

2008

Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change

Alexandra Fiore

Matthew Weinick

Follow this and additional works at: <http://scholarlycommons.law.hofstra.edu/hlelj>



Part of the [Law Commons](#)

Recommended Citation

Fiore, Alexandra and Weinick, Matthew (2008) "Undignified in Defeat: An Analysis of the Stagnation and Demise of Proposed Legislation Limiting Video Surveillance in the Workplace and Suggestions for Change," *Hofstra Labor and Employment Law Journal*: Vol. 25: Iss. 2, Article 6.

Available at: <http://scholarlycommons.law.hofstra.edu/hlelj/vol25/iss2/6>

This document is brought to you for free and open access by Scholarly Commons at Hofstra Law. It has been accepted for inclusion in Hofstra Labor and Employment Law Journal by an authorized administrator of Scholarly Commons at Hofstra Law. For more information, please contact lawcls@hofstra.edu.

NOTES

UNDIGNIFIED IN DEFEAT: AN ANALYSIS OF THE STAGNATION AND DEMISE OF PROPOSED LEGISLATION LIMITING VIDEO SURVEILLANCE IN THE WORKPLACE AND SUGGESTIONS FOR CHANGE

I. INTRODUCTION

What do the phrases “reality television” and “workplace privacy,” have in common? Both phrases, in large part due to improvements in technology, are misnomers. While most savvy reality show viewers realize that their favorite shows are cast, contrived and edited, thereby taking the “reality” out of reality television, many employees continue to rely upon a false notion that they possess an inherent and basic human right to privacy and that this right follows them to work each day. So, while reality show participants elect to expose themselves to the tireless eyes of electronic cameras, many employees may be unaware that hidden cameras are recording their every move.

Video surveillance is becoming increasingly widespread in the workplace. According to a 2005 survey by the American Management Association, a growing percentage of the 526 employers participating reported that they regularly monitor the conduct of their employees.¹ Furthermore, while the sophistication of surveillance equipment is increasing, the cost is falling precipitously. “A decent closed-circuit TV (video surveillance) equipment [sic] costs less than \$3,000, and the cameras, using fiber-optic technology, can acquire a good image from a

1. Am. Mgmt. Ass’n & Nancy Flynn, The ePolicy Inst., *2005 Electronic Monitoring & Surveillance Survey*, AM. MGM’T ASS’N, May 18, 2005, https://www.amanet.org/research/pdfs/EMS_summary05.pdf. “23% [of the participating entities] represent companies employing 100 or fewer workers, 101–500 employees (25%), 501–1,000 (10%), 1,001–2,500 (13%), 2,501–5,000 (7%) and 5,001 or more (22%).” *Id.*

hole the size of a pencil point.”² A range of technology including hidden cameras, recording devices, and tiny wireless cameras, is available for less than five hundred dollars.³

A thin line exists between surveillance and voyeurism. Gail Nelson, an employee of Salem State College in Massachusetts, had to apply prescription ointment to her severe sunburn during the summer of 1995.⁴ At times when she was not expecting clients or visitors, she went to the back of the office, behind partitions, and unbuttoned her blouse to apply the prescribed ointment to her chest and neck.⁵ Gail also changed her clothes numerous times that summer behind the same partitions before or after business hours when the office was empty and the front door was locked.⁶

During that same time period, the college learned about possible unauthorized access to the office.⁷ For security reasons, the college installed hidden surveillance cameras that were set up in the same area where Gail applied her ointment and changed.⁸ She eventually learned of the surveillance and sued the college.⁹ The court, however, granted the Defendant’s motion for summary judgment, ending the suit.¹⁰

The indignity Gail suffered is not an isolated event. In Lafayette, Louisiana, the Wal-Mart Store installed a video camera in the employee unisex bathroom to catch a suspected thief.¹¹ Theft and unauthorized conduct by employees led to the installation of a video camera in the employee locker room at Johnson County Community College.¹² Most recently, workers at a Kentucky distribution center discovered a video

2. Parry Aftab, *The Privacy Lawyer: To Videotape Or Not To Videotape*, INFORMATIONWEEK, Aug. 16, 2004, <http://www.informationweek.com/shared/printableArticleSrc.jhtml?articleID=26806697>.

3. See, e.g., *Wireless Security Cameras*, <http://www.surveillance-spy-cameras.com> (follow links for digital surveillance, wireless hidden cameras, and armor dome cameras) (last visited Mar. 27, 2008).

4. *Nelson v. Salem State Coll.*, 845 N.E.2d 338, 344 (Mass. 2006).

5. *Id.*

6. *Id.* at 344, 347.

7. *Id.* at 343.

8. *Id.*

9. *Id.* at 344.

10. *Id.* at 342.

11. *Meche v. Wal-Mart Stores, Inc.*, 692 So. 2d 544, 546 (La. Ct. App. 1997). The installation of the camera was not completed before it was discovered. *Id.* Wal-Mart Management alleged that in its review of all the surveillance tapes in its possession, none showed any recordings of the bathroom. *Id.* at 547.

12. *Thompson v. Johnson County Cmty. Coll.*, 930 F. Supp. 501, 503-04 (D. Kan. 1996). The locker room was used primarily for storage, however, employees often changed their clothes as well. *Id.*

camera installed in the men's bathroom.¹³

Employers use surveillance to monitor productivity, and to protect property and workers' safety.¹⁴ However, the unchecked use of video surveillance is leading to invasive forms of surveillance, such as direct surveillance, even outside the workplace.¹⁵ This note explores the existing statutory and common law protections workers have against workplace video surveillance. There are few protections available. In public workplaces, the Fourth Amendment is relied upon, but proves insufficient. Private causes of action include invasion of privacy and intentional infliction of emotional distress, but both are difficult to prove and depend on state common and statutory law. Labor unions have statutory protections that non-union workers do not have, but these protections have been limited as well.

There is great disparity amongst applicable laws in various states, public versus private workplaces, and union as opposed to non-union workplaces. Several states, including New York, Connecticut, and New Jersey have enacted statutes to specifically address workplace privacy concerns,¹⁶ however, the scope of these laws is inconsistent and, in many states, inadequate.

Certainly, video surveillance is useful and in some circumstances even necessary. Employers have a right to protect their business interests and property,¹⁷ but this reasoning must not be used as pretext to monitor

13. *Barbo v. The Kroger Co.*, No. 3:07-CV-14-S, 2007 WL 2350179, at *1 (W.D. Ky. Aug. 13, 2007) (suing the manager); *Barbo v. The Kroger Co.*, 3:07-CV-14-S, 2007 WL 2350183, at *1 (W.D. Ky. Aug. 13, 2007) (suing the employer-company).

14. See Hanah Cho, *Think Before You Surf at Work: Employee Monitoring of Internet, E-mail, Phone Use Becomes More Intrusive*, BALTIMORE SUN, Sept. 25, 2006, <http://www.baltimoresun.com/business/careers/bal-cho0925,0,4984114.column?coll=bal-careers-utility>.

15. See Michael Barbaro, *Bare-Knuckle Enforcement for Wal-Mart's Rules*, N.Y. TIMES, Mar. 29, 2007, at A1. Wal-Mart has hired a team of investigators, including former FBI agents. *Id.* These investigators have conducted investigations into sexual relations between employees outside the workplace, monitored phone conversations, and even intimidated workers who question authority. See *id.*

16. N.Y. LAB. LAW. § 203-c (McKinney Supp. 2008); CONN. GEN. STAT. ANN. § 31-48b (West 2003); N.J. STAT. ANN. §§ 2A:156A-1 to :156A-34 (West Supp. 2007).

17. Video surveillance has also proven useful for employers to protect themselves against discrimination and sexual harassment claims. See *Kumar v. United Health & Hosp. Servs., Inc.*, No. 3:04-CV-2782, 2007 WL 200958, at *2 (M.D. Pa. Jan. 22, 2007); *Napreljac v. John Q. Hammons Hotels, Inc.*, 461 F. Supp. 2d 981, 993 (S.D. Iowa 2006), *aff'd*, 505 F.3d 800 (8th Cir. 2007). By recording the allegedly discriminatory or harassing actions, the employer can use the tape as evidence at trial. See *Kumar*, 2007 WL 200958, at *2; *Napreljac*, 461 F. Supp. 2d at 993. However, sexual harassment is emerging as another cause of action to combat video surveillance. E.g. *EEOC v. Smokin' Joe's Tobacco Shop*, No. 06-01758, 2007 WL 1258132, at *1-*2 (E.D. Pa. Apr. 27, 2007).

at will. This note will analyze past proposals considered by Congress and discuss their individual and collective weaknesses. Most proposals introduced in Congress have been incomplete. Those proposals focused on prohibiting cameras from only the most intrusive areas of the workplace, such as restrooms. While restrooms are undoubtedly private areas, where cameras should not be installed, this limited prohibition does not address the larger concerns about the maintenance of workers' individual and collective dignity.¹⁸

The note will conclude with a new, comprehensive legislative proposal that addresses these weaknesses. The revamped legislation would include notice requirements (as to when and how employees will be monitored), provide for monitor free areas (such as break rooms and locker rooms), ensure compliance by imposing civil penalties for minor violations (such as failure to give notice), and criminal prosecution for major infractions (such as monitoring a statutorily prohibited area).

"[Video] surveillance provokes an immediate negative visceral reaction: indiscriminate video surveillance raises the spectre of the Orwellian state."¹⁹ Due to video surveillance's extremely invasive nature and the disparity between state and local laws, Americans need federal legislation designed to protect the privacy and dignity of the workforce.

A. Privacy v. Dignity

American jurisprudence has relied on the concept of privacy to battle workplace surveillance.²⁰ Black's Law Dictionary defines privacy as "[t]he condition or state of being free from public attention to intrusion into or interference with one's acts or decisions."²¹ Privacy in American law has been treated similarly to property rights²² and therefore the protections associated with it have been limited.²³

18. See discussion *infra* Parts I.A.

19. The court was specifically addressing police video surveillance, however, their characterization of video surveillance in general is applicable to the workplace. *U.S. v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987); see generally GEORGE ORWELL, 1984 3-4 (Harcourt Brace Jovanovich 1949) (describing a world where privacy no longer exists and the government has the ability to monitor everything, including a person's thoughts).

20. See *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987); *Vega-Rodriguez v. P.R. Tel. Co.*, 110 F.3d 174, 182 (1st Cir. 1997).

21. BLACK'S LAW DICTIONARY 1233 (8th ed. 2004).

22. See, e.g., *Katz v. United States*, 389 U.S. 347, 350-51 (1967).

23. See Lawrence R. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 382-83 (2000).

The concept of dignity may prove to be a more appropriate framework for understanding the issues presented by electronic workplace surveillance, providing employees with stronger protections. Black's definition of dignity is consistent with how American law has dealt with the topic. Legally, dignity is defined simply as "the state of being noble."²⁴ American law does not consider the concept as having any legal influence. Webster's Dictionary defines dignity as "the quality of being worthy of esteem or honor" and "a high position, rank, or title."²⁵ At the heart of the idea, dignity is a social concept that "promotes a humane and civilized life."²⁶

The concept of dignity is widespread in continental Europe.²⁷ As opposed to property, it is rooted in the conceptions of community and citizenship.²⁸ For instance, workers in France are considered part of an "enterprise community."²⁹ The workplace is a forum for fostering social relationships as well as for personal goals such as self-fulfillment and self-discovery.³⁰ Work is performed not only for economic purposes, but also to fulfill basic human needs.³¹ By reducing the employee to nothing more than a means for production, an employer violates the employee's dignity.³²

Previously proposed and enacted legislation shows that U.S. lawmakers have taken a truly American view of the problem of workplace surveillance.³³ The result is that limitations on video surveillance do not go beyond particularly private areas, such as locker rooms, changing rooms, and bathrooms.³⁴ Only by embracing the European idea of dignity can one truly understand the need for further regulation to regain respect for each other as humans instead of, simply, as bodies.

24. BLACK'S LAW DICTIONARY 488 (8th ed. 2004).

25. WEBSTER'S NEW WORLD COLLEGE DICTIONARY 403 (IDG Books Worldwide, Inc. 4th ed. 2001).

26. Rothstein, *supra* note 23, at 383.

27. *Id.*

28. *Id.*

29. *Id.* at 384.

30. *Id.*

31. *Id.*

32. *Id.* at 383.

33. Compare discussion *infra* Part IV with discussion *infra* Part V.

34. Rothstein, *supra* note 23, at 382-83.

B. Privacy Protection Legislation: An Economic Rationale

Americans spend a considerable amount of time at work. Twenty-eight percent of Americans work more than forty hours per week and eight percent work more than sixty hours per week.³⁵ "An average American gets 14 days of vacation [per year] but takes only 11."³⁶ This means that many workers involuntarily subject themselves to more than two thousand hours of video camera surveillance per year.

"Electronic monitoring acts as an electronic whip that drives the fast pace of today's workplace in the growing service industry."³⁷ The unregulated use of electronic monitoring is turning modern offices into "electronic sweatshops."³⁸ Because of the repetitive nature of office duties and the importance of attention to detail in performing these duties, relentless monitoring places great stress on employees.³⁹ In 1993, the estimated cost of workplace stress in the United States was fifty billion dollars.⁴⁰

General notice of monitoring practices is not a complete solution. The standard form of notice only advises employees that the company "reserves the right to monitor anything at any time."⁴¹ Without notification of the specific types of monitoring, employees do not know if their computers or phone conversations are being monitored, or if video surveillance is used.⁴² They do not know if the monitoring is continuous or random, or even whether management is actually monitoring them at all.⁴³

This uncertainty adds to workplace stress and violates a person's sense of dignity. An Australian Privacy Commissioner's study concluded that video surveillance substantially impacts the work environment.⁴⁴ Video surveillance has the effect of undermining morale

35. Chris Gaylord, *Office Hours: Unions, Wages, White Shirts*, CHRISTIAN SCI. MONITOR, Sept. 5, 2006, at 20.

36. Paul B. Brown, *All Tapped Out, or Maybe Not*, N.Y. TIMES, June 2, 2007, at C5.

37. 139 CONG. REC. 10,354, 10,355 (1993) (statement of Sen. Paul Simon).

38. *Id.*

39. *Id.*

40. *Id.* The estimate is a measure of health care and lost productivity. *Id.*

41. NAT'L WORKRIGHTS INST., PRIVACY UNDER SIEGE: ELECTRONIC MONITORING IN THE WORKPLACE 4 (Dec. 2004), available at http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf.

42. *Id.*

43. *Id.*

44. TIM DIXON, THE PRIVACY COMM. OF NEW S. WALES, No. 67, INVISIBLE EYES: REPORT ON VIDEO SURVEILLANCE IN THE WORKPLACE § 3.4 (Aug. 1995), available at <http://www.austlii.edu.au/au/other/CyberLRes/1995/video/index.html>.

and creating distrust and suspicion between employees and management.⁴⁵ One respondent to the study noted, "I also think that employees have a right to work relatively comfortably in their work environment, unselfconsciously, and I think this is impossible when you know that every movement is being recorded by a camera."⁴⁶

Privacy is a vexing issue for legislators and surveillance is a double-edged sword. The fact that opponents of workplace surveillance typically rely upon non-economic arguments might partially explain why mainstream economics, so far, has been surprisingly silent on this important issue. Generally speaking, critics of electronic monitoring laws emphasize teleological arguments (non-moral results based almost solely on productivity) to support their ideas, whereas proponents of privacy protection laws generally favor deontological arguments, stressing ethical concerns such as humility, dignity, and respect.⁴⁷ Employers generally believe that they should be able to engage in monitoring in order to increase productivity as well as to reduce costs.⁴⁸ Furthermore, they claim that technological surveillance is only implemented when the result is an increase in the total surplus generated in the workplace.⁴⁹ Otherwise, the employer would have a disincentive to monitor because it would not be in the employer's best interest to do so.

Numerous studies, however, demonstrate that increased monitoring often contributes to an atmosphere of distrust amongst employees, which is certainly not conducive to high levels of productivity.⁵⁰ Employees who have their performance monitored incur health problems due to stress and high levels of tension.⁵¹ However, scholars have offered an additional argument that laws restricting workplace surveillance are desirable even if the surveillance does not harm the individual employees.⁵² In essence, this takes those same teleological arguments employed by critics of privacy protection and uses them in favor of legislation.

For example, take as given the fact that an employer is only

45. *Id.*

46. *Id.*

47. G. Stoney Alder, *Ethical Issues in Electronic Performance Monitoring: A Consideration of Deontological and Teleological Perspectives*, 17 J. BUS. ETHICS 729, 730-32, 736 (1998).

48. *Id.* at 731 (citations omitted).

49. Patrick W. Schmitz, *Workplace Surveillance, Privacy Protection and Efficiency Wages*, 12 LAB. ECON. 727, 728 (2005).

50. Alder, *supra* note 47, at 733-34 (citations omitted).

51. *Id.* at 735.

52. Schmitz, *supra* note 49, at 729.

interested in maximizing profits and that an employer who wants his or her employees to work hard must provide incentives to those employees.⁵³ Economists of efficiency wage literature commonly refer to this incentive as “rent.”⁵⁴ So, in other words, the employer must pay the “wealth-constrained” employee a positive rent in order to provide an incentive for exerting effort that is otherwise unobservable.⁵⁵ The alternative, employers argue, is to make the effort observable by implementing video surveillance.⁵⁶ The theory is that an employer will not have to provide as much rent as an incentive to work hard if the effort is directly observable and can be measured by the employer.⁵⁷

However, surveillance has costs of its own. Laws preventing video surveillance can actually increase the total workplace surplus.⁵⁸ Although such laws will decrease employer’s surplus, this loss can be offset and surpassed by the gain to the employees.⁵⁹ After all, the employer invests in surveillance equipment not only to achieve higher rates of effort from employees, but also to reduce the amount of rent that employers must pay those employees to exert effort.⁶⁰ Employer profit is equal to total surplus minus the employees’ rent.⁶¹ Therefore, if the reduction of the employee’s rent due to monitoring is sufficiently large, then the employer will incur monitoring costs even if they are larger than the additional surplus generated by higher effort.⁶² The employer will be wasting resources in order to redistribute wealth.⁶³ Therefore, if surveillance laws were implemented, this could decrease the amount of rent that the employer would have to pay the employee and could increase the two parties’ total surplus.⁶⁴

This theory assumes that the employee does not directly suffer from the loss of his or her privacy. It, therefore, attempts to make surveillance more desirable than it actually is. Even given this advantage, it can be argued that laws restricting surveillance produce the most efficient outcomes for society.

53. *Id.*

54. *See id.*

55. *Id.*

56. *Id.*

57. *See id.*

58. *Id.* at 732.

59. *Id.*

60. *Id.*

61. *Id.* at 729.

62. *Id.* at 732.

63. *Id.*

64. *Id.*

II. FEDERAL CONSTITUTIONAL HISTORY

A. A Constitutional Right to Privacy?

The federal right to privacy has been established as an avenue for public employees only, leaving private employees to rely on other causes of action.⁶⁵ Constitutional privacy rights have only been established via case law. There are no explicit privacy guarantees in the Constitution.⁶⁶ These rights, as developed by the Supreme Court through precedent, are grossly inadequate.

*Griswold v. Connecticut*⁶⁷ is the first United States Supreme Court case to hold that the Constitution provides a right of privacy.⁶⁸ Though privacy is not an enumerated right, the Court infers it from several parts of the Constitution, as well as from previous decisions.⁶⁹ In the past, the Court upheld the right of people to associate, the right of a parent to choose a child's education, and the right to study what one chooses, even though these rights are not explicit.⁷⁰ Justice Douglas stated that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance."⁷¹ The Third, Fourth, Fifth, and Ninth Amendment guarantees each create "zones of privacy."⁷²

The Supreme Court further linked the Fourth Amendment to the notion of privacy in *Katz v. United States*.⁷³ In *Katz*, the petitioner violated federal law by using a public telephone to transmit wagering information interstate.⁷⁴ The FBI used audio surveillance on the phone booth to catch the petitioner in the act by attaching a listening device to

65. The Fourth Amendment is limited to government actors. *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). The Fourteenth Amendment has made the Fourth Amendment applicable to state actors. *Mapp v. Ohio*, 367 U.S. 643, 655 (1961). However, some state constitutions, such as California, extend privacy protection to individuals against private actors. *Hill v. NCAA*, 865 P.2d 633, 644 (Cal. 1994).

66. *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965) (acknowledging that the right of privacy "is not mentioned explicitly in the Constitution").

67. 381 U.S. 479 (1965).

68. *Id.* at 485 (holding there is a marital right of privacy protected by the constitution).

69. *See id.* at 481-86.

70. *Id.* at 482-83.

71. *Id.* at 484.

72. *Id.* at 484-85.

73. 389 U.S. 347, 350-53 (1967).

74. *Id.* at 348.

the outside of the booth.⁷⁵ The Court rejected the “trespass doctrine”⁷⁶ and held the petitioner justifiably relied on privacy by entering the booth and closing the door.⁷⁷ The government violated privacy within the meaning of the Fourth Amendment by monitoring the petitioner’s conversation, despite the fact that the listening device did not “penetrate the wall of the booth.”⁷⁸

In 1987, the Supreme Court directly addressed workplace privacy in *O’Connor v. Ortega*.⁷⁹ The *O’Connor* plaintiff was a doctor placed on administrative leave during an investigation of charges against him.⁸⁰ While on leave, the hospital entered the plaintiff-doctor’s office to inventory property.⁸¹ The administration took several personal items from his desk including a Valentine’s Day card, a photograph, and a book of poetry.⁸² The Court held that the Fourth Amendment’s prohibitions against unreasonable searches and seizures apply to government employers and supervisors, not just law enforcement.⁸³

The *O’Connor* decision extended Fourth Amendment protection to employees’ private property regardless of whether they are suspected of criminal activity.⁸⁴ Furthermore, the decision provided that just because an employee works for the government instead of a private employer does not mean that he or she loses Fourth Amendment rights.⁸⁵ An employee’s Fourth Amendment rights are violated when the employer infringes on a reasonable expectation of privacy.⁸⁶ In determining a reasonable expectation, a court may look to the framers’ intention, an individual’s use of a particular location, and whether “certain areas deserve the most scrupulous protection from government invasion.”⁸⁷

The Court held that the reasonableness standard must be decided on a case-by-case basis.⁸⁸ Courts must balance the worker’s Fourth

75. *Id.*

76. The trespass doctrine requires a “technical trespass . . . under local property law” before Fourth Amendment protections are violated. *Id.* at 353 (citing *Silverman v. United States*, 365 U.S. 505, 510-11 (1961)).

77. *Katz*, 389 U.S. at 353.

78. *Id.*

79. 480 U.S. 709, 714-19 (1987).

80. *Id.* at 713.

81. *Id.* at 712-13.

82. *Id.* at 713.

83. *Id.* at 714, 717-18.

84. *Id.* at 715.

85. *Id.* at 717.

86. *Id.*

87. *Id.* at 715 (citing *Oliver v. United States*, 466 U.S. 170, 178 (1984)).

88. *Id.* at 717-18.

Amendment interests against the importance of the government's intrusion.⁸⁹ While some employees may have a reasonable expectation of privacy in their office or desks, that expectation may be reduced by office practices or procedures and must be assessed in the "context of the employment relation."⁹⁰ Coworkers, supervisors, or the public continually enter some offices.⁹¹ Notably, the Court states that some offices may be open to the extent that they completely eliminate any expectation of privacy.⁹²

B. The Fourth Amendment's Application to Public Workplace Video Surveillance

In a Fourth Amendment claim against a public employer for an unreasonable search by means of video surveillance,⁹³ an employee must prove there was a subjective *and* objective reasonable expectation of privacy.⁹⁴ In most cases, courts have assumed that the plaintiff had a subjective expectation of privacy and have therefore focused their analysis on whether there was an objective expectation.⁹⁵ There is no bright line rule to determine whether a reasonable expectation of privacy exists; courts instead look to the guidelines established by *O'Connor* in making their determination.⁹⁶

The reasonableness standard, as developed, is so narrow that few employees will be protected from video surveillance under the Fourth Amendment. The mere possibility that an unexpected person may enter the area may be enough to defeat an expectation of privacy. Gail Nelson's story is a clear example.⁹⁷ Ms. Nelson hid behind an office partition while changing and applying lotion to intimate areas, but, it

89. *Id.* at 719 (citing *United States v. Place*, 462 U.S. 696, 703 (1983); *Camara v. Municipal Court*, 387 U.S. 523, 536-37 (1967)).

90. *Id.* at 717.

91. *Id.*

92. *Id.* at 718. The Court held that the plaintiff-doctor did have a reasonable expectation of privacy in his office and desk because they were not shared with other employees and the employer did not discourage employees from keeping personal items in the workplace. *Id.* at 718-19.

93. Video surveillance has been held to be a Fourth Amendment search. See *United States v. Torres*, 751 F.2d 875, 882-83 (7th Cir. 1984).

94. *Vega-Rodriguez v. P.R. Tel. Co.*, 110 F.3d 174, 178 (1st Cir. 1997); *Sacramento County Deputy Sheriffs' Assoc. v. County of Sacramento*, 59 Cal. Rptr. 2d 834, 843 (Cal. Ct. App. 1996); *Nelson v. Salem State Coll.*, 845 N.E.2d 338, 346 (Mass. 2006) (citing *Vega-Rodriguez*, 110 F.3d at 178).

95. *E.g.*, *Vega-Rodriguez*, 110 F.3d at 178; *Nelson*, 845 N.E.2d at 346.

96. See discussion *supra* Part II.A.

97. See discussion *supra* Part I.

was reasoned, because the area was not completely closed off from the rest of the office and it was possible for other employees or clients to walk past the area, there was no objectively reasonable expectation of privacy.⁹⁸ It did not matter that she conducted herself discreetly or that many times she applied her medication after hours, while the doors were locked.⁹⁹ The court held the entire office was an “open work area” and despite her subjective belief of privacy, society could not consider such an area to be private.¹⁰⁰

In *Thompson v. Johnson County Community College*,¹⁰¹ the plaintiffs were security officers employed by a community college.¹⁰² The employees had access to a locker room where they kept their belongings and changed clothes.¹⁰³ The college installed a video surveillance camera in the locker room.¹⁰⁴ The security officers did not exclusively use the locker room;¹⁰⁵ it was also a storage area and contained the air conditioning equipment.¹⁰⁶ Access was not restricted and maintenance workers and other individuals could enter the room at will to retrieve items from storage.¹⁰⁷ After considering these factors, the court ruled that the defendants did not have a reasonable expectation of privacy.¹⁰⁸

The court reached the same result in *Brannen*,¹⁰⁹ when school custodians sued their employer, the school district, for covert video surveillance of the break room.¹¹⁰ Applying the *O'Connor* standards, the court held the custodians did not have a reasonable expectation of privacy because the room was open to all school employees.¹¹¹ The court characterized the room as an all purpose room because it contained a microwave, washing machine, and cleaning supplies.¹¹²

98. *Nelson*, 845 N.E.2d at 347.

99. *Id.*

100. *Id.*

101. No. 96-3223, 1997 WL 139760 (10th Cir. March 25, 1997).

102. *Id.* at *1.

103. *Thompson v. Johnson County Cmty. Coll.*, 930 F. Supp. 501, 507 (D. Kan. 1996), *aff'd*, 1997 WL 139670 (10th Cir. 1997).

104. *Id.* at 504.

105. *Thompson*, 1997 WL 139760, at *1.

106. *Id.*

107. *Id.*

108. *Id.* at *2.

109. *Brannen v. Kings Local Sch. Dist. Bd. of Educ.*, 761 N.E.2d 84 (Ohio Ct. App. 2001).

110. *Id.* at 88-89.

111. *Id.* at 91-92.

112. *Id.*

C. The Fourth Amendment Fails to Adequately Protect the Workforce's Dignity

Nelson, Thompson, and Brannen are examples of how the Fourth Amendment fails to provide adequate protections against invasive video monitoring of employees. In *Vega-Rodriguez v. P.R. Tel. Co.*,¹¹³ the court recognized both the invasiveness of surveillance and the constitution's failure to provide protection.¹¹⁴

The *Vega-Rodriguez* plaintiffs were employees of the Puerto Rico Telephone Company ("PRTC").¹¹⁵ Their job was to monitor the company's computers for alarms.¹¹⁶ The plaintiffs worked in the penthouse of an office complex where access was restricted and entry required an access card.¹¹⁷ The workspace was "open" in that employees worked in one large area and did not have separate offices or cubicles.¹¹⁸ PRTC installed three video cameras that surveyed the work area and another one to monitor the main entrance.¹¹⁹ With the employees' knowledge, the cameras operated "all day, everyday," and recorded "every act undertaken in the work area."¹²⁰

The plaintiffs argued that management is expected to watch their employees; however, video surveillance is unrelenting and, "unlike the human eye [a camera] never blinks."¹²¹ The "unrelenting eyes" of a camera prohibit a worker from yawning, scratching, or making any movement in privacy.¹²² The court rejected this as a Fourth Amendment argument.¹²³ In constitutional terms, relying on the Fourth Amendment, the plaintiffs asked the court to prohibit management from doing electronically that which it could legally accomplish with human eyes.¹²⁴ The court concluded that an individual could not have a reasonable expectation of privacy in that which is displayed openly.¹²⁵ Because of

113. 110 F.3d 174 (1st Cir. 1997).

114. *See id.* at 178.

115. *Id.* at 176. PRTC is a quasi-public company thus the fourth amendment applies. *Id.* at 178.

116. *Id.* at 176.

117. *Id.* at 176.

118. *Id.*

119. *Id.*

120. *Id.*

121. *Id.* at 180.

122. *Id.* at 181.

123. *Id.* at 182.

124. *Id.* at 180.

125. *Id.* at 181. This rule is known as the plain view doctrine. *Id.* at 180. The court cautions that its holding *might* be different if the surveillance were covert. *Id.* at 180-81.

the open nature of the workplace, the court concluded plaintiffs had no expectation of privacy.¹²⁶ “[T]he mere fact that the observation is accomplished by a video camera rather than the naked eye, and recorded on film rather than in a supervisor’s memory, does not transmogrify a constitutionally innocent act into a constitutionally forbidden one.”¹²⁷

The Constitution sees no difference between an electronic video camera and a human eye and this is where a fundamental flaw exists in American law. As the *Vega-Rodriguez* plaintiffs point out, there is a practical difference between a human eye and video camera.¹²⁸ A video camera is unrelenting for every minute of every day.¹²⁹ Employees would not expect a supervisor to stand above their desks every second of the day and watch every movement made. A supervisor is also unable to recall an exact moment in time from memory like videotape and to display that memory so that others can see the images in the same way they were perceived. In direct contrast, a recorded video image can exist forever and can be shared with others.

The humiliation exemplified in *Nelson*, the intrusiveness in *Thompson*, and the disrespect in *Vega-Rodriguez*, identifies many of the problems created by unregulated video surveillance. Furthermore, these cases illustrate the need for Congress to enact rules regulating workplace video surveillance. American workers cannot rely solely on the Constitution’s elusive right to privacy.

III. FEDERAL STATUTORY HISTORY

A. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act of 1986¹³⁰ (“ECPA”), also referred to as the Federal Wiretapping Act, prohibits the intentional interception and disclosure of wire, oral, and electronic communications (including those which occur in the workplace).¹³¹ Violators of the Act

126. *Id.* at 180.

127. *Id.* at 181.

128. *See id.* at 180.

129. *See id.* at 181; *cf.* ORWELL, *supra* note 20, at 28 (“Always the eye watching you Asleep or awake, working or eating, indoors or out of doors, in the bath or in bed—no escape. Nothing was your own except the few cubic centimeters inside your skull.”).

130. 18 U.S.C. §§ 2510-2522 (2000).

131. *Id.* § 2511.

are subject to civil liability, including punitive damages.¹³²

The Act protects workplace phone calls, e-mail and Internet access, however, it contains loopholes for employers. Most notably, the Act has been interpreted as completely inapplicable to video-only surveillance.¹³³ Therefore, installation of a video-only surveillance system in a security personnel dressing and changing room did not violate the Act because the statute does not prohibit silent video recordings.¹³⁴ As a result, statutory violations of video surveillance arise only if microphones are used in conjunction with the video cameras, resulting in audio-visual surveillance.¹³⁵ Therefore, employers can circumvent the statute by simply eliminating the audio component while continuing to record employees' actions.

The Federal Wiretapping Act of 1986 set important privacy standards for technologies that were emerging in the 1980's. Unfortunately, opportunities for surveillance in the workplace have expanded tremendously in the last two decades and privacy law has not kept pace.¹³⁶

B. Video Voyeurism Prevention Act of 2004

Congress has also enacted the Video Voyeurism Prevention Act of 2004¹³⁷ ("VVPA"). It is general in coverage and does not apply only to the workplace.¹³⁸ The Act prohibits intentional capturing¹³⁹ of an image of an individual's "private area"¹⁴⁰ when the actor knows the individual

132. *Id.* §§ 2511(4), (5), 2520(b).

133. See *U.S. v. Koyomejian*, 970 F.2d 536, 537 (9th Cir. 1992) ("We . . . now hold that silent video surveillance is neither prohibited nor regulated by [the Act]."); *Audenreid v. Circuit City Stores, Inc.*, 97 F. Supp. 2d 660, 663 (E.D. Pa. 2000) (installing a video camera that did not record sounds in the manager's office did not violate federal or Pennsylvania wiretapping laws).

134. See *Thompson v. Johnson County Cmty. Coll.*, 930 F. Supp. 501, 506 (D. Kan. 1996), *aff'd*, No. 96-3223, 1997 WL 139670 (10th Cir. Mar. 25, 1997).

135. *Thompson*, 930 F. Supp. at 505.

136. See David N. King, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S. CAL. L. REV. 441, 468 (1994); Sandra Byrd Petersen, *Your Life as an Open Book: Has Technology Rendered Personal Privacy Virtually Obsolete?*, 48 FED COMM. L.J. 163, 164 (1995); Alan F. Westin, *Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271, 272 (1996).

137. 18 U.S.C. § 1801 (2000).

138. See *id.* The statute applies to anyone within the "special maritime and territorial jurisdiction of the United States." *Id.*

139. *Id.* § 1801(b)(1) (capture means to videotape, photograph, or film).

140. *Id.* § 1801(b)(3)-(4) (private areas are the "naked or undergarment clad genitals, pubic area, buttocks, or female breast").

has a reasonable expectation of privacy.¹⁴¹ An individual has a reasonable privacy expectation when the person believes he or she can disrobe without concern that images are being captured of private areas¹⁴² or when the person believes the private areas are not visible to public.¹⁴³

The Act is an affirmative recognition of advanced technology's increasing ability to invade privacy.¹⁴⁴ The statute is intended to prohibit "video voyeurism," as opposed to general video surveillance, that may have a legitimate purpose, yet is still intrusive.¹⁴⁵ The Act's weakness in the workplace is the reasonableness standard. Gail Nelson would likely still be unsuccessful had she been able to rely on the VVPA.¹⁴⁶ Though the reasonableness standard in the VVPA appears more subjective, the standard has failed employees time and again and it is a poor standard for the workplace. It relies solely on privacy and neglects to protect dignity.

C. NLRA: Labor Unions are Afforded Some Federal Protection and Demonstrate the Importance of Remedies

The National Labor Relations Act protects employees who engage in "protected activities."¹⁴⁷ Courts have generally held that video surveillance tends to interfere with, restrain, or coerce employees in exercising protected activities.¹⁴⁸ Recent National Labor Relations Board ("NLRB") cases have established that employers must provide notice to labor unions before installing surveillance cameras.¹⁴⁹ The

141. *Id.* § 1801(a).

142. *Id.* § 1801(b)(5)(A).

143. *Id.* § 1801(b)(5)(B). Whether the individual is in a public or private place does not matter in the determination. *Id.*

144. See H.R. REP. NO. 108-504, at 2-3 (2004) (discussing advances in miniaturization technology of cameras and ability to broadcast images across media such as the internet).

145. See *id.* Congress intended to protect "unsuspecting adults, high school students and children[.]" noting that video voyeurism has occurred in "high school locker rooms, department store dressing rooms, and even homes." *Id.* Congress further discussed the prevalence of voyeurism in public places, but limited its discussion to the highly intrusive methods of "upskirting" and "downblousing." *Id.* at 3.

146. There have not been any decisions interpreting the statute as it applies to the workplace.

147. See Labor Management Relations (Taft-Hartley) Act § 7, 29 U.S.C. § 157 (2000).

148. See *NLRB v. Assoc. Naval Architects, Inc.* 355 F.2d 788, 791 (4th Cir. 1966) (it was "the act of photographing itself that had the tendency in these circumstances to intimidate"); *NLRB v. Frick Co.*, 397 F.2d 956, 961 (3d Cir. 1968) (violated 8(a)(1) partly by talking photographs of the strikers); *Sunbelt Mfg., Inc.*, 308 N.L.R.B. 780, 789 (1992) (citing *Certaineed Corp.*, 282 N.L.R.B. 1101, 1114 (1987)) (finding the video taping activities of the company to violate 8(a)(1)).

149. See, e.g., *Colgate-Palmolive Co.*, 323 N.L.R.B. 515, 516 (1997) (requiring an employer to

employer must provide the opportunity to negotiate and bargain over their implementation.¹⁵⁰ Therefore, video surveillance is a “mandatory subject of [collective] bargaining,”¹⁵¹ and a union has the right to bargain over the installation and use of video surveillance cameras.¹⁵²

In *Colgate-Palmolive*,¹⁵³ a 1997 decision, the employer used monitoring to prevent theft and misconduct.¹⁵⁴ Employees caught engaging in such activities were to be disciplined and possibly discharged.¹⁵⁵ The Board compared the use of video surveillance to physical examinations, drug and alcohol testing, and polygraph testing, all of which are “mandatory subjects of bargaining.”¹⁵⁶ The Board reasoned that video surveillance was related to the “work environment” and “[was] not a managerial decision that lies at the core of entrepreneurial control.”¹⁵⁷ The installation of cameras was not “fundamental to the basic direction of the enterprise” and it also impinged “directly on employment security.”¹⁵⁸ In a subsequent 2003 decision, the Seventh Circuit agreed.¹⁵⁹

In the most recent decision, *Anheuser-Busch*,¹⁶⁰ the NLRB would not rescind the discipline of employees even though the employer had illegally and secretly installed hidden cameras.¹⁶¹ The Administrative Law Judge (“ALJ”) found that installation of hidden cameras, which monitor work areas, requires notice and the opportunity for bargaining.¹⁶² Furthermore, the area in dispute could indeed be called a “work area,” thus broadening the definition.¹⁶³

However, surprisingly, the judge did not revoke the discipline employees received from the employer even though it was based

bargain with a union over the installation and use of surveillance cameras); *Nat’l Steel Corp. v. NLRB*, 324 F.3d 928, 934-35 (7th Cir. 2003) (holding employer must provide union with information regarding surveillance cameras in order for union to carry out its representative obligations).

150. *Colgate-Palmolive Co.*, 323 N.L.R.B. at 515.

151. *Id.*

152. *Id.*

153. 323 N.L.R.B. at 515.

154. *Id.*

155. *Id.*

156. *Id.*

157. *Id.*

158. *Id.* (quoting *Ford Motor Co. v. NLRB*, 441 U.S. 488, 498 (1979)).

159. *Nat’l Steel Corp. v. NLRB*, 324 F.3d 928, 932 (7th Cir. 2003).

160. *Anheuser-Busch, Inc.*, 342 N.L.R.B. 560 (July 22, 2004).

161. *See id.* at 561.

162. *See id.* at 560 (citing *Nat’l Steel Corp. v. NLRB*, 324 F.3d 928 (2003)).

163. *See id.*

exclusively on evidence obtained by hidden cameras.¹⁶⁴ The dissenting judge argued that reinstatement and back pay of the employees, i.e. make-whole relief, is the only remedy that would truly restore the status quo, but the majority rejected this argument.¹⁶⁵ They reasoned that the remedy was inconsistent with the policies behind the Act and public policy in general because it would “reward parties who engaged in unprotected conduct.”¹⁶⁶

Although there appears to be more protection afforded union employees, the reality is that employers violating surveillance law are only given a slap on the wrist. As *Anheuser-Busch* demonstrates, the NLRB found the company violated federal labor law,¹⁶⁷ but this decision was, in essence, cold comfort to the employees who were discharged as a result of this violation.

This decision highlights the importance of proper remedies in any proposed future federal legislation concerning video surveillance. Not only must justice be served and the status quo restored, but penalties must also exist in order to provide incentives for employers to comply with the regulations. The proposed legislation at the conclusion of this note will serve both to punish and to deter.

IV. LACK OF STATUTORY PROTECTION AT THE STATE LEVEL

Another potential source of employee protection is state constitutional privacy provisions. Ten states have recognized a right to privacy.¹⁶⁸ However, only California has applied this right to private actors.¹⁶⁹ Since most state constitutions do not protect employee privacy, employees must instead rely on state statutory provisions when seeking a remedy. State legislatures have begun enacting laws but with limited success.

There are three broad categories of state statutes affording protection to employees.¹⁷⁰ The first category mirrors the Wiretapping

164. *Id.* at 561.

165. *Id.* at 561, 563 (Member Walsh dissenting).

166. *Id.* at 561.

167. *Id.* at 560.

168. ALA. CONST. art. I § 22; ARIZ. CONST. art. II § 8; CAL. CONST. art. I § 1; FLA. CONST. art. I §§ 12 & 23; HAW. CONST. art. I §§ 6 & 7; ILL. CONST. art. I §§ 6 & 12; LA. CONST. art. I § 5; MONT. CONST. art. II § 10; S.C. CONST. art. I § 10; WASH. CONST. art. I § 7.

169. *See Hill v. NCAA*, 865 P.2d 633, 644 (1994) (holding that the California state constitutional privacy provision “creates a right of action against private entities as well as government entities”).

170. *See, e.g., N.J. STAT. ANN. § 2A:156A-3* (West Supp. 2007); N.Y. LAB. LAW § 203-c

Act and provides only video with audio protection and no explicit protection from video only monitoring.¹⁷¹ The second category protects only the most intensely private employee actions from video surveillance.¹⁷² The third enacts only a notice requirement.¹⁷³ The first two categories of legislation, while evidencing legislatures' recognition of the need for increased protection, do not substantively expand workers' rights. The third category affords more protection by mandating notice, but still falls short. It gives employers a legal safety net to avoid litigation simply by posting a notice of surveillance, and it ignores employees' dignity rights.

Recently, the New York State legislature enacted a statute that provides, "[n]o employer may cause a video recording to be made of an employee in a restroom, locker room, or room designated by an employer for employees to change their clothes, unless authorized by court order."¹⁷⁴ Under this new law, both private and public sector employees are protected.¹⁷⁵ The statute creates a civil cause of action that allows employees to sue their employer for damages including attorneys' fees and costs as well as injunctive relief.¹⁷⁶

Like New York, Rhode Island and California prohibit making an audio or video recording of an employee in locker rooms and restrooms, and other areas employers designate for employees to change clothes.¹⁷⁷ The Rhode Island statute creates a civil action and allows courts to award damages and attorney's fees, and grant injunctive relief.¹⁷⁸ These statutes and others like it merely codify the common law;¹⁷⁹ they do not make any strides towards increased employee protection.¹⁸⁰

(McKinney Supp. 2008); CONN. GEN. STAT. ANN. § 31-48b (West 2003); DEL. CODE ANN. tit. 19, § 705 (2006); W. VA. CODE ANN. § 21-3-20 (LexisNexis 2002).

171. See, e.g., N.J. STAT. ANN. § 2A:156A-3; CONN. GEN. STAT. ANN. § 31-48b.

172. W. VA. CODE ANN. § 21-3-20(a). As interpreted by most courts, the most "intensely private" areas include places like restrooms and changing room stalls.

173. See, e.g., DEL. CODE ANN. tit. 19, § 705.

174. N.Y. LAB. LAW § 203-c(1) (McKinney Supp. 2008).

175. See *id.* § 203-c.

176. *Id.* § 203-c(3).

177. R.I. GEN. LAWS § 28-6.12-1(a) (Supp. 2007); CAL. LAB. CODE § 435(a) (West 2003).

178. R.I. GEN. LAWS § 28-6.12-1(c)(1)-(2).

179. Employees already have strong causes of action such as common law invasion of privacy, intentional infliction of emotional distress, and fourth amendment claims (for public actors) where employers engage in video surveillance in a restroom or other clearly private areas.

180. See R.I. GEN. LAWS § 28-6.12(a) (prohibiting video recording in locker rooms, restrooms and other rooms designated by employer as a clothes changing room); W. VA. CODE ANN. § 21-3-20(a) (LexisNexis 2002) (providing that employers cannot use any electronic surveillance systems in areas designated for health or comfort of employees or for safeguarding their possessions such as restrooms, showers, locker rooms, dressing rooms, and employee lounges).

The New Jersey Wiretapping and Electronic Surveillance Control Act¹⁸¹ (“WESCA”) and other similar state statutes, mirror the Federal Wiretapping Act and fail to prohibit the interception of images.

Connecticut law falls into the third category of statutes, requiring employers to give notice before engaging in electronic monitoring.¹⁸² Employers must conspicuously post a notice concerning the types of electronic monitoring in which they will engage.¹⁸³ “Electronic monitoring” is broadly defined by the statute as “the collection of information on an employer’s premises concerning employees’ activities or communications by any means other than direct observation, including the use of a computer, telephone, wire, radio, camera, electromagnetic, photo electronic or photo-optical systems.”¹⁸⁴ Prior written notice is not required when an employer has reasonable belief that an employee is engaged in conduct that creates a hostile work environment, violates the law, or infringes on employer or employees’ legal rights.¹⁸⁵

In addition to the notice statute, Connecticut has enacted a first category statute that regulates the use of electronic surveillance.¹⁸⁶ The statute prohibits use of electronic surveillance in areas used for employees’ personal comfort and health, and areas used to safeguard their possessions.¹⁸⁷ The statute also forbids an employer from overhearing or recording conversations and discussions related to the employment contract negotiations between parties.¹⁸⁸ Violators may be subject to civil penalties as well as imprisonment.¹⁸⁹

West Virginia’s statute is similar to Connecticut’s. The West Virginia statute prohibits an employer from operating an electronic surveillance system or device to record or monitor employees in areas employees use for health or comfort, or to safeguard their possessions.¹⁹⁰ There is no civil cause of action, but violators may be criminally liable for a misdemeanor offense and fined according to the number of

181. N.J. STAT. ANN. §§ 2A:156A-1 to -34 (West Supp. 2007).

182. CONN. GEN. STAT. ANN. § 31-48d(b)(1) (West 2003).

183. *Id.*

184. *Id.* § (a)(3).

185. *Id.* § 31-48d(b)(2).

186. *See id.* § 31-48b(b).

187. *Id.* Examples of such areas include restrooms, locker rooms, and lounges. *Id.*

188. *Id.* § 31-48b(d).

189. *Id.* § 31-48b(c), (e).

190. W. VA. CODE ANN. § 21-3-20(a) (LexisNexis 2002). For example restrooms, shower rooms, dressing rooms and employee lounges. *Id.*

previous offenses committed.¹⁹¹

Congress' inaction has lead to this patchwork of state laws which grant employees limited rights at best. While each type of statute is a positive step in the direction, none provides enough limitation on employers' otherwise unfettered abuse of this intrusive and invasive form of monitoring.

V. COMMON LAW PROVIDES REMEDIES IN ONLY THE MOST EGREGIOUS CASES

In a Harvard Law Review article published in 1890, Louis Brandeis and his law partner Samuel Warren first proposed a new tort action for the invasion of privacy.¹⁹² They wrote primarily to propose new remedies for the abuses of print media.¹⁹³ Their article was influential in convincing the states to recognize privacy-based torts.¹⁹⁴ The U.S. Supreme Court later articulated that the right to privacy was "the right to be let alone."¹⁹⁵ However, it wasn't until 1960 that William Prosser formulated four basic theories under which employees could file a common law invasion of privacy tort claim against employers who engage in unconsented monitoring of electronic communications.¹⁹⁶

There are four basic common law invasion of privacy torts that have been recognized by most jurisdictions: (1) unreasonable intrusion upon the seclusion of another; (2) misappropriation or exploitation of a person's name or likeness; (3) public disclosure of private facts; and (4) depiction of a person in a false light.¹⁹⁷ However, these privacy torts have yet to punish and deter unreasonable surveillance of employees in the private workplace. In New York, for example, courts have declined to recognize a common law right to privacy altogether.¹⁹⁸ The New

191. *Id.* § 21-3-20(b). Fines range from \$500 dollars to \$2,000 dollars. *Id.*

192. Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196-97 (1890).

193. *See id.* at 197.

194. E. Leonard Rubin, *Rights of Publicity and Entertainment Licensing*, in UNDERSTANDING THE INTELLECTUAL PROPERTY LICENSE 2006, at 261, 265 (PLI Patents, Copyrights, Trademarks, and Literary Prop. Course Handbook Series No. 9070, 2006).

195. *Katz v. United States*, 389 U.S. 347, 350 (1967) (footnote omitted).

196. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960); W. PAGE KEETON ET. AL., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 851 (West Group 5th ed. 1984) (1941).

197. *See* RESTATEMENT (SECOND) OF TORTS § 652A (1977).

198. *See, e.g., Hurwitz v. United States*, 884 F.2d 684, 685 (2d Cir. 1989) (stating "[n]o so-called common law right of privacy exists in New York"); *Cohen v. Hallmark Cards, Inc.*, 382 N.E.2d 1145, 1146 n. 2 (N.Y. 1978) (stating "[i]n New York, there exists no so-called common-law right to privacy").

York Court of Appeals stated, “[w]e have in the past recognized that, in this State, there is no common-law right of privacy and the only available remedy is that created by Civil Rights Law §§ 50 and 51.”¹⁹⁹ Instead, some plaintiff employees attempt to bring their cases under a defamation theory.²⁰⁰ However, this theory is concerned with publication rather than monitoring of electronic communication.

In the employment context, the unreasonable intrusion upon the seclusion of another tort proves most relevant because it is associated with either: a physical intrusion into a place in which the plaintiff has secluded his or herself; the use of the defendant’s senses, with or without mechanical aids, (e.g., wiretaps, microphones, or just plain spying) to oversee or overhear the plaintiff’s private affairs; or some other form of investigation or examination into the plaintiff’s private concerns, such as opening his or her private and personal mail.²⁰¹ Unlike the other common law causes of action, this tort is based on the psychological distress caused by the intrusion itself and therefore it is not necessary that the wrongdoer (i.e., employer) learn anything embarrassing or private about the person harmed or that the employer wrongfully disclose that information.²⁰² Although this right is recognized by most jurisdictions, courts rarely find for employees who assert employers invaded their right to privacy through electronic monitoring.

When courts have considered claims in the workplace, they have generally found for the plaintiffs only if the challenged intrusions involved information or activities of a highly intimate nature. Where the intrusions have merely involved unwanted access to data or activities related to the workplace, however, claims of intrusion have failed.²⁰³

199. *Freihofer v. Hearst Corp.*, 480 N.E.2d 349, 353 (N.Y. 1985). Civil Rights Law section 50 protects an employee’s right to privacy if the employer uses, for advertising purpose or for trade, the “name, portrait, or picture of any living person without having first obtained written consent of such person.” N.Y. CIV. RIGHTS LAW § 50 (McKinney 2002). It also classifies a violation of this section as a misdemeanor. *Id.* Civil Rights Law section 51 grants the employee a cause of action for injunction and damages. N.Y. CIV. RIGHTS LAW § 51 (McKinney Supp. 2008).

200. An employee may bring a claim for defamation if an employer has, without an applicable privilege, communicated something false and defamatory about an employee. If the statement is true the employer has an absolute defense. *See* John B. Lewis, *I Know What You E-Mailed Last Summer*, SECURITY MGM’T, Jan. 2002, (citing *Lian v. Sedgwick James of N.Y., Inc.*, 992 F. Supp. 644, 649 (S.D.N.Y. 1998)).

201. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

202. *See id.* § 652B cmt. a & cmt. b.

203. *Med. Lab. Mgt. Consultants v. Am. Broad. Co., Inc.*, 30 F. Supp. 2d 1182, 1188 (D. Or. 1998) (citing *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611, 621 (3d Cir.1992); *Doe v. Kohn Nast*

This is because in a majority of jurisdictions, to succeed on an intrusion upon seclusion claim, the plaintiff has the burden of proving that (1) there was an intrusion,²⁰⁴ (2) the intrusion was intentional,²⁰⁵ (3) the plaintiff had a reasonable expectation of privacy in the matter intruded upon,²⁰⁶ and (4) the intrusion was “highly offensive to a reasonable person.”²⁰⁷ Even if the employee succeeds in proving all the elements, she may still lose if the employer had a legitimate business reason for the intrusion that outweighs the employee’s privacy interest.²⁰⁸

It is extremely difficult for an employee to succeed on an intrusion claim in all but the most egregious circumstances. Many plaintiffs lose because they have not carried their burden of showing an intrusion in the first place.²⁰⁹ Courts generally find the employer’s actions do not rise to the requisite level of intrusion unless they have videotaped employees while they were undressed.²¹⁰ Even if the employee is able to prove an intrusion existed, she must then prove the invasion was intentional.²¹¹

& Graf, P.C., 862 F. Supp. 1310, 1326 (E.D. Pa. 1994)); *Smith v. Col. Interstate Gas Co.*, 777 F. Supp. 854, 857 (D. Colo.1991)).

204. *Harkey v. Abate*, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (stating that a “necessary element of this type of invasion of privacy is, of course, that there be an ‘intrusion’”).

205. *See Peavy v. Harman*, 37 F. Supp. 2d 495, 521 (N.D. Tex. 1998), *rev’d in part on other grounds sub nom.*, *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158 (5th Cir. 2000) (finding that defendant’s subjective belief as to the legality of eavesdropping with a police scanner was irrelevant to the satisfaction of the element of intent and that “plaintiffs need only prove that the [defendants] desired the consequences of their actions or reasonably believed that such consequences were likely to result therefrom”).

206. *Med. Lab.*, 30 F. Supp. 2d at 1188 (D. Ariz. 1998) (citations omitted) (“[A] plaintiff can recover ‘only if he had an objectively reasonable expectation of seclusion or solitude in the place, conversation, or data source’”).

207. *Id.* at 1189 (quoting RESTATEMENT (SECOND) OF TORTS § 652B (1977)) (“[T]he intrusion must be found to be ‘highly offensive to a reasonable person’”).

208. *See Smyth v. Pillsbury Co.*, 914 F. Supp. 97, 101 (E.D. Pa. 1996) (“[T]he company’s interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.”).

209. *See Reuber v. Food Chem. News, Inc.*, 925 F.2d 703, 718-19 (4th Cir. 1991) (citing *The Florida Star v. B.J.F.*, 491 U.S. 524, 533 (1989)) (“The intrusion prong of invasion of privacy requires a positive act by a defendant . . . that encroaches on a plaintiff’s seclusion”).

210. *See Doe v. B.P.S. Guard Servs., Inc.*, 945 F.2d 1422, 1423 1427 (8th Cir. 1991) (holding security guard firm liable for invasion of privacy because the guards videotaped models while they were changing in a dressing area at a fashion show); *Speer v. Dep’t of Rehab. & Corr.*, 646 N.E.2d 273, 274 (Ohio Ct. Cl. 1994) (monitoring of employees in area within the workplace generally considered private, such as restroom, constitutes an actionable invasion of privacy); *Harkey v. Abate*, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (finding that the installation of hidden viewing devices alone constitutes an interference of privacy and that absence of proof that the devices were utilized, though relevant to the question of damages, is not fatal to the plaintiff’s case).

211. RESTATEMENT (SECOND) OF TORTS § 652B.

While some jurisdictions have found that an unintentional intrusion—one which was thought to be legitimate by the intruding party—may destroy a cause of action for “intrusion on seclusion,”²¹² others have allowed the suit to proceed.²¹³

The most contested issue is determining what constitutes an objectively reasonable expectation of privacy. The general rule is there is no objective reasonable expectation of privacy in public.²¹⁴ Furthermore, there is no expectation of privacy in the workplace. Courts are usually not receptive to employees’ claims that their work environments contain sufficiently private spaces where they may not be monitored.²¹⁵ Some employees have tried to overcome this rule by proving that the employers have carved out exceptions by leading the employees to believe that they had an expectation of privacy in certain instances.²¹⁶

Lastly, courts evaluate whether the intrusion would be highly offensive to a reasonable person.²¹⁷ Most courts interpret this as requiring a balancing test between the employer’s interests in intruding and the employee’s privacy interest.²¹⁸ A plaintiff can recover “only if the plaintiff had an objectively reasonable expectation of seclusion or

212. See *Smyth*, 914 F. Supp. at 100-01 (holding that, although the employee had been told that the e-mails could not be intercepted or used against the employee, the employee exhibited no expectation of privacy in the message because the employee had voluntarily made an e-mail communication to his supervisor).

213. See, e.g., *Acuff v. IBP, Inc.*, 77 F. Supp. 2d 914, 924 (C.D. Ill. 1999) (citing *W. PAGE KEETON ET. AL., PROSSER AND KEETON ON THE LAW OF TORTS* § 8, at 29 (5th ed. 1984)) (holding that the requisite intent was present because the employer “was on notice that examinations and/or medical treatments were taking place” in the video-taped room and the employer “had in mind a belief or knowledge that consequences other than catching an alleged thief were substantially certain to result from the videotaping”).

214. See *Salazar v. Golden State Warriors*, No. C-99-4825 CRB, 2000 U.S. Dist LEXIS 2366, at *5-6 (N.D. Cal. Mar. 3, 2000) (noting that a public place cannot be distinguished from a private place based on the amount of traffic or light); *Fayard v. Guardsmark, Inc.*, No. 89-0108, 1989 U.S. Dist. LEXIS 14211, at *6 (E.D. La. Nov. 29, 1989) (holding that the surveillance of “activities in the public view” is not enough to support a cause of action).

215. See *Cox v. Hatch*, 761 P.2d 556, 564 (Utah 1988) (finding no reasonable expectation of privacy in a “common workplace”); *Marrs v. Marriott Corp.*, 830 F. Supp. 274, 283 (D. Md. 1992) (holding that where an employee was videotaped picking a lock on a desk drawer, the employee had no reasonable expectation of privacy because it was in an “open office”).

216. See *Smyth*, 914 F. Supp. at 101 (holding that, although the employee had been told that the e-mails could not be intercepted or used against the employee, the employee exhibited no expectation of privacy in the message because the employee had voluntarily made an e-mail communication to his supervisor).

217. *Johnson v. Allen*, 613 S.E.2d 657, 660 (Ga. App. 2005).

218. See *id.*

solitude in the place.”²¹⁹

Another available common law cause of action is intentional infliction of emotional distress.²²⁰ This action is also premised on privacy. Plaintiffs may claim that the intrusion into one’s privacy created emotional distress.²²¹ To establish a claim of intentional infliction of emotional distress, a plaintiff must prove (1) intentional or reckless conduct, (2) which is extreme and outrageous, (3) a causal connection between the wrongful conduct and the emotional distress, and (4) severe emotional distress.²²² This cause of action’s roadblock is that the conduct must be so extreme and outrageous that it goes beyond all “bounds of decency, and to be regarded as atrocious, and utterly intolerable in a civilized community.”²²³ The surveillance of the female restroom in *Johnson* was egregious enough to survive defendant’s motion for summary judgment²²⁴ but the general surveillance in *Clark* was not.²²⁵

American employees have no meaningful constitutional, common law, or statutory protection from employers’ abuse of video monitoring. Even a restroom may not be a sanctuary protected by privacy law.²²⁶ This void in the law “accords the employer near plenary power to govern the workplace; in fact to govern the worker.”²²⁷

VI. COMPARATIVE LAW: AN INTERNATIONAL PERSPECTIVE

“Americans reflexively dismiss Europe as a clapped-out old

219. *Shulman v. Group W. Prod.*, 955 P.2d 469, 490 (Cal. 1998).

220. *Johnson*, 613 S.E.2d at 659 (Ga. App. 2005) (employer used video surveillance in female restroom for three years to combat suspected drug use); *Clark v. Elam Sand & Gravel, Inc.*, 777 N.Y.S.2d 624, 625 (N.Y. Sup. Ct. 2004) (employer used general video surveillance in the workplace without giving notice to employee).

221. See *Johnson*, 613 S.E.2d at 661.

222. *Id.*

223. *Clark*, 777 N.Y.S.2d at 625 (citations omitted); *Johnson*, 613 S.E.2d at 661.

224. *Johnson*, 613 S.E.2d at 661.

225. *Clark*, 777 N.Y.S.2d at 626.

226. *Johnson*, 613 S.E.2d at 660. (citing *In re C.P.*, 555 S.E.2d 426 (Ga. 2001)) (no privacy in a public restroom when restroom is used in a way other than its intended purpose).

227. Matthew W. Finkin, *Menschenbild: The Conception of the Employee as a Person in Western Law*, 23 COMP. LAB. L. & POL’Y J. 577, 577 (2002); see also RESTATEMENT (SECOND) OF TORTS § 652B cmt. a (1977) (stating that intrusion on seclusion “does not depend upon any publicity given to the person whose interest is invaded or to his affairs”); see also *Med. Lab. Mgmt. Consultants v. Am. Broad. Co., Inc.*, 30 F. Supp. 2d 1182, 1191 (D. Ariz. 1998) (noting that “[t]he basis of the tort [of intrusion] is not publication or publicity. Rather the core of this tort is the offensive prying into the private domain of another.” (quoting *Russell v. ABC*, No. 94C5768, 1995 U.S. Dist LEXIS 7528, 1995 WL 330920, at *21 (D. Ill. May 31, 1995))).

continent—a wonderful place to visit but hardly the anvil of the future. Europeans, equally reflexively, dismiss America as the embodiment of all the evils of modernity—a testosterone-driven adolescent bereft of history and tradition.”²²⁸ Part I.A. introduced the dignity concept adopted by many foreign nations, especially in Continental Europe.²²⁹ These countries do not idly proclaim their respect for workers; many countries have enacted legislation to actively protect their workforce.²³⁰ We recognize America’s sovereignty and distinct value system, however, it is useful to examine the protections afforded citizens in foreign countries because, in the increasingly borderless global economy, the United States is at risk of losing its competitive edge if it fails to harmonize with the rest of the world.²³¹

New South Wales, Australia passed the Workplace Video Surveillance Act of 1998.²³² The Act prohibits only covert video surveillance of employees.²³³ Overt surveillance is not prohibited, but the statutory definition of covert surveillance includes what could be considered overt by laypersons.²³⁴ Covert surveillance may be used when the surveillance’s purpose is not to monitor employees acting in their capacity as employees.²³⁵ Employers may seek a Magistrate’s order to use covert surveillance with the belief that employees are engaged in illegal activities.²³⁶ Violations may result in criminal

228. *Old America v. New Europe*, THE ECONOMIST, Feb. 22, 2003, at 32.

229. See *supra* Section I. A.

230. French law even extended to taping of a “Big Brother” reality television episode. Christophe Vigneau, *Information Technology and Worker’s Privacy: The French Law*, 23 COMP. LAB. L. & POL’Y J. 351, 351 n.1 (2005). Producers were required to allow participants private time off camera. *Id.*; see *supra* note 1 and accompanying text (discussing reality television).

231. Cf. Judson MacLaury, *Government Regulation of Workers’ Safety and Health, 1877-1977*, <http://www.dol.gov/oasam/programs/history/mono-regsafepart06.htm> (last visited July 13, 2008) (discussing the history of worker’s compensation legislation in the United States). Germany paved the way in providing protection to its workforce by adopting a worker’s compensation system in 1884. *Id.* While other European countries followed the lead of Germany, America continued to force its workers to rely on existing common law actions that made it hard for worker’s to prove employer fault. *Id.* At first, legislators enacted statutes making it easier for employees to recover, but the result was disastrous liabilities for employers forcing them to take out expensive liability insurance. *Id.* In the early 1900’s, some states such as Maryland, began enacting their own worker’s compensation systems. *Id.* It wasn’t until 1921 that worker’s compensation gained widespread support and was adopted by forty six jurisdictions, nearly forty years after Germany first enacted its worker’s compensation laws. *Id.*

232. See Privacy NSW, *Guide to the Workplace Video Surveillance Act* at 1, 5 (Feb. 2002), available at <http://www.privacy.org.au/Papers/workvideo2002.pdf>.

233. *Id.* at 2. The act does not prohibit surveillance of independent contractors. *Id.*

234. See *id.*

235. For example when video surveillance is used for security purposes. *Id.*

236. *Id.* at 3. When such an order is obtained, the employer may only use the surveillance for

prosecution by the government.²³⁷ Employees' sole remedy is to report the violation to the police because the Act does not create a civil cause of action.²³⁸

Canada enacted the Personal Information Protection and Electronic Documents Act of Canada²³⁹ ("PIPEDA"). The statute's purpose is to regulate the collection of information regarding an "identifiable individual."²⁴⁰ The Act recognizes the expanding use of technology and a person's right to privacy.²⁴¹ Video surveillance is not explicitly prohibited.

In 2002, Canadian Pacific Railway employees brought a complaint to the Canadian Privacy Commissioner under PIPEDA after the railway installed six video cameras in its maintenance yard without giving the employees notice.²⁴² The employees claimed "this system could be used for monitoring the conduct and work performance of workers and that would be an *affront to human dignity*."²⁴³

PIPEDA allows an organization to collect information where a reasonable person would consider it appropriate under the circumstances.²⁴⁴ The Privacy Commissioner established a four prong test to determine whether the surveillance was reasonable: 1) does the measure fulfill a specific need, 2) the probability the measure will be effective in meeting the need, 3) the proportionality of the loss of privacy to the gained benefit, and 4) the availability of a less intrusive method to achieve the goals.²⁴⁵

The Commissioner found that although there were some incidents of vandalism, the railroad had not demonstrated a "real and specific" harm.²⁴⁶ He noted the lack of statistical evidence to show the cameras' effectiveness in deterring criminals; he suggested that posted notices of

the purpose specified in the order. *Id.* It may not use the surveillance for general monitoring of the employee such as to determine whether the employee is present or tardy for work. *See id.*

237. *Id.* at 4.

238. *Id.*

239. Personal Information Protection and Electronics Documents Act ("PIPEDA"), 2000 S.C., ch. 5 (Can.).

240. *See Eastmond v. Canadian Pac. Ry.*, [2004] F.C. 852, ¶ 7 (Can.).

241. *Id.* ¶ 26 (*citing* PIPEDA).

242. *Id.* ¶¶ 1-2 (the railroad claimed the cameras were necessary for security purposes).

243. *Id.* ¶ 2 (*emphasis added*). The complaint also alleged that a security problem did not exist, the surveillance was done in secret without the consultation of the union, and it would adversely affect workers' morale. *Id.*

244. PIPEDA, 2000 S.C., ch. 5, div.1(5)(3) (Can.).

245. *Eastmond*, [2004] F.C. 852, ¶ 13.

246. *Id.* ¶ 14.

surveillance may be just as effective without actually using cameras.²⁴⁷ Additionally, there was no evidence the railroad tried utilizing alternatives to video surveillance, such as better lighting.²⁴⁸ Finally, regarding the loss of privacy, the Commissioner stated:

While I acknowledge that the system provides a poor picture resolution and the cameras are not trained on areas where there is a reasonable expectation of privacy, it may nevertheless be possible to identify an individual during the day . . . I am concerned that the mere presence of these video cameras has given rise to the perception among employees that their comings and goings are being watched, whether or not that is actually the case, and that the adverse psychological effects of a perceived privacy invasion may be occurring.²⁴⁹

After weighing the factors, the Commissioner decided the surveillance was not reasonable and violated PIPEDA.²⁵⁰

The Canadian court adopted the Commissioner's test.²⁵¹ The court noted that an employee does not shed his expectation of privacy simply by entering into an employment relationship, but also acknowledged the employer's rights regarding business and property interests.²⁵² In further discussing the importance of balancing the parties' interests, the court opined that worker surveillance may contribute to a "diminution of one's sense of personal dignity or privacy."²⁵³ Although the court ultimately held that the surveillance was not unreasonable, the factors considered by the court highlight the difference in the way American courts and other courts view video surveillance.²⁵⁴

French courts have also held that employees enjoy a right to have the intimacy of their private life protected while in the workplace.²⁵⁵ Like the Canadian court, the French court balanced the employees' right of privacy against the employer's right of control.²⁵⁶ The court used the European Convention on Human Rights and the French Civil Code as

247. *Id.*

248. *Id.*

249. *Id.*

250. *Id.* ¶ 15.

251. *See id.* ¶ 126-27.

252. *Id.* ¶ 159.

253. *Id.*

254. *Compare id.* ¶ 177, with *Vega-Rodriguez v. P.R. Tel. Co.*, 110 F.3d 174, 180-81 (1st Cir. 1997) (court only looked at employees' objective and subjective expectation of privacy, as opposed to the reasonableness of the employer's surveillance).

255. *Vigneau*, *supra* note 230, at 355.

256. *Id.* at 355-56.

guidelines in reaching a decision.²⁵⁷

The Italian legislature has specifically recognized its workforce's dignity. As early as 1970, the legislature enacted legislation to protect workers.²⁵⁸ Title I of the statute is entitled "The Freedom and Dignity of the Employee."²⁵⁹ Article 4 of the Worker's Statute addresses video surveillance.²⁶⁰ The statute's language declares that video surveillance is a direct assault on workers' human dignity.²⁶¹ Furthermore, the act forbids any form of remote video surveillance of employees.²⁶²

The European Union has also recognized the importance of employees' privacy rights. Directive 95/46/EC protects the "fundamental rights and freedoms of natural persons."²⁶³ The directive applies to the processing of personal data.²⁶⁴ It leaves precise implementation to the member states and does not explicitly prohibit video surveillance.²⁶⁵ However, in its recitals, the directive states that image data (e.g. video surveillance) that is used for "public security, defence [sic], national security" or otherwise used for State activities such as criminal investigations are not within the scope of the directive.²⁶⁶ Member states must provide judicial remedies to persons whose rights have been breached.²⁶⁷

VII. LEGISLATIVE PROPOSALS

A. Federal Proposals

Since 1993, there have been three legislative proposals introduced in the United States Congress addressing workplace surveillance.²⁶⁸ None has passed and most are inadequate. Senator Simon (D-Ill.)

257. *Id.* at 355.

258. Claudia Faleri, *Information Technology and Worker's Privacy: The Italian Law*, 23 COMP. LAB. L. & POL'Y J. 399, 400 (2005). The Worker's Statute, Law 300/70, imposed restrictions on management but did not create any rights for individual employees. *Id.*

259. *Id.* at 401.

260. *Id.*

261. *Id.*

262. *See id.*

263. Council Directive 95/46, art. 1, 1995 O.J. (L 281) 1 (EC).

264. *Id.* art. 3.

265. *Id.* arts. 1-34.

266. *Id.* pmbl. ¶ 16.

267. *Id.* art. 22.

268. *See infra* notes 275, 285, 292.

proposed the most comprehensive bill in 1993.²⁶⁹ He noted that the United States has supported laws that protect its neighbors and government from spying on the nation, and lack of laws protecting its citizens from being spied on in the workplace.²⁷⁰ He also suggested that monitoring is a “de facto” form of discrimination because women are more commonly employed in the types of jobs that are monitored.²⁷¹

The Privacy for Consumers and Workers Act (“PCWA”) regulates electronic monitoring in the workplace, including video surveillance.²⁷² It requires that employers give notice to employees of monitoring practices.²⁷³ Specifically, employers must advise employees as to the types of monitoring used, when the monitoring will occur, a description of the monitoring, how the information collected will be used, and whether there are any exceptions to the notice requirement.²⁷⁴ Employers must also advise potential employees during the interview process of any electronic monitoring to be used during employment.²⁷⁵ The Secretary of Labor must provide a notice regarding employee rights under the Act to employers, which employers must post.²⁷⁶ The bill allows employers to monitor without notice when they have a “reasonable suspicion” that an employee is engaged in, or about to be engaged in, misconduct that either violates criminal or civil laws, constitutes willful gross misconduct, or will severely, adversely impact the employer’s business.²⁷⁷

The bill also regulates the amount of monitoring an employer may engage in and establishes limitations on what the employer may do with the information gathered.²⁷⁸ It provides a tiered system based on length of service on the amount of random monitoring an employer may use.²⁷⁹ The Act completely prohibits any monitoring in “private areas” defined as bathrooms, locker rooms, and dressing rooms.²⁸⁰

While the PCWA is the most comprehensive plan, it needs

269. 139 Cong. Rec. 10,354-55 (1993) (statement of Sen. Simon).

270. *Id.*

271. *Id.* For example, clerical positions and phone operators. *Id.*

272. *Id.* at 10,355.

273. *Id.* at 10,356.

274. *Id.*

275. *Id.*

276. *Id.*

277. *Id.* Prior to commencing the monitoring, the employer must sign a written statement declaring its compliance with the statute and describing the suspicious conduct. *Id.* The statement must be kept for three years. *Id.*

278. *Id.* at 10,356-57.

279. *See id.* at 10,356.

280. *Id.* at 10,357.

improvement. The distinctions between continuous and random monitoring are confusing. Rules must be straightforward and easily interpreted. The prohibition against random monitoring of employees with more than five years of service²⁸¹ is unfair to employers. Management must ensure their newest employees are doing work properly, but it is also important to ensure that older employees haven't fallen into bad habits. The list of excluded areas is a good start, but should be expanded to break rooms and lunch rooms. Surveillance of prohibited areas should not be left to the employer's discretion to act when there is reasonable suspicion. If criminal behavior is suspected, the police must be contacted to conduct a proper investigation.

The Notice of Electronic Monitoring Act ("NEMA") was introduced by Representative Charles Canady (R-FL) and the Senate's version was introduced by Senator Charles Schumer (D-NY) in 2000.²⁸² NEMA would have established a private right of action against employers who failed to give notice of wire or network monitoring.²⁸³ It does not prohibit monitoring and only requires employers give notice.²⁸⁴ There are exceptions to the notice requirement when an employer reasonably suspects misconduct.²⁸⁵ Senior Staff Counsel, James X. Dempsey, testified on behalf of the Center for Democracy and Technology generally supporting NEMA.²⁸⁶ However, he voiced concern about one "oversight in the drafting" dealing with the use of hidden video cameras in the workplace.²⁸⁷

As the bill is currently drafted, it does not cover video cameras that do not pick up sound. Yet there have been some truly egregious cases of employers using hidden cameras to secretly spy on their employees. Consider the following cases from the ACLU's web site: A few years ago, postal workers in New York City were horrified to discover that management had installed video cameras in the restroom stalls. Female workers at a large Northeastern department store discovered a hidden video camera installed in an empty office space that was commonly

281. *Id.*

282. See H.R. 4908, 106th Cong. (2d Sess. 2000) (introduced by Congressman Canady); 146 CONG. REC. S15,685 (2000) (Senate version of NEMA introduced by Senator Schumer).

283. See H.R. 4908 § 2711(a)(1).

284. *Id.* § (a)-(b).

285. *Id.* § (c)(1)-(2).

286. Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 5018, H.R. 4987, and H.R. 4908 Before the Subcomm. on the Constitution of the Comm. on the Judiciary, 106th Cong. 49, 50 (2000).

287. *Id.* at 57 (statement of James X. Dempsey).

used as a changing room. Waiters in a large Boston hotel were secretly videotaped dressing and undressing in their locker room.²⁸⁸

While this proposal is a step in the right direction, its failure to include video surveillance is a mistake. Senator Schumer acknowledged that electronic surveillance is destroying employees' privacy in the workplace.²⁸⁹ Unfortunately, Senator Schumer did not recognize the dignity and privacy concerns raised by video surveillance, specifically.

Congressman Thomas Petri (R-WI) introduced the Employee Changing Room Privacy Act, in February, 2005.²⁹⁰ Congressman Petri recognized several instances of inappropriate surveillance, including Gail Nelson's case.²⁹¹ The legislation prohibits employer's audio and video monitoring of employees in dressing rooms, restrooms, or any other area where the employer may reasonably expect employees to change clothes.²⁹² The bill creates a private cause of action for aggrieved employees.²⁹³

Additionally, the bill allows for enforcement actions led by the Secretary of Labor against employers who violate the prohibition against video or audio monitoring.²⁹⁴ Employers are entitled to a hearing and the Secretary of Labor may adjust the penalty based on several factors including the fine's effect on the employer's business and the circumstances surrounding the violation.²⁹⁵ The Secretary may also obtain an injunction by bringing a civil suit.²⁹⁶

This proposal is an encouraging development. However, Congress has not taken any further action on the bill since its referral to the House Subcommittee on Workforce Protections in March 2005.²⁹⁷ The bill restricts monitoring of restrooms and dressing rooms, but then incorporates the weakness of an expectation test for protection of other areas employees may use to change. Case law has proven that the

288. *Id.* (statement of James X. Dempsey) (citing ACLU, *Privacy in America: Electronic Monitoring*, ACLU, Oct. 22, 2003, <http://www.aclu.org/privacy/workplace/15646res20031022.html>).

289. 146 CONG. REC. S15,632 (2000).

290. H.R. 582, 109th Cong. (2005); 151 CONG. REC. E152 (daily ed. Feb. 2, 2005) (statement of Rep. Petri).

291. Compare 151 CONG. REC. at E153, with *supra* text accompanying notes 4-11.

292. H.R. 582 § 2; 151 CONG. REC. at E152.

293. H.R. 582 § 4(a).

294. *Id.* § 3(b).

295. *Id.* § 3(b), (c)(1)-(2).

296. *Id.* § 3(h).

297. See Thomas: Library of Congress, H.R. 582, <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR00582:@@L&summ2=m&> (last visited Oct. 15, 2008).

reasonable expectation of privacy test is not an adequate protection for employees. Congress needs to define a clear right that employers can rely on as opposed to limiting the extent to which employers can monitor.

The first federal privacy-enhancing bill was proposed over a decade ago in response to a gap in the law.²⁹⁸ Unfortunately there is still no express protection afforded to employees when it comes to video surveillance, which is arguably the most invasive and personal of all monitoring practices.

B. Private proposals

Several private organizations that defend workers' rights have recommended electronic monitoring statutes. The American Civil Liberties Union ("ACLU") believes that electronic surveillance, including video surveillance, is a major threat to employees' right to privacy and urges its members to encourage their legislators to adopt its "Model Statute on Electronic Monitoring."²⁹⁹ Their "Model Statute" includes a notice requirement to all employees and applicants, a restriction of monitoring of locker rooms, restrooms, and lounges, and prohibition of monitoring used for disciplinary action or performance evaluations.³⁰⁰

The ACLU's proposal is useful as a general guideline but it does not offer specifics. It also encompasses all forms of electronic monitoring and is not limited to video surveillance. The proposal creates many rights for the employee and does little to protect the rights of the employer. Additionally, the model statute does not provide any guidance regarding remedies or enforcement.

In addition to the model statute, the ACLU proposed a "Fair Electronic Monitoring Policy."³⁰¹ It includes the same essential components of the model statute such as the notice requirement and prohibition of monitoring of "areas designed for the health or comfort of employees."³⁰²

298. Privacy for Consumers and Workers Act, S. 984, 103d Cong. (1993); 130 CONG. REC. 10,354 (1993).

299. ACLU, *Through the Keyhole: Privacy in the Workplace, an Endangered Right*, ACLU, July 26, 1998, <http://www.aclu.org/privacy/workplace/15648res19980726.html>.

300. *Id.*

301. ACLU, *Privacy in America: Electronic Monitoring*, ACLU, Oct. 22, 2003, <http://www.aclu.org/privacy/workplace/15646res20031022.html>.

302. *Id.*

In a 2004 article, the National Workrights Institute (“NWI”) proposed the “Workplace Privacy Act” (“WPA”).³⁰³ The Act is both comprehensive and fair in addressing all forms of monitoring except video. The WPA generally allows workplace monitoring by employers when it is done on the employer’s premises, when it is done in the “normal course of employment,” when the employee is engaged in activity related to the performance of his duties, or when done in the interests of protecting the employer’s property.³⁰⁴ The section does not regulate video surveillance. Video is only regulated by section 2(e) which prohibits video and audio monitoring in bathrooms, dressing rooms, locker rooms, and “other areas” employees use to change clothes.³⁰⁵ The Act provides for an exception when the employer has received a court order to use video.³⁰⁶

The NWI’s proposal is almost a model proposal; however, it does not adequately regulate video surveillance. With the exception of establishing prohibitions to places in the workplace where an employer may use video surveillance, it does not regulate video in any other way. The proposal is vague as to whether video is permissible in other areas of the workplace and whether an employer must provide notice of video monitoring.

C. Our Proposal: Workplace Dignity and Security Act

Attempts to address video surveillance intrusions into privacy in the workplace have been largely ad hoc and have produced a regulatory maze that provides little protection to employees. New technological advances have made video surveillance cheaper and more effective than ever. The effects of globalization mandate that American law keep pace with the laws of other nations. Our proposal will take into account the strengths and weaknesses of previous attempts and incorporate both employer and employee interests.

The Workplace Dignity and Security Act³⁰⁷ attempts to balance the employers’ needs to maintain a secure and safe workplace against the employees’ needs to work in a respectful and dignified environment.³⁰⁸

303. NATIONAL WORKRIGHTS INST., PRIVACY UNDER SIEGE: ELECTRONIC MONITORING IN THE WORKPLACE 20-22 (2004), http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf.

304. *Id.* at 20 (§ 2(a)(1)(A)-(B) of proposed “Workplace Privacy Act” (“WPA”).

305. *Id.* at 21 (§ 2(e)(1) of proposed WPA).

306. *Id.* at 21 (§ 2(e)(1)(A) of proposed WPA).

307. Offered as an amendment to Title 29 U.S.C.

308. *Cf. Eastmond v. Canadian Pac. Ry.*, 2004 F.C. 1842 ¶ 13 (Can.) (Canadian court decision

It establishes areas that are completely protected against surveillance so employees have a safe haven. It provides for areas of the workplace that may be monitored with just cause and with appropriate notice to employees. It is not the role of an employer to catch criminals; therefore, it provides that suspected criminal activity must be reported to proper law enforcement. It allows the Secretary of Labor to bring a criminal proceeding and also creates a private cause of action so employees may enforce their rights. It limits employers' liability by capping statutory damages and by allowing employers to obtain a "Permissive Use Permit," which would provide a safe haven against liability if its terms are adhered to.

The Workplace Dignity and Security Act

a) Employees have a right to be free from video surveillance used by employers in a way that does not conform to the purpose of this Act.

b) Absolute prohibitions: Employers may not use video camera surveillance in any restroom, lunch room, break room, dressing room, changing room, or any other area designated by an employer as an area employees may use to undress or otherwise utilize during breaks.

c) General prohibition: Employers may not use video camera surveillance in the workplace except for a legitimate business purpose when there are no suitable alternatives available.

1) Employee performance is never a legitimate business purpose.

2) Suspicion of criminal activity is never a legitimate business purpose. Prevention of criminal activity may be a legitimate business purpose. Employers suspecting criminal activity must contact law enforcement.

3) Where an employer uses video camera surveillance to generally monitor a workspace, there will be a presumption against a legitimate use. Where an employer uses video camera surveillance

utilizing four part balancing test).

to monitor hallways and exits or entrances, there will be a presumption in favor of legitimate use.

4) Employers approved by the Secretary of Labor for a Permissive Use Permit may use video surveillance in accordance with the Permit.

d) Notice: Any employer engaging in video camera surveillance in accordance with section (b) shall post notice in a conspicuous place in the workplace and provide all potential employees with a copy of the notice prior to the commencement of employment.

1) Notice must provide what areas are monitored and at what times.

2) Employers shall also post a notice of employees' rights under the Act as provided by the Secretary of Labor.

e) Permissive Use Permit: Any employer may apply to the Department of Labor for a Permissive Use Permit.

1) The employer will include in the application the reasons necessary for video surveillance, the locations to be monitored, the equipment to be used, and the times the surveillance will be used.

2) The Permissive Use Permit will allow an employer to use video camera surveillance for the purposes stated in the application. An employer using video surveillance in conformity with the Permit will be immune from any civil or criminal action arising from its use.

3) The Secretary of Labor may, in his sole discretion, issue or deny any application for a Permissive Use Permit.

f) Enforcement: The Secretary of Labor may bring criminal

proceedings against any employer³⁰⁹ who violates any section of the Act.

1) Section (a) violations: Employers in violation of section (a) of the act may be sentenced to 1 year in prison and may be fined up to \$25,000.

2) Section (b) violations: Employers in violation of section (b) of the act may be fined up to \$5,000.

g) Private Remedies: Employees whose rights under this section have been violated may bring a private cause of action against their employer.

1) Employees may recover statutory damages of no more than \$25,000 and may recover attorney's fees.

VIII. CONCLUSION

The United States government proudly declares its support for human rights.³¹⁰ Although American policy claims to be embodied in the Universal Declaration of Human Rights, the two are remarkably different.³¹¹ Whereas the Universal Declaration of Human Rights is replete with the word dignity,³¹² American policy is nearly devoid of it.³¹³ In the 18th Century, when the Constitution and Bill of Rights were

309. An employer is defined as a business entity as well as individuals within the business directly responsible for the violation.

310. See Department of State, Human Rights, <http://www.state.gov/g/drl/hr> (last visited Feb. 22, 2007) [hereinafter DOS].

311. Compare *id.*, with Universal Declaration of Human Rights, G.A. Res. 217A, at 71, GAOR, 3d Sess., 183d plen. mtg., U.N. Doc. A/810 (Dec. 10, 1948) [hereinafter UDHR].

312. UDHR, *supra* note 311, pmbl., arts. 1, 22, 23.

313. DOS, *supra* note 310. A Westlaw search for the word "dignity" in all U.S. federal statutes returns forty results. *E.g.* 2 U.S.C. § 814(b)(1)(A)(ii) (2000) (establishing and administering "Congressional Recognition for Excellence in Arts Education Awards Program"); 8 U.S.C. § 1448(d) (2000) (ensuring dignity of naturalization ceremony); 12 U.S.C. § 1701q(a) (2000) (enabling elderly persons to live with dignity); 16 U.S.C. § 1a-1 (2000) (finding the national park system increases national dignity). In addition, Congress has found that agriculture, courts, military medals, the government, and the Nation's Capital all have dignity worth protecting. See 40 U.S.C. § 18301 (Supp. IV. 2006); 40 U.S.C. § 6734 (Supp. V. 2007); 36 U.S.C. § 40502(2) (2000); 36 U.S.C. § 20102 (2000).

ratified, the government was viewed as the only major threat to individual rights.³¹⁴ The Founders did not imagine that one day, concentrations of corporate power would exist on a scale that would rival or exceed governmental power.

U.S. law protects important workers' rights such as minimum wage,³¹⁵ safety and health,³¹⁶ benefits packages,³¹⁷ and leave for workers to care for families.³¹⁸ It is time for Congress to protect workers' privacy and dignity from video surveillance.

The uniformity and comprehensiveness of federal legislation is necessary to ensure the privacy and dignity rights of America's workingmen and workingwomen are adequately represented and protected. We implore Congress to act on the important issue of workplace video surveillance.

Alexandra Fiore & Matthew Weinick***

314. ACLU, *The Rights of Employees*, http://www.acluf.org/take_action/download_resources/info_papers/12.cfm (last visited Apr. 2, 2008).

315. Fair Labor Standards Act (FLSA) of 1938, 29 U.S.C. § 201, 202 (2000).

316. Occupational Safety and Health Act (OSHA) of 1970, 29 U.S.C. § 651 (2000).

317. Employee Retirement Income Security Act (ERISA) of 1974, 29 U.S.C. § 1001 (2000).

318. Family Medical Leave Act (FMLA) of 1974, 29 U.S.C. § 2601 (2000).

* I would like to thank my co-author, Matt, for his patience, hard work and support throughout the entire publication process. Thank you to the editors and staff of the Hofstra Labor & Employment Law Journal, without whom this publication would not have been possible. Thanks to my sister, Jackie, for teaching me the true meaning of strength and for giving me perspective, and to my parents for their unwavering love and support. I would like to dedicate this Note to my wonderful grandmother, Anna Mae Richter. Nana, I couldn't have done this without you.

** Thank you to my note partner, Alex, I could not have asked for a better co-author. Thank you to my parents, Mike and Suzanne, for always believing in me. Most of all, thank you Amy, your love and support made this note, and so much more, possible.