearly delineate the types of infractions monitored for and the potential resulting discipline, and should contain the particulars of the types of monitoring that will take place. The policy should be consistently enforced, and any discipline imposed should be mitigated by the private nature of the conduct or communication.

Alternatively, the package of safeguards might include notifying the employee that monitoring will begin after discovery of the potential infraction and before a verification process. The employee should be informed of the alleged infraction for which monitoring is taking place, the potential resulting discipline, and the particulars of the type of monitoring. The employer should consistently follow the procedure in every instance that there is a reasonable suspicion of the type of infraction, so as to avoid arbitrary off-duty monitoring.

Some may argue that employers should be able to monitor employees' conduct without reasonable suspicion when the monitoring involves time that the employee is being paid while on leave. In such a situation, the employer has a clear interest in ascertaining whether the employee is actually using the leave for the granted purpose. The cost of malingering can be high, and the employer has limited means, other than surveillance, to discover malingering.

If such an exception is made, it should be a narrow one. The monitoring should be subject to a safeguard package, such as those two illus-

---

436 *See* Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24 BERKELEY J. EMP. & LAB. L. 377, 390 (2003) (noting that employees "have been discharged for associating with known criminals or their relatives").

trated above, that provides a high level of privacy protection. The only difference would be that the employer could engage in noticed-random monitoring during normal working time. Yet, on the other hand, an employee is entitled to a certain amount of leave, provided there is medical or other proof, and should not be assumed to be malingering or dishonest unless some reason indicates otherwise. Thus, such an exception is probably unwarranted in most situations.

c. Monitoring the Employer's Property on the Employee's Property

As employees spend more time at home working with employer-issued equipment, the issue of monitoring employer property that resides on the employee's property becomes a salient one.[437] One case suggests that monitoring the property of an employer, such as an employer-owned vehicle, is appropriate when it is at an employee's home during worktime.[438] The arbitrator reasoned that first-hand observation of an employee's company vehicle parked at the employee's home carried more weight than GPS reports disclosing the same.[439]

In instances where an employer is monitoring the use of its own equipment, such as a computer or vehicle, then an exception to the rule permitting no monitoring inside or in private areas is permissible. Work equipment should be used, generally, for work, and the same concerns of misuse of equipment exist even when the equipment is on the employee's property. Thus, a package of safeguards such as that discussed for surveillance of on-duty communications should suffice to protect the employee's privacy. The employer should not, however, be permitted to use its equipment to monitor the employee's behavior unrelated to use of the equipment. For example, an employer could not have the computer tapping into an employee's conversations in her house or have a GPS monitoring where she was moving about in her home.

---

437 Another important issue with the accessibility of new communications technology is that of the employee using personal equipment at work. Two arbitration cases reviewed raise the issue of searching employees' equipment located on employer property. *See* Trane Co., 124 Lab. Arb. Rep. (BNA) at 677; U.S. Steel Corp., 121 Lab. Arb. Rep. (BNA) 1557, 1559 (2005) (Bethel, Arb.) (concluding that collective bargaining agreement precluded employer from threatening to discipline employees who refused to consent to a random search of vehicles in company parking lot). In contrast to employer equipment, which is generally used for work, personal equipment is generally used for personal reasons. Thus, safeguards like those proposed for off-duty conduct would be appropriate as to the employer's monitoring of personal equipment.

438 *See* Beverage Mktg. Inc., 120 Lab. Arb. Rep. (BNA) 1388, 1391 (2005) (Fagan, Arb.).

439 *See id.* at 1389.

D. Adequate Remedies for Violation of Protections Should Include the Safeguards Suggested by the Arbitration Decisions and Additional Sanctions

As previously discussed, adequate protections might be implemented through minimum standards or safe-harbor policies, or some other creative means. Whatever the source of the protection, there must be significant consequences for employers who proceed without the required safeguards and an adequate remedy for the employee whose privacy is violated in order for the protection to be effective. Several of the safeguards work equally well as remedies. First, whenever an employer acts in a manner that contravenes the applicable policy, the employee who is aware of the monitoring should have the right to affirmatively refuse the invasion.[440] Second, whenever the policy does not provide compensation as a safeguard, compensation for the invasion of privacy can serve as an effective remedy. Third, the concept of mitigating discipline based on the right to privacy can be extended, when not provided for in the policy, to serve as a remedy for policy violations. Finally, in all cases, removal of any discipline imposed as a result of monitoring outside the scope of the policy can serve as an effective remedy.

Additionally, administrative fines or similar penalties could be used as an appropriate remedy.[441] If use of an attorney is contemplated as part of the enforcement scheme, then payment of attorneys' fees would also be an appropriate remedy.

E. Some Level of Privacy Protection Must Be a Nonwaivable Right

When protections are provided for employees' right to privacy, whether the individual employee should be able to exchange the right of privacy from employer monitoring for additional compensation is likely to become a contentious issue. Several factors suggest that the right should be nonwaivable.[442] The right is a fundamental one to which employees are entitled regardless of their level of personal wealth. Additionally, the unequal bargaining position of employees and employers means that employees might agree to compensation in lieu of privacy when they would actually prefer the latter.

Other considerations, however, weigh in favor of permitting such an exchange. Certain employees are salaried precisely because they are expected to be available at varying hours in return for salaried compensa-

---

440 At a minimum, this remedy should be available for attempted invasions of personal computer use and off-duty activity. *See supra* Section VII.C.1.

441 French law imposes fines for failing to adequately notify employees of electronic monitoring. Rustad & Paulsson, *supra* note 30, at 892.

442 This is similar to the way in which an employee cannot waive the right to mandated breaks in exchange for more compensation.

tion. Other employees such as doctors, especially in certain specialties, may be needed urgently by their employers and patients with little notice at any time of the day.

Additionally, whether an exchange is permissible might be a result not only of the type of employee at issue but also of the type and extent of monitoring at issue. Trading compensation in return for wearing a pager on certain days seems less invasive of an employee's privacy than trading compensation for twenty-four hour remote monitoring of her personal home computer. A workable policy would set a floor of privacy rights which an employee could not trade away based on the general type and extent of monitoring; it would also differentiate between types of employees.

CONCLUSION

Almost one hundred twenty years ago, Louis D. Brandeis urged that technological change necessitated protection of the right to privacy.[443] Justice Brandeis was also astutely aware of the extensive power of corporations, including the power to "subject labor to capital" and infringe employees' "liberties and opportunities."[444] It is all too poignant then that the common law protection for which his article was the impetus has generally failed to protect employees' right to privacy.

The introduction of recent technology such as GPS, e-mail, and blogging has rendered this failure more acute. This Article proposes a solution: protection for employee privacy from technological monitoring based on the safeguards recognized by labor arbitrators. Indeed, the law of the shop is one of the few places in America that workplace privacy has been recognized. While the protection is neither as systematic nor robust as would be ideal, the safeguards suggested by the decisions can serve as a starting point for developing an adequate framework of protection. Thus, by surveying recent arbitration decisions dealing with privacy, GPS, e-mail, blogging, and the Internet, this Article fills a gap in the literature.

---

443 *See* Samuel Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

444 *See* Liggett v. Lee, 288 U.S. 517, 548 (1933) (Brandeis, J., dissenting) ("The prevalence of the corporation in America has led men of this generation . . . to accept the evils attendant upon the free and unrestricted use of the corporate mechanism as if these evils were the inescapable price of civilized life and, hence, to be borne with resignation. Throughout the greater part of our history a different view prevailed. Although the value of this instrumentality in commerce and industry was fully recognized, incorporation for business was commonly denied long after it had been freely granted for religious, educational and charitable purposes. It was denied because of fear. Fear of encroachment upon the liberties and opportunities of the individual. Fear of the subjection of labor to capital.").

But more remains to be done. Useful concepts and ideas would likely also be disclosed by other sources that reflect the law of the shop, such as court decisions and unpublished arbitration decisions. Review of collective bargaining agreements and corporate privacy policies in the union sector may provide additional insight.

Additionally, a legal scholar who cherishes the right to privacy might conduct a case study of a union workplace and its employees. Such a study might provide insight on the details of effective implementation of privacy safeguards. It would also, doubtless, provide insight on the human need for privacy—even in the workplace.