Summer 2006

Bargaining for Privacy in the Unionized Workplace

Ann C. Hodges
University of Richmond, ahodges@richmond.edu

ANN C. HODGES*

Bargaining for Privacy in the Unionized Workplace

Abstract: This article considers whether collective bargaining can enhance privacy protection for employees in the United States. Employers are increasingly engaging in practices that invade employee privacy with few existing legal protections to limit their actions. While data on the extent of bargaining about privacy is limited, it appears that unions in the U.S. have primarily used the grievance and arbitration procedure to challenge invasions of privacy that lead to discipline of the employee instead of negotiating explicit contractual privacy rights. In contrast to the U.S., labor representatives in many other countries, particularly in the European Union, have greater legal rights of consultation with employers and take a more proactive approach to protection of employee privacy. While this approach offers promise for achieving greater privacy for employees and more flexibility for employers, the article concludes that it is unlikely to be widely adopted in the U.S. because of the limited power of labor unions.

1. INTRODUCTION

With the events of September 11, 2001, the focus of the nation shifted to national security and prevention of additional attack. The swiftly enacted USA Patriot Act[1] provided the government with sweeping powers of

* Professor of Law, University of Richmond. I wish to thank my colleagues Daniel T. Murphy and Porcher L. Taylor, III, both of the University of Richmond, and Maurizio Del Conte, Professore Associato, Bocconi University for their comments on earlier drafts and Luke P. Wright, for his helpful research assistance.

1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-156.

The International Journal of Comparative Labour Law and Industrial Relations, Volume 22/2, 147-182, 2006.

investigation and surveillance in order to provide protection from terrorism. Although passed by overwhelming majorities in both houses of Congress, the Patriot Act quickly generated criticism from civil libertarians and privacy advocates. The confluence of the Patriot Act with the advancements in technology that render monitoring of citizens and employees infinitely easier and cheaper makes the focus on workplace privacy particularly timely.

While we purport to place a high value on privacy in the United States, actual protection of privacy is quite limited. Few can afford to live without employment, yet our right to privacy in the workplace is more circumscribed than in most other spheres of public life. Legitimate employer interests justify some intrusions on employee privacy. Yet many scholars have suggested that greater protection of employee privacy is warranted and is likely to come only by additional legislation.[2]

In many other countries, stronger legislative protection for employee privacy exists. In addition, worker representatives in other countries often bargain for privacy protection for workers. While many of the most salient privacy issues are mandatory subjects of bargaining, U.S. unions do not appear to have placed significant priority on many privacy issues in bargaining. Negotiated privacy protections offer some advantages over legislation. Yet given the shrinking percentage of employees covered by collective bargaining agreements, such protection may not reach many workers.

This paper considers collective bargaining as a possible avenue for increased privacy protection for workers. Section 2 reviews briefly current employer practices that raise privacy concerns, along with existing legal protection for privacy in the workplace. Section 3 looks at the most significant current issues regarding employee privacy and concludes that most are mandatory subjects of bargaining under the National Labor Relations Act, at least as they apply to employees rather than applicants for employment, and probably under many state collective bargaining laws as well. Section 4 looks at the context in which privacy issues have arisen in the unionized workplace, as well as the information that exists on the extent

2 See, e.g., M. W. Finkin, 'Second Thoughts on a Restatement of Employment Law', *U. Pa. J. Lab. & Emp. L.*, Vol. 7, 2005, p. 279, pp. 280-281; S. E. Wilborn, 'Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace', *Ga. L. Rev.*, Vol. 32, 1998, p. 825, pp. 879-880. *Cf.* W. R. Corbett, 'The Need for a Revitalized Common Law of the Workplace', *Brook. L. Rev.*, Vol. 69, 2003, p. 91 (arguing for revitalization of common law rather than legislation to address issues of electronic monitoring and genetic discrimination). But see C. Pearson-Fazekas, '1984 Is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law', *Duke L. & Tech. Rev.*, No. 15, 2004 (arguing that existing law is sufficient, employee privacy rights in the workplace are limited, and there is little incentive for employer abuse).

to which privacy protections have been incorporated in collective bargaining agreements. Section 5 looks at the international data on privacy and collective bargaining. Section 6 concludes that collective bargaining would be an effective way to provide additional privacy protection for employees, but since so few employees are covered by collective bargaining agreements, this solution is of limited utility in the U.S. today.

2. Existing Practice and Existing Law

The agenda for the conference illustrates the foremost privacy issues in today's workplace – electronic monitoring, privacy of medical and other employee records, medical, genetic and drug testing, and other restrictions on off-duty conduct. In recent years much of the focus has been on electronic monitoring, as technology has enabled employers to engage in constant supervision of employees at work, as well as to access employees' electronic communications. Among the most current issues are the employer's use of employee-tracking technology to monitor employees and employer restrictions on employee blogs.[3] While there is no dispute that employers have the right to monitor employees to ensure that they are engaging in productive work and not violating workplace rules, the ability to conduct constant monitoring with electronic technology has altered the nature of supervision.[4] As the technology enabling such monitoring has decreased in cost, monitoring has increased and, according to critics, raised employee stress levels.[5] Technology has also increased the ability of employers to engage in genetic testing and discrimination, bringing this issue to the forefront of the concerns of privacy advocates.[6]

---

3 See 'Technology Issues Outpace Guidance From NLRB, Attorneys Tell ABA Conference', *Daily Lab. Rep. (BNA)*, No. 46, March 10, 2005; 'Employee Tracking Technology Raises Privacy Concerns and Potential Employee Backlash', *Daily Lab. Rep. (BNA)*, No. 80, April 27, 2004; T. Zeller, Jr., 'When the Blogger Blogs, Can the Employer Intervene', *N.Y. Times*, April 18, 2005, at C1; J. Boog, 'Employers Wrestle with "Blogosphere"', *Nat'l L.J.*, April 4, 2005, p. 5.

4 For example, employers are using tracking systems on company vehicles to monitor employee location, driving speed, and time of stops. See 'Employee Tracking Technology Raises Privacy Concerns and Potential Employee Backlash', *Daily Lab. Rep. (BNA)*, No. 80, April 27, 2004. Identification badges are used directly on employees to determine how long employees spend on particular tasks and in certain locations. See *id.* Cell phones and handheld computers can also be used to track employees. See *id.* Employers are even using infrared technology on bathroom sinks and soap dispensers to see how long employees spend washing their hands. See *id.*

5 W. R. Corbett, *op. cit.*, *supra* note 2, pp. 102-103.

6 *Id.*, pp. 104-105.

2.1. Current Practice

Employers investigate and monitor employees for several legitimate reasons. Employers seek to hire and retain those workers who will be most productive. They want to be sure that employees are working effectively and efficiently.[7] Employers want healthy employees who are less likely to be absent or impose high health insurance costs. In addition, employers are concerned about potential liability for injury to employees or injury to third parties.[8] Further, employers desire to prevent loss of confidential information and breaches of computer security.[9] Finally, where some problem occurs, missing inventory for example, employers investigate to determine the cause of the loss. All of these matters have the potential to affect the employer's profitability, thus spurring substantial employer concern. Despite the legitimacy of employer motives,[10] however, employer practices intrude on employee privacy interests. Employees have an interest in protecting and controlling the use of personal information about them.[11] Additionally, employees have a privacy interest in engaging in some kinds of behavior free from regulation or surveillance.[12] These privacy interests clash with legitimate employer interests in ensuring productivity, preventing liability, and protecting the company from loss, necessitating some reconciliation by law or agreement.

According to an American Management Association study in 2001, 82.2 per cent of major U.S. employers are 'actively recording and/or reviewing employee communication and behavior in the workplace' using

---

7 It has been estimated that 'cyber-loafing', employees surfing the internet at work, costs businesses $54 billion per year. 'Workers, Surf at Your Own Risk', *Bus. Wk.*, June 12, 2000, p. 105.

8 Some companies have settled sexual harassment suits based on e-mails at the cost of several million dollars, while others have fired employees who sent sexually offensive e-mails, presumably to avoid such claims. See 'Workers, Surf at Your Own Risk', *op. cit.*, *supra* note 7, p. 105.

9 Indeed, employer concerns about privacy of employee, customer or citizen data may prompt monitoring or restrictions on the use of certain technologies. See *TLK2UL8R: The Privacy Implications of Instant and Text Messaging Technologies in State Government,* Research Brief, National Association of State Chief Information Officers, 2005, pp. 6-7, available at <http://www.nascio.org/nascioCommittees/privacy/instantMessagingBrief.pdf> (last visited September 29, 2005).

10 Certainly, there are improper motives for employer monitoring as well, including curiosity, voyeurism, and a desire to interfere with employee efforts to unionize. See D. R. Nolan, 'Privacy and Profitability in the Technological Workplace', *J. Lab. Res.*, Vol. 24, 2003, pp. 207, 215-216.

11 R. L. Belair, *Employee Rights to Privacy,* Proceedings of New York University Thirty-Third Annual National Conference on Labor, 1981, pp. 3-4.

12 *Id.*

electronic monitoring.[13] Monitoring increased dramatically in the short time between 1997 and 2001. For example, '[i]n 2001, 36.1 per cent of firms reporting monitored computer files, compared to 13.7 per cent in 1997; 46.5 per cent monitored e-mail in 2001, compared to 14.9 per cent in 1997.'[14] The 2005 AMA survey on electronic monitoring and surveillance shows that monitoring has continued to increase since 2001.[15] Seventy-six per cent of employers surveyed monitor employees' web site connections, while 36 per cent track 'content, keystrokes and time spent at the keyboard.'[16] Fifty per cent of employers kept and reviewed employees' computer files and 55 per cent stored and reviewed employees' e-mail.[17] Twenty-five per cent of employers had terminated an employee for violating e-mail policy.[18] Over 80 per cent of employers notified the employees of monitoring and retention of files.[19]

Monitoring of telephone conversations and video surveillance also increased dramatically. The percentage of employers monitoring employee phone usage and tracking the phone numbers called increased from 9 per cent in 2001 to 51 per cent in 2005.[20] In 2001 only 9 per cent of employers surveyed taped employee phone calls, while 19 per cent taped calls of at least some employees in 2005 and 3 per cent taped calls of all employees.[21] The percentage of employers using video monitoring to detect theft, violence and sabotage jumped from 33 per cent in 2001 to 51 per cent in 2005.[22] Monitoring for performance also has increased, with 10 per cent of employers videotaping some employees and 6 per cent taping all employees.[23] As for existing policies, the following per-

13 R. Bigler and W. Petzel, 'Employer Snooping: What Rights Do Workers Really Have?', Feb. 13, 2002, available at <http://www.lraonline.org/print.php?id=98>, citing the *American Management Association Study.*

14 M. W. Finkin, 'Information Technology and Workers' Privacy: The United States Law', *Comp. Lab. L. & Pol'y J.*, Vol. 23, 2002, pp. 471-474.

15 American Management Association, *2005 Electronic Monitoring and Surveillance Survey*, 2005, available at <http://www.amanet.org/research/pdfs/EMS_summary05.pdf > (last visited September 29, 2005) (hereinafter 'AMA, *2005 Survey*').

16 *Id.* The survey consisted of 526 employers of various sizes. *Id.*

17 *Id.* In a 2004 survey of 840 employers, 60 per cent monitored external e-mail using software. See American Management Association, *2004 Workplace E-Mail and Instant Messaging Survey Summary,* available at http://www.amanet.org/research/pdfs/IM_2004_Summary.pdf> (last visited May 6, 2005) (hereinafter 'AMA, *2004 Survey*').

18 *Id.* The same percentage reported terminations for e-mail use and terminations for internet abuse in the 2005 survey. AMA, *2005 Survey.*

19 AMA, *2005 Survey.*

20 *Id.*

21 *Id.*

22 *Id.*

23 *Id.*

centages of employers reported maintaining the specified policies: personal e-mail use – 84 per cent; personal internet use – 81 per cent; personal instant messenger use – 42 per cent; operation of personal web sites on company time – 34 per cent; personal postings on corporate blogs – 23 per cent; and operating personal blogs on work time – 20 per cent.[24]

Employers have been slower to adopt monitoring in newly emerging areas of technology.[25] As of 2004, only 11.1 per cent of responding employers used software to manage instant messaging.[26] As for global positioning technology, 5 per cent of responding employers in 2005 used it to monitor cell phones, 8 per cent to keep track of company vehicles, and 8 per cent to monitor employee id cards.[27] Fifty-three percent of employers used such technology 'to control physical security and access to buildings and data centers.'[28] Fingerprint scans were used by 5 per cent of employers, facial recognition technology by 2 per cent of employers and iris scans by 0.5 per cent of employers.[29]

A 2004 survey by the Society for Human Resource Management revealed that employers most often monitor computer use and internet use.[30] On the other hand, the employers rarely engaged in desk searches, opened postal mail, or listened to employee phone conversations.[31] About one quarter of employers frequently used electronic identification cards to monitor employee movement, while fewer used cameras to do so on a frequent basis.[32] A Government Accounting Office study of 14 large employers found that all routinely store information on employees' computer activity.[33] Eight of the companies used the files to investigate

---

24 *Id.*

25 *Id.*

26 AMA, *2004 Survey.* A number of respondents, 28.4 per cent, however, were unsure if their employer used software to monitor instant messaging. *Id.*

27 AMA, *2005 Survey.*

28 *Id.* These access cards can be used to monitor employee location in the building also, which raises privacy concerns. See E. Balkovich, T. K. Bikson, and G. Bitko, *9 to 5;* 'Do You Know if Your Boss Knows Where You Are?', 2, *Rand Corp.*, 2005, pp. 16, available at <http://www.rand.org/pubs/technical_reports/2005/RAND_TR197.pdf> (last visited September 29, 2005)(hereinafter 'Rand Study').

29 AMA, *2005 Survey.*

30 SHRM Research, *Workplace Privacy*, p. 21, January 2005, available at <http://www.shrm.org/surveys/Workplace%20Privacy%20Poll%20Findings%20-%20A%20Study%20by%20SHRM%20and%20CareerJournal.com.pdf>. Large organizations engaged in more monitoring than smaller ones. *Id.*, p. 22.

31 *Id.*, p. 21.

32 *Id.*, pp. 19-20.

33 U.S. General Accounting Office, Employee Privacy: Computer-Use Monitoring Practices and Policies of Selected Companies, GAO-02-717, September 27, 2002, available at <http://www.gao.gov/new.items/d02717.pdf> (Last visited May 6, 2005) (hereinafter 'GAO Report').

reports of employee violations of company policies, while six regularly reviewed employee computer activity to determine whether any violations had occurred.[34] A Rand Study of six employers using radio-frequency identification cards for employee access in the workplace demonstrated that cards were used not only for access but also for the collection and retention of personally identifiable data regarding employee movement.[35] Five of the six organizations used such data to investigate incidents such as theft or other alleged misconduct or to determine compliance with work rules.[36] In three organizations, the data was available not only to security departments but also to other departments such as human resources, legal and line management.[37] None of the organizations had a policy regarding the use of the system which was provided to all employees, thus limiting employee knowledge.[38] The authors concluded that privacy was of low priority to the organizations, subordinate to security, investigation, emergency procedures and employment policies.[39]

An AMA study on medical testing in 2004 revealed that 63 per cent of the responding companies required medical testing of new hires, employees, or both.[40] Most of the testing was for illegal substances or fitness for duty, with about 15.1 per cent of companies testing for susceptibility to workplace hazards.[41] Drug testing and fitness-for-duty testing have decreased since 1995 and 1997 respectively, while testing for HIV peaked in 1997 and has decreased since.[42] A small percentage of employers appear to engage in genetic testing, with breast/colon cancer, sickle-cell anemia, and Huntington's Disease listed as reasons for testing.[43]

2.2. Legal Restrictions

Legal restrictions on employers whose investigative and monitoring tactics infringe on employee privacy are limited. The Employee Polygraph

34 *Id.*, p. 3.
35 Rand Study, *op. cit.*, *supra* note 28, p. 12.
36 *Id.*
37 *Id.*
38 *Id.*, pp. 14, 15, 16.
39 *Id.*, p. 16.
40 American Management Association, *AMA 2004 Workplace Testing Survey: Medical Testing*, available at <http://www.amanet.org/research/pdfs/Medical_testing_04.pdf> (last visited September 29, 2005).
41 *Id.*
42 *Id.*
43 *Id.*

Protection Act restricts the use of polygraph exams,[44] and many states also have polygraph laws[45] with the more protective state laws superseding the federal.[46] The Americans with Disabilities Act ('ADA') limits the ability of covered employers to require medical exams.[47] For employees, exams must be job-related.[48] For applicants, exams can be required only after a conditional job offer has been made, and any disqualification based on the exam must be job-related.[49] In addition, medical records must be kept confidential and separate from other personnel records.[50] Drug tests, however, are excluded from these ADA restrictions.[51] Some states have passed laws regulating drug testing in various ways, but none prohibit testing.[52] Also, in recent years, a number of states have enacted legislation either preventing employers from requiring genetic testing, or limiting the use of the results of such tests.[53] President Clinton issued Executive Order 13145 which limits disclosure of genetic information and prohibits discrimination based on genetic information in federal employment.[54] In addition, the EEOC interprets the ADA to prohibit

---

44 See 29 U.S.C. §§ 2001-2009. The Polygraph Act contains exemptions for government employers and some private employers involved in the security, national defense and pharmaceutical industries, however. See 29 U.S.C. §2006.

45 For a listing of state laws, see M. W. Finkin, *Privacy in Employment Law,* (2d ed.), 2003, pp. 490-540. For discussion of state law restrictions on polygraphs, see H. D. Kelly, Jr. & W. A. Herbert, *When James Bond Enters the Workplace: Uses and Abuses of Technology – A Guide for In-House Counsel and Litigators,* 2004, pp. 31-32, available at <http://www.bna.com/bnabooks/ababna/annual/2004/kelly.doc>, (last visited June 8, 2005).

46 See 29 U.S.C. § 2009 (providing that the law does not preempt more restrictive state laws or collective bargaining agreements.)

47 42 U.S.C. § 12112(d).

48 42 U.S.C. § 12112(d)(4)(A).

49 42 U.S.C. § 12112(d)(2),(3).

50 42 U.S.C. § 12112(d)(3)(B). HIPAA regulations also deal with the privacy of medical records but apply to employers only when they act in the capacity of plan sponsors under ERISA. See M. Finkin, *supra* note 45, at pp. 44-45.

51 42 U.S.C. § 12114(d). Indeed various federal agencies require drug testing of employees in certain industries. See, e.g., Omnibus Transportation Employee Testing Act, 49 U.S.C. §§ 45101-45106 (requiring drug testing of employees in the transportation industry.) Also, the Drug Free Workplace Act requires federal grantees to maintain drug free workplaces. 41 U.S.C. § 701 et seq.

52 M. A. Rothstein and L. Liebman, *Employment Law,* (5th ed.), 2003, p. 241. For a comprehensive listing of such laws, see M. Finkin, *op. cit., supra,* note 45, pp. 542-690.

53 M. Finkin, *op. cit., supra* note 45, pp. 22, 791-822; W. R. Corbett, *op. cit., supra,* note 2, p. 113; W. A. Herbert, *The NLRA in a Technological Society: A Law Not Busy Being Born, Is Busy Dying,* 2005, pp. 13-17 (copy on file with the author).

54 Exec. Order No. 13145, 65 Fed. Reg. 6877 (Feb. 8, 2000).

genetic discrimination.[55] Finally some states protect employee personnel files from disclosure and/or provide employee access to the information contained there.[56]

In addition to specific legislation, most states have either a common law or statutory cause of action for invasion of privacy. The reasonable expectation of privacy has been imported from the constitutional context into both common law and statutory privacy contexts.[57] Thus, if employees do not have a reasonable expectation of privacy, any invasion of privacy is lawful. The incentive then is for employers to defeat the expectation of privacy by either employment rule or requiring employee consent to searches as a condition of employment.[58] It is rare that employees are able to challenge employer infringements on privacy successfully using the common law.[59]

Regarding technological monitoring, as Professor Finkin states in his article detailing the U.S. law on workplace privacy and information technology, '[d]espite the wealth of legal thought, the state of the law in the United States relevant to the topic addressed here has been put in one short sentence: "No successful standards, legal or otherwise, exist in the United States for limiting the collection and utilization of personal data in cyberspace."'[60] In addition to the common law, two federal statutes, the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act, limit data collection and interception of communications, but exceptions permit most employer monitoring of employees

---

55 W. R. Corbett, *op. cit., supra* note 2, p. 113. It is not clear, however, that courts will defer to the EEOC's interpretation of the statute. *Id.* The EEOC brought a claim against the Burlington Northern Santa Fe Railway Company challenging genetic testing based on the ADA and reached a settlement with the company providing $2.2 million to the tested workers. 'EEOC's First Genetic Testing Challenge Settled for $2.2 Million, Parties Announce', *Daily Lab. Rep. (BNA),* No. 90, at A-1 (May 9, 2002).

56 M. Finkin, *op. cit., supra,* note 45, pp. 717-756.

57 D. R. Nolan, *op. cit., supra* note 10, p. 220.

58 *Id.*, p. 221.

59 M. Finkin, *op. cit., supra,* note 45, at xxviii. Egregious cases may be the exception to this rule. For example, the Georgia Court of Appeals recently allowed a state law invasion of privacy claim to proceed to trial where the employer allegedly utilized video surveillance in the women's restroom for over two years in response to a rumor that drug dealing was occurring in the restroom. *Johnson* v. *Allen*, 2005 Ga. App. Lexis 311. For further discussion of cases in which employees have been successful in common law invasion of privacy cases, see H. D. Kelly and W. A. Herbert, *op. cit., supra* note 45, pp. 6-8, 17-18.

60 M. Finkin, *op. cit., supra* note 14, p. 471, quoting P. Schwartz, *Privacy, Participation, and Cyberspace: An American Perspective*, in *Zur Autonomie des Individuums: Liber Amicorum Spiros Simitis,* D. Simon and M. Weiss (eds.), 2000, pp. 337-338.

who use the employer's communication systems.[61] A few state laws require that notice of monitoring be given to the employees.[62] Additionally, the National Labor Relations Act prohibits employer surveillance of union or protected concerted activity.[63]

There is also a group of state statutes that protect employees' rights to engage in certain lawful activities while off-duty. Most of the laws protect employees' right to use tobacco products, but some extend to alcohol, some to use of any lawful product, and a few to other lawful activities.[64] Some of these laws have exceptions allowing employers to limit employee rights for job related reasons.[65] In the absence of these statutory restrictions, employers may lawfully refuse to hire or terminate employees for off-duty conduct, so long as they do not violate any other legal limitation such as discrimination laws or constitutional rights.[66]

---

61 D. R. Nolan, *op. cit., supra,* note 10, pp. 224-25. One of the exceptions is consent. *Id.* An employer could require employees to consent to any and all monitoring, thus bringing its actions within the statutory exception while at same time defeating any expectation of privacy at common law.

62 See D. R. Nolan, *op. cit., supra* note 10, p. 225; M. Finkin, *supra* note 14, pp. 477-478; M. Finkin, *op. cit., supra* note 45, pp. 757-762. Some states also have laws similar to ECPA, but they generally contain the same exceptions. D. R. Nolan, *op. cit., supra* note 10, p. 225.

63 *The Developing Labor Law,* (4th ed.), P. Hardin and J. E. Higgins, Jr., (eds.), 2001, p. 162.

64 See M. Finkin, *op. cit., supra* note 45, pp. 113-114, 691-716. For a discussion of these laws as they relate to romantic relationships, see S. Stiller, 'Statutes Limiting Regulation of Workplace Romances', *Arbitration 1998: The Changing World of Dispute Resolution, Proceedings of the Fifty-First Annual Meeting, National Academy of Arbitrators,* p. 22, 1999. Notably, an office romance recently led to the termination of Boeing's CEO, although the use of the company's computers to send romantic e-mails and the company's image concerns suggest that the situation might not fall into the category of off-duty conduct with no impact on employment. See 'The End of the Office Affair? Face Value', *The Economist*, March 12, 2005, p. 64.

65 See M. Finkin, *op. cit., supra,* note 45, pp. 113-114.

66 Discrimination laws protect employees from discrimination on the basis of religion, unless the employee's belief or practice cannot be reasonably accommodated, pregnancy, and in some states, political affiliation and marital status. See M. Finkin, *op. cit., supra* note 45, pp. 367-380, 391-393, 397-398. In the public sector, there also may be constitutional restrictions on termination or discrimination based on, *inter alia,* political affiliation, religious belief, and protected speech. See, e.g., *Barrow* v. *Greenville Indep. Sch. Dist.*, 332 F.3d 844 (5th Cir. 2003) (recognizing constitutionally protected privacy right to direct education of children including enrolling them in private school); 'Jury Awards $35,455 to Teacher Denied Job Because Her Children Attend Private School', *Gov't Empl. Rel. Rep. (BNA),* Vol. 43, p. 2105, at p. 413 (April 26, 2005) (reporting on favorable jury verdict for Barrow); *Hudson* v. *Craven*, 403 F.3d 691 (9th Cir. 2005) (finding that college did not violate speech and associational rights of teacher by refusing to renew her contract because of her attendance at a WTO protest rally with some of her students).

This would include employee blogging and participation in computer chat rooms.[67]

Public-sector employees have more protection than private-sector employees by virtue of the Constitution, which establishes the right of privacy as fundamental.[68] Based on the right of privacy, public employees may limit employer inquiries into their private lives.[69] Also, the Fourth Amendment has been applied to drug testing and other workplace searches.[70] Workplace searches are subjected to a different test than those conducted for law enforcement purposes, however.[71] First, the employee must have a reasonable expectation of privacy and then a balancing test is applied to determine whether legitimate employer interests outweigh the employee's privacy interests.[72] Under this standard, governmental drug testing has been upheld in a number of employment contexts, but

---

67 M. Finkin, *op. cit., supra* note 14, pp. 486-488.

68 See *Griswold* v. *Connecticut*, 381 U.S. 479, 486 (1965). Enforcement of constitutional privacy rights may not be easy, however. See, e.g., *Giaccio* v. *City of New York*, 16 Am. Disabilities Cas. (BNA) 653 (2005) (dismissing city employee's constitutional privacy claim based on release of drug and alcohol test results to the media because plaintiff did not allege that the action occurred as a result of a policy or practice of the municipality as required for an action under Section 1983). See also *City of Sherman* v. *Henry*, 928 S.W.2d 464 (Tex. 1996), *cert. denied,* 519 U.S. 1156 (1997) (finding that refusal to promote employee based on his affair with the wife of a fellow officer does not violate privacy rights under the U.S. or Texas constitutions).

69 Wilborn, *supra* note 2, at 866 & n.155. The Privacy Act also provides some protection to federal employees. See *United States Dep't of Defense* v. *Fed'l Lab. Rel. Auth.*, 510 U.S. 487 (1994) (holding that Privacy Act bars disclosure of employees' home addresses to requesting unions). Claims of violation of the Privacy Act have been brought in arbitration under collective bargaining agreements. See, e.g., National Ass'n of Gov't Employees, Local R4-27 and U.S., Dep't of Defense, 60 FLRA No. 5 (2004)(upholding arbitrator's decision that Privacy Act was not violated by agency that contacted employee's medical provider to discuss recommended work schedule). As in *U.S. Dep't of Defense* v. *FLRA*, *supra,* the Privacy Act may be used to prevent unions from obtaining information for purposes of collective bargaining. See U.S. Dep't of the Air Force, 51 FLRA 599 (1996) (holding that Privacy Act barred disclosure of employee performance ratings and awards by name to union). But See *Department of the Air Force* v. *Fed'l Lab. Rel. Auth.*, 104 F.3d 1396 (D.C. Cir. 1997) (finding supervisor's privacy interest did not outweigh the union's need for copy of letter disciplining supervisor to determine whether to proceed with grievance).

70 See *O'Connor* v. *Ortega*, 480 U.S. 709 (1987); *National Treasury Employees Union* v. *Von Raab*, 489 U.S. 656 (1989). Psychological testing is not considered a search under the Fourth Amendment, however. See *Greenawalt* v. *Indiana Dep't of Corrections*, 397 F.3d 587 (7th Cir. 2005).

71 The Court in *Von Raab* noted that 'requiring a warrant in this context would serve only to divert valuable agency resources from the Service's primary mission.' 489 U.S. at 666-667.

72 See *NTEU* v. *Von Raab*, 489 U.S. at 665-666.

limited in others.[73] The result typically depends on the jobs of the employees being tested and the nature of the testing. Like drug testing cases, cases applying the Fourth Amendment to electronic monitoring and computer file searches have mixed results, some finding violations of privacy rights and others allowing monitoring or searches.[74]

2.3 Proposed Legislation

Despite agitation over the lack of workplace privacy, enactment of any comprehensive legislation seems remote. Privacy advocates have lobbied for legislation at the state and federal levels with limited success.[75] The two exceptions have been in the area of genetic information and tobacco use, the former probably attributable to deep public concern over the use of genetic information and the latter to the strength of the tobacco lobby. As Professor Finkin has noted, privacy legislation in the U.S. tends to be limited and enacted in direct response to particular perceived problems.[76] Outside those contexts, employees in the private sector nonunion workplace have limited protection for privacy interests, while employees in the public sector have greater but still limited protection. But what of the unionized workplace? Are conditions there any different?

---

73 See, e.g., International Union, United Auto., Aerospace, and Agric. Implement Workers of Am. v. Fink, 385 F.3d 1003 (6th Cir. 2004) (rejecting Fourth Amendment challenge to random drug testing of employees carrying firearms, health care workers caring for individuals in state care, corrections employees with unsupervised access to prisoners, probationers or parolees, and employees with unsupervised access to controlled substances), *cert. denied,* 125 S. Ct. 1972 (2005). Notably, this challenge was brought by the union to the testing program incorporated in its collective bargaining agreement with the state. 385 F.3d at 1006.

74 *Compare Varnado* v. *Department of Employment and Training*, 687 So. 2d 1013, 1024-1030 (La. Ct. App. 1996)(finding search of employee's files on state-owned computer violated employee's reasonable expectation of privacy) and *State* v. *Bonnell*, 856 P.2d 1265, 1273 n.5 (Haw. 1993) (finding violation of Hawaii constitutional provision comparable to the Fourth Amendment based on video surveillance of the employees' break room) *with Vega-Rodriguez* v. *Puerto Rico Telephone Co.*, 110 F.3d 174 (1st Cir. 1997) (allowing video surveillance of workplace); *Sacramento County Deputy Sheriffs' Ass'n* v. *Sacramento County*, 59 Cal. Rptr. 2d 834 (Ct. App. 1996) (same) and *Biby* v *Board of Regents, University of Nebraska*, 419 F.3d 845 (8th Cir. 2005) (finding employee had no reasonable expectation of privacy in his computer files where employer's computer policy informed employees that university could search files for legitimate reasons).

75 See D. R. Nolan, *supra* note 10, p. 227 (discussing proposed federal legislation). Most recently, legislation has been introduced to protect employee privacy in changing areas. See *Employee Changing Room Privacy Act,* H.R. 582, introduced by Rep. Tom Petri (R-Wis.) and Rep. Rob Andrews (D-N.J.).

76 M. Finkin, *supra* note 14, pp. 472-473.

3. Privacy as a Mandatory Bargaining Subject

Under the National Labor Relations Act, employers are required to bargain only over mandatory subjects of bargaining.[77] The NLRB has held that both medical exams and drug testing of employees are mandatory subjects of bargaining.[78] The same is true of the installation of video surveillance cameras.[79] In finding video surveillance to be a mandatory subject of bargaining, the Board stated:

> [T]he installation of surveillance cameras is both germane to the working environment, and outside the scope of managerial decisions lying at the core of entrepreneurial control.
>
> As to the first factor – germane to the working environment – the installation of surveillance cameras is analogous to physical examinations, drug/alcohol testing requirements, and polygraph testing, all of which the Board has found to be mandatory subjects of bargaining. They are all investigatory tools or methods used by an employer to ascertain whether any of its employees has engaged in misconduct.
>
> The Respondent implemented the installation and use of surveillance cameras because of an increase in workplace theft and other suspected employee misconduct in the facility, such as reports of employees sleeping instead of working. The Respondent acknowledges that employees caught involved in theft and/or other misconduct are subject to discipline, including discharge. Accordingly, the installation and use of surveillance cameras has the potential to affect the continued employment of employees whose actions are being monitored.

---

77 *NLRB* v. *Wooster Div., Borg-Warner Corp.*, 356 U.S. 342 (1958).

78 See Lockheed Shipbuilding Co., 273 NLRB 171, 177 (1984)(medical exams); Johnson-Bateman Co., 295 NLRB 180 (1989) (drug testing).

79 See Colgate-Palmolive Co., 323 NLRB 515 (1997). *Accord, National Steel Corp.* v. *NLRB*, 324 F.3d 928 (7th Cir. 2003)(ordering employer to provide union with information regarding hidden security cameras and negotiate about confidentiality protections); Anheuser-Busch, Inc., 342 NLRB No. 49 (2004), *enf'd sub. nom, Brewers and Maltsters Local 6* v. *NLRB*, 414 F.3d 36 (D.C. Cir. 2005)(finding employer violated NLRA by failing to bargain with union prior to installation of hidden surveillance cameras in area used for work and breaks, and by refusing to supply information to the union about the use and installation of the cameras).

> Further, as the judge finds, the use of surveillance cameras in the restroom and fitness center raises privacy concerns which add to the potential effect upon employees. We agree that these areas are part of the work environment and that the use of hidden cameras in these areas raises privacy concerns which impinged upon the employees' working conditions. The use of cameras in these or similar circumstances is unquestionably germane to the working environment...
>
> The installation and use of surveillance cameras in the workplace are not among that class of managerial decisions that lie at the core of entrepreneurial control. The use of surveillance cameras is not entrepreneurial in character, is not fundamental to the basic direction of the enterprise, and impinges directly upon employment security. It is a change in the Respondent's methods used to reduce workplace theft or detect other suspected employee misconduct with serious implications for its employees' job security, which in no way touches on the discretionary 'core of entrepreneurial control.' (footnotes omitted).[80]

Although the Board has not ruled on whether other forms of electronic monitoring are mandatory bargaining subjects, it seems likely that the rationale of *Colgate-Palmolive* would apply, leading the Board to find that bargaining is required. Similarly, since genetic testing is a form of medical testing, it is probable that the Board would conclude that bargaining over such testing is required. It also seems likely that most restrictions on off-duty conduct such as smoking, alcohol, and fraternization would be conditions of employment subject to bargaining. Unions are generally only entitled to demand bargaining over these issues as they impact current employees, however. In *Star Tribune*, the Board concluded that hiring practices are not negotiable unless they vitally affect the terms and conditions of employment of the employees.[81]

Another factor which may affect the bargaining obligation is whether the employer's implementation of a new system implicating privacy rights is in fact a change in working conditions. If not, bargaining will not be required. The Board has addressed this issue in several cases. In *Rust Craft Broadcasting*,[82] the Board concluded that the change from manual timekeeping to mechanical timekeeping was not an unlawful unilateral

80 *Colgate-Palmolive,* 323 NLRB at 515-516.
81 295 NLRB 543 (1989).
82 225 NLRB 327 (1976).

change because it was merely a different method of recording time. A change from a time clock to supervisory recording of employees' work time required bargaining, however.[83] Because of the involvement of supervisors in direct monitoring and the employees' inability to check the accuracy of the records, the new system was a significant change.[84] In 2001, an administrative law judge found that a change from signing in and out to a biometric system using fingerprints was more like the former than the latter, and no bargaining was required.[85] In reaching that conclusion, the judge distinguished the case from *Vincent*, finding that no more supervisory oversight was involved and there was no evidence that employees could not check the accuracy of their records.[86] Further the judge noted that there was no evidence that the fingerprints recorded by the system could be used in criminal or workplace investigations, other than those involving time of arrival and departure.[87]

Similarly, the General Counsel refused to issue a complaint in a case where the employer replaced a two-way radio system in employee vehicles with a computer unit containing a Global Positioning System (GPS).[88] The *Roadway Express* case is a troubling application of the unilateral change doctrine. A GPS is far more intrusive than a two-way radio as it allows the company to track each move of the truck as it happens. The company can determine the truck's route, the length of time a trip takes and how long a break the driver takes. The General Counsel found the systems to be the same because both use a mechanical method of obtaining the same information.[89] According to the General Counsel, the only difference was whether the employer or the employee initiated the use of the system for reporting.[90] In fact, however, it is a change from time-specified radio reports to at least potential constant employer monitoring. Thus the correct analogy is a change from supervisory monitoring of work, which is not constant, but initiated on occasion by the employer, to constant monitoring by video surveillance, which the Board has found negotiable. One could also analogize it to the change from supervisory investigation of theft to use of hidden security cameras to detect theft, also negotiable.[91] Since the Board has found employee pri-

83 Vincent Industrial Plastics, 328 NLRB 300 (1999).
84 *Id.* at 300, n. 1.
85 Res-Care, Inc., 2001 NLRB Lexis 397.
86 *Id.* at *23.
87 *Id.* at *23-*24.
88 Roadway Express, Inc., Case No. 13-CA-39940-1 (2002).
89 *Id.*
90 *Id.*
91 See Colgate-Palmolive Co., 323 NLRB at 519.

vacy to be a condition of employment, the greater impact of GPS systems on privacy should lead to the conclusion that this unilateral change required bargaining.[92]

Scope of bargaining issues in the public sector are less straightforward, as federal law applies to federal employees and multiple state laws govern bargaining at the state and local level. Furthermore, to the extent that other statutory and constitutional provisions exist which deal with these subjects, those laws will impact bargaining. While this is also true in the private sector, in the public sector statutory restrictions on bargaining subjects are more common. In the federal sector, the Federal Labor Relations Authority held that certain union proposals relating to drug testing were not negotiable because they interfered with the employer's rights under statutes and executive orders.[93] Other proposals of the union were negotiable, however, as they impinged on no management rights.[94]

While many of the privacy-related issues are likely to be conditions of employment and thus commonly within the description of bargainable subjects under most public sector statutes, other laws and managerial rights may limit bargaining. For example, the Minnesota Court of Appeals recently considered whether Sherburne County Minnesota must adopt bargaining over a new drug testing policy.[95] The court first noted that the state statute governing drug testing permits collective bargaining over testing policies so long as the negotiated policies meet or exceed the statutory requirements and do not conflict with the employee protection standards in the statute.[96] The court then concluded that the drug testing policy was a subject in which matters of inherent managerial policy, exempt from bargaining, overlapped with mandatorily negotiable terms and conditions of employment.[97]

> In cases where there is such an overlap, a two-step process is required: first, the court must determine whether the policy has an impact on 'terms and conditions of employment,' and second, if it does, the court must ascertain whether the policy's establishment is separate and distinct from its implementation.

---

92 For further critical analysis of the decision in *Roadway Express*, see Herbert, *supra* note 53, at 10-11.

93 See F. Elkouri and E. A. Elkouri, 'Resolving Drug Issues', (1993) pp. 141-142, *citing* 'Department of the Army, U.S. Army Armament, Munitions and Chem. Command', 30 FLRA, No. 115, 1988.

94 *Id.*, p. 142.

95 *Law Enf't Lab. Serv.* v. *Sherburne Co.*, 695 N.W.2d 630 (Minn. App. 2005).

96 *Id.*, p. 634.

97 *Id.*, p. 634-636.

> If the establishment and the implementation are not separate and distinct, implementation is not subject to mandatory bargaining....But if establishment and implementation are separate and distinct, implementation is subject to bargaining.(citations omitted).[98]

The court determined that the establishment of the policy was an inherent managerial right that did not require bargaining and that no bargaining was required over the employee classifications subject to testing.[99] Nevertheless, there were other areas of implementation that were separable from the establishment of the program and thus, subject to negotiations.[100]

A similar decision was reached in a California case involving a request to bargain over the impact of the installation of a new security monitoring system.[101] After a homicide at the facility, the employer adopted a new system to keep track of employees and visitors.[102] The new system required employees upon entry and exit to use a personal ID number, typing it on a keypad or swiping an ID card, and also to touch a fingerprint scanner. The administrative law judge rejected the employer's argument that the "system was a non-negotiable upgrade of the existing system."[103] The judge noted, based on precedent, that bargaining over the decision to install the equipment was not required. The judge concluded, however, that the employer was required to bargain over the impact of the decision on the employees including, but not limited to, the privacy effects of storage of the fingerprints of employees and union representatives, the possibility of discipline as a result of use of the system, and the impact of delays at entry points on compensable employee hours.[104] The decision became final because no exceptions were filed, but is not precedential.[105] The analysis in these two decisions exemplifies the way many public-sector agencies are likely to treat employer policies and practices that implicate privacy, requiring, at a minimum, bargaining over the impact on terms and conditions of employment unless clearly excluded from bargaining by the legislature. In some states, bargaining over the

98 *Id.*, p. 635.
99 *Id.*, p. 636.
100 *Id.*, pp. 636-637.
101 See *California St. Employees Ass'n* v. *California Youth Authority*, 23 PERC (LRP) P30114 (1999), *aff'd without exceptions*, 23 PERC (LRP) P30149 (1999).
102 All facts are taken from the opinion of the administrative law judge.
103 *Id.*
104 *Id.*
105 23 PERC (LRP) P 30149 (1999).

decision may not be required because it is considered inherently managerial.[106] Drug testing as a bargaining subject has been addressed by more states than other privacy-related issues. Grodin, Malin and Weisberger report that state and local jurisdictions vary on whether drug testing of employees is a mandatory subject of bargaining.[107]

Because of constitutional limitations on employers in the public sector, another question arises for unions there. Can the union bargain away the employees' constitutional rights? Existing cases have mixed results, some holding such a waiver is permissible[108] and others finding to the contrary.[109] In *Jackson v. Liquid Carbonic Corp.*, the court suggested that the union's agreement to drug testing in the collective bargaining agreement affected the employees' expectations of privacy.[110] Under this rationale, the union may limit the employees constitutional rights without a direct waiver. Also, in the federal sector, the Civil Service Reform Act may limit employees to the contractual grievance procedure for constitutional and statutory privacy claims.[111]

---

106 See, e.g., City of Syracuse, 14 NYPERB P4645 (1981) (finding management had right to install video surveillance cameras without negotiating with the union). See also Roswell Park Cancer Institute, 34 NYPER (LRP) P4582 (2001), *aff'd*, 34 NYPER (LRP) P3040 (2001) (finding no duty to bargain where security cameras are used for monitoring broader group than just employees and there is no indication that employees are threatened with discipline or must participate in surveillance).

107 J. R. Grodin *et al.*, *Public Sector Employment: Cases and Materials*, 2004, p. 229. The authors note, however, widespread agreement that testing of applicants is not a mandatory bargaining subject. *Id.*

108 See *Bolden* v *SEPTA*, 953 F.2d 807, 826-29 (3d Cir. 1991) (indicating that union may consent to drug testing that implicates employees' Fourth Amendment rights so long as union does not breach its duty of fair representation) and cases cited therein; *Geffre* v. *Metro. Council*, 174 F. Supp. 2d 962 (D. Minn. 2001) (same).

109 See *Anonymous Fireman* v. *Willoughby*, 779 F. Supp. 402, 415 (N.D. Ohio 1991) (allowing HIV testing but finding union cannot waive employee's constitutional right through collective bargaining).

110 863 F.2d 111, 119 (1st Cir. 1988).

111 See *Whitman* v. *Dep't of Transp.*, 382 F.3d 938 (9th Cir. 2004) (holding that court had no subject matter jurisdiction over the plaintiff's claims that the FAA violated his constitutional right of privacy and his statutory right to nondiscriminatory drug testing because the FAA personnel system incorporated the civil service requirement that the collective bargaining agreement's grievance procedure would be the exclusive remedy for matters within its coverage unless the matter was excluded by the contract or fell within a statutory exception), *cert. granted*, 2005 U.S. Lexis 5032 (June 27, 2005). The Federal Circuit and the Eleventh Circuit have both held that the collective bargaining agreement is exclusive only as to administrative and not judicial claims, leading to the circuit split that prompted the grant of certiorari in *Whitman*. See *Asociacion de Empleados del Area Canalera* v. *Panama Canal Comm'n*, 329 F.3d 1235 (11th Cir. 2003); *Mudge* v. *United States*, 308 F.3d 1220 (Fed. Cir. 2002).

4. BARGAINING OVER PRIVACY

It appears that both public and private sector unions have the right to demand bargaining over many issues impacting employee privacy. But are they? Evidence is somewhat limited.

4.1. Privacy Provisions in Collective Bargaining Agreements

A 1992 Bureau of Labor Statistics Survey investigated privacy provisions in 614 collective bargaining agreements, covering 1000 or more workers each.[112] Of the 614 contracts, 380 contained some reference to privacy.[113] While this suggests significant focus on privacy in collective bargaining, a closer look at the classifications used reveals that the study employed a very broad definition of privacy provisions. A review of the survey data suggests that many areas of privacy were addressed in a limited way, or not at all, in the agreements studied. To be classified as containing a privacy provision, the contract had to have one or more of the following: 1. a requirement of notice that information was being placed in the employee's personnel file; 2. a restriction on the use of employee records; 3. a right to access and comment on employee personnel records; 4. a provision for confidentiality of employee records or files; or 5. one or more particular limitations on substance abuse testing.[114]

The notice and access requirements have limited impacts on the employee privacy concerns considered here. Further, the most common provisions were those protecting the use of employee records, primarily disciplinary records.[115] Most of those contract clauses dealt with warnings and notices of discipline placed in employee files.[116] The second most common privacy provision related to substance abuse plans and employee assistance programs, more directly relevant to current employee privacy concerns.[117]

---

112 U.S. Department of Labor, Bureau of Labor Statistics, 'Privacy Provisions in Major Collective Bargaining Agreements, 1992', *Bulletin,* No. 2448, 1994. There are several obvious limitations on this data. It is 13 years old, it encompasses only the private sector, and includes only large collective bargaining units. *Id.*

113 *Id.*, p. 3.

114 *Id.* at 3. The study also classified as privacy provisions restrictions on discrimination based on sexual orientation and marital status, and prohibitions on sexual harassment. *Id.*, pp. 44-45.

115 *Id.*, p. 4.

116 *Id.*, p. 5.

117 *Id.* One hundred and four contracts safeguarded privacy in substance abuse programs. *Id.*, p. 28.

Ninety contracts contained clauses relating to confidentiality of employment records, many relating to access to information in connection with investigation and processing of employee grievances.[118] Eighty-one dealt specifically with medical records.[119] Some provisions required only employee access to records, however, while others limited the employer's ability to engage in medical testing.[120]

Seventy-eight contracts limited employer surveillance, but only 17 of those contained provisions dealing with electronic monitoring.[121] Fourteen of the 17 dealt with telephone monitoring.[122] The report suggests that the limited focus on electronic monitoring might be a result of union emphasis on protective legislation rather than bargaining or the relative lack of surveillance at the time.[123] Professor Finkin suggests another explanation: monitoring is more likely to affect white-collar employees, managers and supervisors, who are less frequently unionized.[124] No more recent comprehensive data was located,[125] but monitoring has cer-

---

118 *Id.*, pp. 18-20. Others required employers to reprimand employees in private. *Id.*, p. 20. These provisions raise another privacy issue that arises in the unionized workplace. Employees (and employers) may be concerned about disclosure of private employee information to the union. While the National Labor Relations Act requires the employer to provide to the union information relevant and necessary to bargaining and contract administration, some confidential information need not be disclosed without authorization from the employee. See, e.g., *Detroit Edison* v. *NLRB*, 440 U.S. 301 (1979)(limiting disclosures of employee test scores); Johns-Manville Sales Corporation, 252 NLRB 368 (1980)(finding no violation where employer refused to supply names of employees partially disabled by pneumoconiosis without employee authorization). But see *Dep't of the Air Force* v. *Fed'l Lab. Rel. Auth.*, 104 F.3d 1396 (D.C. Cir. 1997)(relying on NLRA authority to order employer to give union supervisor's disciplinary letter where union showed it needed the letter to determine whether to file a grievance and also finding that the release of the material to the union under these circumstances was consistent with the Privacy Act). See also *supra* note 69.

119 *Id.*, p. 21.

120 *Id.*, pp. 25-26.

121 *Id.*, p. 38. The largest group of these dealt with polygraph testing. *Id.* Fifteen agreements limited searches of lockers and/or personal belongings. *Id.* at 42.

122 *Id.*

123 M. Finkin, *op. cit.*, *supra* note 14, at 502-503.

124 *Id.*

125 A BNA survey of 122 unionized employers in 2003 revealed that 66 per cent had a drug and alcohol policy in their collective bargaining agreement; 55 per cent had a sexual harassment policy; 30 per cent had a smoking policy; 29 per cent had an internet/e-mail policy; and 12 per cent had an AIDS/HIV policy. See J. Joseph *et al.*, *Employer Bargaining Objectives 2004*, *BNA*, 2004, p. 55 available at <http://ecommercecenter.bna.com/press/protected/2004ebo.pdf > (last visited July 7, 2005). The survey does not indicate, however, whether these policies contained any privacy provisions. Fifteen percent of employers planned to try to strengthen their drug and alcohol policies in upcoming negotiations while 17 per cent wanted to increase smoking restrictions and 6 per cent desired to strengthen their internet policy. *Id.*, p. 59.

tainly increased substantially since 1992.[126] Moreover, some of the more recent monitoring techniques, such as GPS location monitoring, are more likely to affect blue-collar or unionized employees, such as truckdrivers and other delivery people.[127] The increasing number of NLRB cases dealing with computer issues suggests also that these issues are becoming more relevant to workers who are, or are seeking to become, unionized.[128] Finally, many public-sector employees covered by union contracts utilize computers in their work.

An unscientific review of some union web sites found limited discussion of privacy issues other than drug testing. A 1997 memo on the website of the American Federation of State, County and Municipal Employees (AFSCME) discussed e-mail at work and recommended negotiation of an e-mail policy "to make sure that the workplace doesn't turn into an "electronic sweatshop.'"[129] The article identified several collective bargaining agreements and memoranda of understanding addressing e-mail. Several addressed solely union use of e-mail, authorizing it with reasonable limitations.[130] One provision, in a Newspaper Guild and Pioneer Press contract, stated: "'To ensure Productivity and good morale, the Pioneer Press affirms that users of electronic mail and voice mail systems shall have a zone of privacy ...'"[131] The AFSCME article described the provision as allowing the employer to view e-mail or voicemail of employees based on reasonable cause, such as a lawsuit, suspicion of a crime, or the need to perform work in the employee's absence, if there were no other way to obtain the information.[132] Further, certain procedur-

126 See *supra* notes 13-43 and accompanying text.

127 See *Technology Issues Outpace Guidance from NLRB, Attorneys Tell ABA Conference, supra* note 3 (union attorney indicates that GPS monitoring is a troubling issue for unions).

128 See *id.*; M. H. Malin and H. H. Perritt, Jr., 'The National Labor Relations Act in Cyberspace: Union Organizing in Electronic Workplaces', *U. Kan. L. Rev.*, Vol. 49, 2000 p. 1; S. S. Robfogel, 'Electronic Communication and the NLRA: Union Access and Employer Rights', *Lab. Law.*, Vol. 16, 2000, p. 231; G. A. Wilcox, 'Section 7 Rights of Employees and Union Access to Employees: Cyber Organizing', *Lab. Law.*, Vol. 16, 2000, p. 253; Guard Publishing Co., 2002 NLRB Lexis 70 (2002)(finding that employer violated NLRA by discriminatory rule prohibiting use of e-mail for union purposes and by insisting on contract proposal that would codify discriminatory rule); Computer Associates, Int'l, Advice Memorandum, 1-CA-38933 (2001) (authorizing issuance of a complaint against employer's maintenance of rule prohibiting all non-business use of e-mail, internet and intra-net).

129 AFSCME, *E-mail at Work*, available at <http://www.afscme.org/wrkplace/cbr397_2.htm> (visited April 19, 2005).

130 *Id.*

131 *Id.*

132 *Id.*

al steps, including notification of the employee were required before review.[133] In addition, the provision noted that any enforcement of the policy that resulted in discipline would be subject to the contractual just cause standard.[134]

The National Education Association Office of Higher Education also has addressed the issue of e-mail privacy, recommending negotiation of a policy to protect employees.[135] At the time of the article, however, no NEA higher education contracts dealing with e-mail privacy were found, although several addressed use of e-mail by the union.[136] The Communications Workers of America's web site indicates that the union has negotiated limitations on electronic monitoring.[137] The Newspaper Guild's Model Contract suggests a provision regarding electronic monitoring which states:

> There shall be no secret surveillance of employees nor shall electronic supervisors, tape recordings, telephone monitoring systems, monitoring of employees' electronic files or voice mail, or similar procedures or devices be used.[138]

No indication of the number of contracts containing such provisions exists. The Model Contract also recommends a clause on outside activities, which states: 'Outside Activity. Employees shall be free to engage in any activities outside of working hours.'[139] Again, however, there is no indication of the number of contracts containing such provisions. The National Association of Government Employees' agreement with the Federal Aviation Administration explicitly bars discipline for off-duty conduct unless it 'hampers his/her effectiveness as an employee or affects the public's confidence in the Agency.'[140] The contract also pro-

133 *Id.*

134 *Id.*

135 'E-mail and Privacy', *NEA Update,* Vol. 2, No. 6, October 1996, available at http://www.2.nea.org/he/heupdate/v2n06.pdf (last visited September 29, 2005).

136 *Id.*

137 Communications Workers of America, *Verizon East Bargaining Briefing Paper,* <http://www.cwa-union.org/verity_search_results.cfm> (visited April 29, 2005).

138 The Newspaper Guild, U.S. Model Contract, Article XXIV- General Provisions, available at <http://www.newsguild.org/barg/display.php?storyID=148> (visited April 29, 2005).

139 *Id.*

140 National Agreement Between the Nat'l Ass'n of Gov't Employees, SEIU/AFL-CIO and the Fed'l Aviation Administration, Dep't of Transportation, Article 5, Section 6, February 25, 2004, available at <http://www.faa.gov/ahr/policy/agree/agrees/term/nage/nage1.cfm> (last visited September 29, 2005). This provision is similar to the test applied by arbitrators under a just cause requirement. See *infra* notes 171-72 and accompanying text.

tects the confidentiality of medical information of employees with AIDS or HIV.[141]

Additional anecdotal evidence indicates that some unions and employers are negotiating provisions relating to electronic monitoring. An article regarding GPS-equipped cell phones used by employers to track employees indicates that 500 employees of the city of Chicago carry such phones to 'increase their productivity.'[142] The article indicates that the unions representing the employees obtained several limitations on the use of these devices, including permitting the employees to shut down the tracking features during lunch breaks and after work hours.[143] The Teamsters and UPS, and the City of Orlando and its police union, reportedly have negotiated about employer use of GPS technology.[144] Some federal sector unions reportedly have negotiated policies relating to personal use of phones and computers, along with agreements on video surveillance.[145] The California State Employees Association has negotiated with the state about electronic entry and exit monitoring systems in correctional facilities, one using fingerprints.[146]

Drug testing has been a focus for unions for a longer period of time than electronic monitoring. There are numerous NLRB cases[147] and arbitration decisions[148] relating to drug testing. In particular, unions in the construction industry have addressed drug testing, perhaps because many

141 *Id.* at Article 41, Section 3. The contract also extensively addresses substance abuse, including privacy issues. *Id.* at Articles 36, 37 and 38.

142 B. Chamy, *Big Boss is Watching,* CNET News.com, available at <http://news.com.com/Big+boss+is_watching/2100-1036_3-5379953.html?part=rss&tag=5> (last visited May 2, 2005).

143 *Id.*

144 See 'Employee Tracking Technology Raises Privacy Concerns and Potential Employee Backlash', *Daily Lab. Rep. (BNA),* No. 80, April 27, 2004. Another report indicates that after negotiations the City of Orlando rejected the use of tracking devices, while the Teamsters and UPS agreed to prohibit monitoring on employees' personal time. See 'Employer Use of GPS Units in Work Vehicles, Cell Phones, Stirs Employee Privacy Concerns', *Gov't Empl. Rel. Rep. (BNA),* Vol. 42, 2071 (August 17, 2004). The Teamsters have also barred use of GPS technology to study efficiency or set time standards. *Id.*

145 See 'As Employee Monitoring Expands, Attention Turns to Information, Policies', *Lab. Rel. Wk. (BNA),* Vol. 19, No. 11 (March 17, 2005) (reporting on comments by union attorney David Kelly).

146 See *California State Employees Ass'n* v. *California Youth Authority*, 23 PERC (LRP) P30114 (1999).

147 *Developing Labor Law*, *op. cit.*, *supra* note 63, at pp. 1214-1215 and nn. 311-318.

148 See F. Elkouri and E. A. Elkouri, *How Arbitration Works,* (6th ed.), Alan Miles Ruben, Ed. in Chief, 2003, pp. 947-48, 1005-1012; C. L. Redel and A. Abbey, 'The Arbitration of Drug Use and Testing in the Workplace', *Arb. J.*, Vol. 48, No. 1, March 1993, p. 80.

employees work on government contracted projects covered by the Drug Free Workplace Act. In addition, as noted by Sheet Metal Workers Local 36,

> The facts about drug and alcohol use are sobering to those of us in the construction industry. Someone under the influence faces twice the risk of on-the-job injury as a clear headed worker; construction workers are more likely to abuse drugs and alcohol than any other employee group; and the industry has a higher on-the-job injury rate.[149]

Many construction union apprenticeship programs prominently require drug testing for applicants.[150] Some unions have negotiated or adopted detailed drug testing programs.[151] The IBEW instituted drug testing for all of its officers and management personnel in 2005 after negotiating an agreement with the National Electrical Contractors' Association requiring local unions to 'institute minimum standards providing for drug-free pools of construction workers nationwide, through voluntary screening

149 See *Labor Management Partnership, Sheet Metal Air Conditioning Contractors Association and Sheet Metal Workers Local 36,* available at <http://www.sheetmetal36.org/LABOR%20AND%20MANAGEMENT%20PARTNERSHIP.htm > (Last visited May 2, 2005). In 1999, the union approved a new drug testing program requiring initial testing of all members and continued random and cause testing. *Id.* Apprenticeship applicants are also tested. *Id.*

150 See, e.g., *West Virginia Construction Craft Laborers' Apprenticeship Program*, available at <http://www.wvccl.org/apprenticeship.htm> (last visited May 2, 2005); *Bridge, Structural and Reinforcing Iron Workers, Local No. 1*, available at <http://www.iwlocal1.com/local_1_information.htm> (last visited May 2, 2005). See also Apprenticeship Programs with the Union Building Trades, available at <http://www.thehighschoolgraduate.com/editorial/AC/ACtrades.htm> (last visited May 2, 2005) (informing readers of apprenticeship opportunities with 15 different building trades unions which require applicants to be drug free because '[n]umber one, it's the law. Secondly, worksites can be dangerous enough without impairment due to drug abuse. Lastly, property owners and contractors along with the Union Building Trades maintain a zero tolerance for drug abuse among the workforce.')

151 See, e.g., *Management and Unions Serving Together Drug Testing Policy,* available at <http://www.must.org/formsanddocs/mustdrugtesting_081204.pdf> (last visited May 2, 2005) (detailing drug testing policy of an organization composed of unions and construction contractors in southeastern Michigan and specifying confidentiality provisions); *MMC Chosen to Administer Substance Abuse Program, Promote Safety at Ohio Construction Sites*, (January 2003) available at http://www.estetacommunications.com/NewsReleases/Cleveland.htm > (last visited May 2, 2005) (describing substance abuse program implemented by the Union Construction Industry Partnership (UCIP), a joint labor-management cooperative, to advance construction safety and implement a drug-free workplace).

of journeymen and apprentices.'[152] The union indicated an intent to negotiate about drug testing with its own unionized employees in the upcoming contract negotiations.[153] Project Labor Agreements negotiated for large construction projects may contain drug testing requirements also.[154]

4.2. Privacy in Arbitration

Virtually all collective bargaining agreements contain a grievance and arbitration procedure to resolve disputes arising under the agreement. Arbitrators have confronted privacy issues even where there is no contract provision directly addressing the subject. Most commonly, the issues arise where employees are disciplined or discharged and their challenge to the employer's action alleges a violation of privacy rights. In some cases, unions argue that arbitrators should suppress evidence obtained through searches that would violate the Fourth Amendment, even in the private sector where it does not directly apply.[155] In addition, some arbitrations involve unilaterally-issued employer rules that impact employee privacy, challenged by unions as unreasonable under the collective bargaining agreement.[156] Like the courts, arbitrators tend to apply a balancing test in cases involving privacy, considering the business need for the employer's action and the protections for employee privacy rights.[157] Another salient factor in these cases is whether the employer significantly changed working conditions.[158] In public-sector arbitrations implicating privacy, arbitrators use the balancing test utilized in constitutional cases.[159]

---

152 'IBEW Implements Drug Testing For Officers, Reps, Management Staff' *IBEW Journal*, January/February 2005 available at <http://www.ibew.org/stories/05journal/0501/p19.htm >(last visited May 2, 2005).

153 *Id.*

154 See San Diego County Water Authority Project Labor Agreement, available at <http://www.sdcwa.org/infra/esp-PLA.phtml >(last visited May 2, 2005) (requiring substance abuse testing).

155 See, e.g., Aldens, Inc., *Lab.Arb. (BNA),* Vol. 58, McGury, 1972, p. 1213 (excluding evidence); Commodity Warehousing Corp., *Lab. Arb. (BNA),* Vol. 60, Doppelt, 1973, p. 1260 (admitting evidence).

156 The agreement may expressly authorize issuance of reasonable rules but even where it does not, arbitrators will usually require that rules be reasonable.

157 Elkouri and Elkouri, *supra* note 148, p. 1153.

158 *Id.*

159 See *id.*, p. 1155.

A brief review of arbitral treatment of some particular privacy-related issues will illustrate the role of privacy in arbitration. One group of cases involves employer efforts to obtain information that employees deem private. In these cases, most arbitrators will require employees to turn over information where the employer shows a legitimate need and the request is neither vague nor overbroad.[160] In the public sector, arbitrators may look for a compelling need and a narrowly tailored request for information.[161] Arbitrators do not always reach the same conclusions in these cases, however, even on similar facts.[162]

Like cases involving employee information, cases challenging employer surveillance go both ways depending on the facts. Where the employer shows a particular need, the surveillance is likely to be upheld so long as it is not overly intrusive.[163] Typically, however, the cases do not involve specific contractual provisions relating to either privacy or surveillance, but rather challenges to the reasonableness of employer practices or to discipline resulting from surveillance. Employer searches of employee belongings and/or lockers have been the subject of a number of arbitrations. The touchstones of such decisions are notice to employees and reasonableness of the search.[164] In these cases, arbitrators may find an increased expectation of privacy if the employer requires or allows employees to use their own locks.[165]

Arbitrators frequently deal with issues relating to drug and alcohol testing.[166] Where tests are not properly conducted, discipline is commonly set aside.[167] When an employer unilaterally adopts random drug testing, arbitrators will typically apply a reasonableness analysis to determine whether random testing is justified and whether to uphold discipline based on such tests.[168] If the job is safety-sensitive and there is evidence of a serious drug problem, random testing is more likely to be

160 See *id.*, pp. 1153-1155.
161 See *id.*, p. 1155.
162 See *id.*, pp. 1156-1157 (discussing cases reaching different results on whether employers can require employees to wear name tags where union challenged the requirement on privacy grounds).
163 See *id.*, pp. 1157-1159.
164 See *id.*, pp. 1161-1164.
165 *Id.*, p. 1162. One arbitrator even upheld a search of an employee's residence authorized by his ex-wife who had control over it at the time. *Id.*, p. 1164.
166 For a thorough review of issues relating to drugs and alcohol in the workplace, see F. Elkouri and E. A. Elkouri, *Resolving Drug Issues*, 1993.
167 Elkouri and Elkouri, *supra* note 148, p. 1006.
168 *Id.*, pp. 1007-1008. Results of the cases differ, however, even on similar facts. See F. Elkouri and E. A. Elkouri, *op. cit. supra* note 166, pp. 233-235.

upheld.[169] Arbitrators have also required employees to provide information to their employers about prescription drugs they are taking based on the employer's interest in ensuring workplace safety and ensuring that drug test results are accurate.[170]

Off-duty conduct is also frequently the subject of arbitration, usually under provisions requiring just cause for discipline. The standard treatment is to limit discipline to situations where the employer can demonstrate that the conduct impacts the employer's business.[171] Such a rule limits the control that the employer retains over the employee's private life. In some jobs, notably in the education sector, arbitrators have engaged in heightened scrutiny of the employees' private lives because of the nature of the job, finding termination warranted more frequently.[172]

This review of arbitral authority indicates that even where unions have not negotiated privacy provisions in collective bargaining agreements, they will utilize privacy arguments in challenging discipline under just cause provisions or in challenging employer-implemented rules. Privacy arguments are accepted by arbitrators where employers cannot show a substantial need to invade employee privacy. Thus, while it appears that specific privacy provisions have not been extensively incorporated in collective bargaining agreements, unions have utilized privacy arguments to challenge employer rules and employee discipline that impacts on privacy rights.

5. The International Approach

The International Labour Office (ILO) recommends the involvement of workers' representatives in matters relating to employee privacy, including collection of personal data and electronic monitoring.[173] The Council of Europe makes a similar recommendation for its members, but there is

169 F. Elkouri and E. A. Elkouri, *op. cit.*, *supra* note 148, pp. 1008-1010.

170 See F. Elkouri and E. A. Elkouri, *op. cit.*, *supra* note 166, pp. 75-79.

171 F. Elkouri and E. A. Elkouri, *supra* note 148, pp. 938-939. See, e.g., 'Champion Int'l', *Lab. Arb. (BNA)*, Vol. 96, Statham, 1991, p. 325, (reinstating employee who pled guilty to off-duty drug dealing because there was no nexus to employment despite substance abuse policy and rule authorizing discipline for criminal conviction that reflects unfavorably on company or employee involved).

172 F. Elkouri and E. A. Elkouri, *op. cit.*, *supra* note 148, pp. 1311-1314. The test does not differ but because education employees are viewed as role models for students, their off-duty conduct is more frequently deemed to have affected the job.

173 J. T. Aranda, 'Information Technology and Workers' Privacy: The Role of Worker Representatives', *Comp. Lab. L. & Pol'y J.*, Vol. 23, 2002, pp. 533-535.

no binding treaty provision so requiring.[174] In several European Union member states, however, the law requires involvement of worker representatives where employers undertake certain actions that impact employee privacy. Germany, Italy, Spain, and France all require either notice or consultation or both when the employer installs or changes systems for worker surveillance,[175] as do Sweden, the Netherlands and Luxembourg.[176] France, Germany and Italy have particularly stringent requirements for consultation. If the works council in France is not consulted about monitoring, it is a criminal offense.[177] If notice to the employee and consultation of the works council have not occurred, any information gathered is invalid and cannot be used as proof of any wrongdoing by the employee.[178] German law prohibits collection of data regarding employee phone calls and e-mails unless the employee or the

174 *Id.* The European Commission is planning to issue a directive on protection of workers' personal data in 2005, after having consulted with the social partners, employer and union federations, on the issue in 2001 and 2002. See *Commission Issues Five-Year Social Agenda* (February 2005), available at <http://www.eiro.eurofound.ie/2005/02/feature/eu0502205f.html > (last visited September 30, 2005); A. Broughton, *Commission Issues Second Stage Consultation on Data Protection*, available at <http://www.eiro.eurofound.ie/2002/11/feature/eu0211206f.html>, (last visited September 30, 2005). This directive would supplement existing general directives on the processing of personal data which apply to the workplace but do not specifically address workplace issues. See C. Delbar, M. Mormont and M. Schots, *New Technology and Respect for Privacy at the Workplace,* (2003, available at <http://www.eiro.eurofound.ie/2003/07/study/tn0307101s.html>, (last visited September 30, 2005). The suggested framework proposed by the EC at the second stage consultation included a provision that worker representatives be consulted before installation, modification or evaluation of any system of employee surveillance. See *id.*

175 See J. T. Aranda, *supra* note 173, pp. 536-537; A. L. Goldman, 'Overview and U.S. Perspective', *Comp. Lab. L. & Pol'y J.,* Vol. 24, 2002, p. 1. Finnish law also requires employers to inform employees of electronic monitoring and discuss the monitoring with those employees, while substantially restricting such monitoring by law. A. Suviranta, 'The Impact of Electronics on Labor Law in Finland', *Comp. Lab. L. & Pol'y J.*, Vol. 24, 2002, pp. 93-107.

176 C. Delbar *et al.*, *op. cit.*, *supra* note 174. In the Netherlands, the Works Council has a veto power on any changes in personal data collection or employee monitoring. *Id.* Luxembourg requires co-determination by a joint committee regarding any technical equipment used to monitor employees. *Id.* In Sweden, negotiation is required on any changes in matters involving personal integrity, such as medical tests, and those involving information and communication technology. *Id.*

177 J.-E. Ray and J. Rojot, 'A Comparative Study of the Impact of Electronic Technology on Workplace Disputes', *Comp. Lab. L. & Pol'y J.*, Vol. 24, 2002, pp. 117-134.

178 *Id.* The collective agreement cannot waive the statutory protections. *Id.*, pp. 133-134.

union consents.[179] No collective bargaining agreement can supersede the law unless it 'observes statutory provisions and especially the obligation of both social partners to protect and promote the free development of the personality of the employees.'[180] In Germany, the employer also must pay for expert advice for the union if it is necessary to understand any new system.[181] The German law provides the union and the employer with significant authority over the privacy protection available to employees.[182] In Italy, an agreement with the local union must precede installation of video surveillance for security or productivity purposes.[183] If a union is set up after the installation, the union must agree to retaining the system.[184] Failure to comply subjects the employer to a criminal sanction.[185]

In the United Kingdom, the legislation does not require consultation but the Employment Practices Data Protection Code issued by the Information Commissioner recommends consultation with trade unions over any practice that involves employees' personal data.[186] While Belgium has no specific legal requirement of consultation with worker representatives on privacy issues created by new technologies, existing general law and practice would require information and consultation.[187] These laws and regulations provide opportunities for worker representatives to influence the employer's adoption and application of technology that impacts worker privacy.[188]

---

179 A. Hoeland, 'A Comparative Study of the Impact of Electronic Technology on Workplace Dispute: National Report on Germany', *Comp. Lab. L. & Pol'y J.*, Vol. 24, 2002, pp. 147, 165-166.

180 *Id.*, p. 166.

181 J. T. Aranda, *op. cit., supra* note 173, p. 536.

182 *Id.*

183 P. Balboni, 'Video Surveillance and Related Privacy and Data Protection Issues: The Italian Experience', to be published in *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy,* S. Nouwt, B. R. de Vries and C. Prins (eds.), 2005, available at <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=721422#PaperDownload > , p. 20.

184 *Id.*, p. 22.

185 *Id.*

186 J. T. Aranda, *op. cit., supra* note 173, p. 537.

187 R. Blanpain, 'Some Belgian and European Aspects', *Comp. Lab. L. & Pol'y J.,* Vol. 24, 2002, pp. 47, 63, 64.

188 See M. Rustad and S. R. Paulsson, *Monitoring Employee E-Mail And Internet Usage: Avoiding the Omniscient Electronic Sweatshops: Insights from Europe,* available at <http://lsr.nellco.org/suffolk/ip/papers/6>, 2005, p. 48 (noting that the right to privacy for European workers is 'inextricably linked with the development of trade unions, worker self-control and self-determination).

Legislation in Europe also provides for union representation of employees challenging invasions of privacy. A European Community Directive 'requires that: "Each [national] supervisory authority shall hear claims lodged by any person, *or by an association representing that person*, concerning the protection of his rights and freedoms in regard to the processing of personal data. ..." (emphasis added)'[189] The laws of Germany and Italy make similar provisions for workers to be aided by works council members and associations, respectively.[190] Unions in Belgium also have such representation rights.[191]

Finally, some collective bargaining agreements in other countries deal with privacy issues.[192] Australian unions in some industries have negotiated limitations on employer surveillance of employee computer use.[193] In New Zealand, the introduction of new technology is negotiable and some collective agreements have incorporated provisions relating to the subject.[194] A 2003 report on technology and privacy in the European Union reports that multi-employer bargaining on the issue is not common, citing agreements in Belgium, Norway and Denmark as the exceptions.[195] Collective agreements at the workplace level are not unusual, however.[196] The study notes that such bargaining is occurring not only in Austria, Belgium, Germany, the Netherlands, Norway, Spain and Sweden, all of which have legislation or central agreements requiring at least some consultation, but also in Finland, Greece, Italy, Luxembourg, Portugal, and the United Kingdom.[197]

In Belgium, the national collective agreement, which applies to all private employers, governs employee privacy and online communications

189 J. T. Aranda, *op. cit., supra* note 173, p. 539. The Council of Europe and the ILO make similar recommendations. *Id.*, pp. 539-540.

190 *Id.*, p. 540.

191 R. Blanpain, *op. cit., supra* note 187, p. 64.

192 See J. T. Aranda, *op. cit., supra* note 173, at 538-539 (describing the Belgian National Agreement on video surveillance and the recommendation of the French National Commission for Computer Technologies and Personal Freedom that privacy concerns relating to computers be negotiated between employers and unions).

193 R. McCallum and A. Steward, 'The Impact of Electronic Technology on Workplace Disputes in Australia', *Comp. Lab. L. & Pol'y J.*, Vol. 24, 2002, pp. 19, 39-40.

194 J. M. Howells, 'Electronic Technology and Workplace Issues: The New Zealand Situation', *Comp. Lab. L. & Pol'y J.*, Vol. 24, 2002, pp. 225, 240-241. The contract provisions discussed in the article do not focus on privacy issues, however, and the law in New Zealand does not limit employer monitoring in any significant way, except for a notice requirement. See *id.*, pp. 234-35, 240.

195 C. Delbar *et al.*, *op. cit., supra* note 174.

196 *Id.*

197 *Id.* The exact number of such agreements is unknown, but the report cites examples of specific agreements in France and Spain. *Id.*

data.[198] Detailed information regarding monitoring or control must be provided to the workers' representatives or in the absence of a representative, to the workers themselves.[199] The only legitimate reasons for such action are the following: 1. 'Prevention of unacceptable or slanderous acts ... ;' 2. Protecting the employer's confidentiality interests; 3. Protection of the information technology network; or 4. '*[B]ona fide* control of the policy rules' of the employer concerning use of technology.[200] Additionally, the employer's control must not interfere with the employees' private lives any more than necessary to achieve the legitimate purposes of the employer.[201] The agreement also strictly limits the employer's use of data to identify individuals sending or receiving electronic communications.[202]

In Norway, the central 'basic agreement' contains a supplementary agreement on monitoring which requires notice and discussion with the union, bars discrimination in monitoring, and mandates consultation with the union regarding the handling of information received through monitoring.[203] The Danish trade union confederation and the confederation of employers also negotiated a supplement requiring notice of new monitoring controls.[204] In addition, the social partners in the European Union have negotiated a framework for telecommuting workers which contains provisions regarding worker privacy and limitations on employer monitoring of workers.[205] This agreement will be implemented by the trade unions and employers, rather than by EU Directive.[206]

Though some variations exist, many of the countries discussed have much broader legal protection for privacy than the U.S.[207] and, in addition, provide for an important consultative role for worker representatives on matters relating to employee privacy. The legislative and collectively

198 R. Blanpain, *op. cit., supra* note 187, p. 60.
199 *Id.*, p. 62.
200 *Id.*, p. 61.
201 *Id.*
202 *Id.*, p. 63.
203 C. Delbar *et al., op. cit., supra* note 174.
204 *Id.* There is also a general provision in the national agreement in Greece recognizing employee rights to privacy. *Id.*
205 A. Broughton, *Social Partners Sign Teleworking Accord,* available at <http://www.eiro.eurofound.ie/2002/07/feature/eu0207204f.html>, (last visited September 30, 2005).
206 *Id.*
207 See M. Rustad and S. R. Paulsson, *op. cit., supra* note 188, pp. 51-89 (discussing European legislation and noting the importance of privacy as a fundamental human right in Europe which is protected without distinction between public and private workplaces); Delbar *et al., op. cit., supra* note 174, (discussing privacy legislation at the European Community and national level).

bargained provisions enable labor organizations in these countries to play a proactive role in shaping the employer's privacy policy within the limits of the law.

6. Collective Bargaining as a Vehicle for Privacy Protection for U.S. Employees

Can collective bargaining play a greater role in privacy protection for employees in the United States? First, it is important to recognize the role that collective bargaining has played to date. While there does not appear to be widespread negotiation of privacy provisions in collective bargaining agreements, contractual privacy protection has developed for unionized employees through arbitration. Such protection is comparable to the constitutional protection available in the public sector. Unions have contested employee discipline and challenged employer rules and practices on privacy grounds. They have established some general rules regarding privacy that are typically applied by arbitrators interpreting general provisions in collective bargaining agreements, to the benefit of represented employees. In interpreting agreements, arbitrators balance the employer's legitimate business needs with the employees' privacy interests. These arbitral principles then shape the future conduct of unionized employers dealing with privacy issues. In this time of shrinking, and thus weaker unions, arbitration under contractual just cause provisions and reasonable rule requirements may be the best vehicle available for protecting the privacy of employees represented by unions.

The limitation of this approach is its lack of predictability. Arbitrators are not bound by precedent and, as seen above, arbitrators may reach different determinations on similar facts. Thus, without predictable rules, employees may be uncertain of their rights. This uncertainty may lead employees to permit privacy infringements out of fear of termination, or to risk discharge without sufficient information as to the probability that a termination will be upheld in arbitration. Thus, at least in some cases, the protection may be more theoretical than real.

To combat this problem, unions could increase their efforts to negotiate explicit contractual privacy protections, supplementing the reactive approach to privacy with a more proactive one. Collective determination of privacy protections has some significant advantages. Collectively-bargained privacy provisions, with or without enhanced legal regulation, can be targeted at the issues most relevant to the particular workplace and the privacy concerns of the employees in the bargaining unit. Negotiation of privacy protections can provide employers with the flexibility necessary to operate in their particular markets, while ensuring the protection of

employee privacy interests.[208] As noted above, there are a wide range of privacy issues affecting workers – from computer monitoring to genetic testing to off-duty smoking bans. Some may be of little importance to workers in a particular workplace while others may be of vital interest. The union can identify and address those issues of importance and trade off in bargaining those that are not. In addition, unions and employers can respond to changes in technology more quickly than legislatures, dealing collectively with new issues raised by rapidly evolving technologies.[209] Furthermore, litigation pursuant to legislation is a time-consuming and expensive method of protecting employee rights. Collective action, through bargaining, provides an alternative method of protecting privacy that requires fewer resources from the employee, employer and government. Thus the goal of privacy protection may be achieved more efficiently.

Is collective bargaining a substitute for enhanced privacy legislation or a supplement to such legislation?[210] Initially, it should be noted that

---

208 J. T. Aranda, *op. cit., supra* note 173, pp. 538-539.

209 *Id.* For example, after a security breach involving identifiable information of employees at the Federal Deposit Insurance Corporation, the National Treasury Employees Union, which represents almost 5000 FDIC employees, demanded additional assistance from the agency for employees to prevent and respond to identity theft. See 'FDIC Informs Employees of Data Breach; Union Seeks Better ID Theft Assistance', *Gov't Employee Rel. Rep. (BNA),* Vol. 43, at p. 43 (June 28, 2005).

210 Unions should be aware that by negotiating privacy protections, they may in some cases waive employee rights to judicial action. In the private sector, the Supreme Court has not ruled on whether the union can waive employee rights, but has held that for such a waiver to be effective, it must be clear and unequivocal. *Wright* v. *Universal Maritime Serv. Corp.*, 525 U.S. 70(1998). Only the Fourth Circuit has found such a waiver. See, e.g., *Safrit* v. *Cone Mills Corp.*, 248 F.3d 306, 308 (4th Cir. 2001) (finding that collective bargaining agreement's provisions 'clearly and unmistakably' waived the employee's right to litigate her sex discrimination claim in court). The majority of courts have declined to find union waivers of employee rights to litigation. See, e.g., *Rogers* v. *New York University,* 220 F.3d 73 (2d Cir. 2000); *Air Line Pilots Ass'n* v. *Northwest Air Lines, Inc.*, 199 F.3d 477 (D.C. Cir. 1999); *Bratten* v. *SSI Servs. Inc.*, 185 F.3d 625 (6th Cir. 1999). Public employers, like private employers, have attempted to limit judicial litigation of statutory claims based on collective bargaining agreements, with limited success. See R. J. Kramer, 'Wright or Wrong: Can Employers and Unions Waive an Employee's Right to a Judicial Forum for Statutory Claims', *Urban Lwyr.*, Vol. 36, 2004, pp. 825, 832-836. In the federal sector, however, under the Civil Service Reform Act, judicial action may be precluded where a collective bargaining agreement covers the dispute unless the action falls within one of the statutory exceptions or unless the collective bargaining agreement excludes the matter from the grievance procedure. See 5 U.S.C. § 7121; *Whitman* v. *Dep't of Transp.*, 382 F.3d 938 (9th Cir. 2004). While *Whitman* found that the court had no jurisdiction over the plaintiff's constitutional privacy claim because it was covered by his collective bargaining agreement, the circuits are split on the issue and the Supreme Court has granted certiorari in *Whitman* to resolve the issue. 2005 U.S. Lexis 5032 (June 27, 2005).

employers are not required to bargain with unions regarding hiring practices so that collective bargaining is unlikely to protect the privacy rights of applicants for employment. Nor will it protect managers and supervisors. Thus, many individuals will not be protected by negotiated privacy protections. Yet passage of comprehensive privacy legislation seems unlikely. Additionally, even narrower legislation relating to workplace privacy has failed to pass at the federal level and in most states. While repeated revelations of privacy invasions outrage the public for a time, most recently the Choicepoint scandal, the push for protection, particularly at the workplace level, is generally insufficient to move legislation forward. In addition, there is an anti-regulatory political climate present in the U.S. today that does not bode well for privacy legislation. Critics of regulation argue, *inter alia*, that extensive regulation in this era where businesses need flexibility to respond to rapidly changing market conditions hampers the competitiveness of American business. Increased regulation is one factor influencing the relocation of operations overseas. If more expansive legal regulation is unlikely, then unions, where they exist, can provide greater protection for employees than the law currently provides while offering employers the flexibility that may be necessary to compete in global markets.

Moreover, even in the face of privacy legislation, there is a role for collective bargaining, as legal regulation necessarily paints with a broad brush.[211] Like the worker representatives in European countries with stronger privacy legislation, U.S. unions can assist in shaping the specific workplace rules to implement legislative directives. The evidence suggests that more unions are focusing on issues of computer privacy. As computers become ever more prevalent in the workplace,[212] privacy concerns will increase. Proactive participation by labor organizations on the front end can provide employees a greater voice in setting the terms of their employment and limiting employer inroads on employees' private lives. The new frontiers of privacy – computer monitoring, particularly location monitoring, and off-duty employee blogging – provide avenues for unions to test their ability to obtain collectively bargained privacy protections. Instead of merely arbitrating the grievance of the employee discharged for creating a blog that offends the employer, the union can negotiate the rules on off-duty blogging. Negotiated rules will provide a better balance of employer needs and employee rights than those created

211 J. T. Aranda, *op. cit., supra* note 173, p. 538.

212 As of 2001, almost 57 per cent of the workforce aged 25 and over used a computer at work and almost 42 per cent used the internet and/or e-mail. GAO Report, *supra* note 33, p. 4.

unilaterally, since even enlightened employers may be unaware or unconvinced of employee needs and interests.

To the extent that legislation exists, unions can provide assistance to employees in enforcing their legal rights.[213] In general, enforcement of legal rights is more effective in the unionized workplace because the union has resources to assist employees and protects employees from retaliation for asserting their rights. Furthermore, in some areas involving privacy, particularly those relating to technology, professional experts may be necessary and affordable only with union representation.

One significant limitation to this approach, however, is the shrinking percentage of workers covered by collective bargaining agreements in the U.S. Unionization in the private sector is particularly limited. Unions represent such a small percentage of the workforce that even universal negotiation of privacy protections would benefit a fraction of the workforce. And as unionization has decreased, collective power has decreased also, making it more difficult for unions to achieve their goals in collective bargaining. Thus, a desire for more contractual privacy protection may not be reflected in reality.[214] In addition, there is a risk that a weak union might be forced to sacrifice employee privacy protections available by statute if the law permits union waiver.[215] In the public sector, where unionization is more prevalent, collectively-bargained privacy protections could have a greater impact. Moreover, more unionized employees in the public sector are likely to be affected by employer techniques like computer monitoring. Although public employees have constitutional privacy protections, contractual privacy rights may be quicker and cheaper to enforce through the grievance and arbitration procedure. In the public sector, however, the right to bargain may be more limited as a result of statutory provisions.

There is another possible approach to regulation of workplace privacy. In the current political climate there is a trend toward self-regulation, in the workplace and elsewhere.[216] If this trend continues, we may see privacy issues in the workplace addressed through legislative or judicial provisions that promote self-regulation. As explained by Professor

213 Unions could play a similar role in an expanded regime of common law privacy rights. See W. R. Corbett, *op. cit., supra* note 2, pp. 154-159.

214 For example, the UAW mounted a legal challenge on constitutional grounds to a provision in bargaining agreement it negotiated, suggesting that it had insufficient power to eliminate the clause in negotiations. See *supra* note 73.

215 Given the very limited protections currently available to private sector employees, however, this is not a significant risk at present.

216 For extensive discussion of this trend, see C. Estlund, 'Rebuilding the Law of the Workplace in an Era of Self-Regulation', *Colum. L. Rev.*, Vol. 105, 2005, p. 319.

Estlund, self-regulation can be effective if there are organizations that serve as monitors.[217] A labor organization could participate as an internal monitor where it has representation rights, but Estlund suggests that unions can also serve as monitors of self-regulation where they do not represent a majority of the workers.[218] Unions might join with organizations dedicated to protecting privacy rights of all citizens to monitor businesses to insure respect for privacy of customers as well as employees. In addition joint employer-employee committees might serve a monitoring role in some industries to insure compliance with privacy protections.[219] Unions could assist employee committee representatives even without majority representation rights. While resource limitations may affect the ability of unions to perform such functions, employees who see the benefit of unions in this context might later become union members or organize their workplaces.

Does this theoretical expansion of the union role in enforcement of employee privacy interests show practical promise? Despite the benefits described, a significantly greater role for collective bargaining in privacy protection seems somewhat unlikely in the present climate. Private-sector unions are losing members and power. The public sector, where unionization rates are stable, offers greater promise than the private sector where existing legislation does not limit bargaining rights. The intrusiveness of new technologies in monitoring employees, and the growing concern about citizen and consumer privacy, may spur unions to put more emphasis on negotiating privacy protections. In an ideal world, collectively-bargained privacy protections could balance employer needs and employee interests, providing flexibility to tailor the provisions to fit current conditions and alter them with changing technology. Realistically, however, collective bargaining will probably continue to play a restricted role in the privacy arena. Existing protection through arbitration may remain the primary vehicle for protecting the privacy rights of employees in the unionized workplace.

217 *Id.*, pp. 355-383.
218 *Id.*, pp. 388-389.
219 J. T. Aranda, *op. cit., supra* note 173, pp. 537-538.