The John Marshall Journal of Information Technology & Privacy Law

Volume 25
Issue 1 *Journal of Computer & Information Law - Winter 2007*

Article 1

Winter 2007

From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace, 25 J. Marshall J. Computer & Info. L. 1 (2007)

Robert D. Sprague

ARTICLES

FROM TAYLORISM TO THE OMNIPTICON: EXPANDING EMPLOYEE SURVEILLANCE BEYOND THE WORKPLACE

ROBERT SPRAGUE†

I. INTRODUCTION

Frederick Taylor and his scientific management techniques were heralded in the early twentieth century as the quintessential achievement in workplace efficiency.[1] When representing clients opposing a rate increase requested by railroads, Louis Brandeis, before he became a U.S. Supreme Court Justice, turned to Taylorism to bolster his argument that the railroads were inefficient and therefore did not deserve a rate increase.[2] Brandeis viewed Taylor's techniques as one of the greatest contributions to society, and the publicity surrounding Brandeis' use of Taylorism to defeat the railroad's rate increase request led to the adoption and promotion of scientific management worldwide.[3]

Taylor recognized that efficiencies could be gained only through "the watchfulness of management."[4] This, according to Kanigel, led to an "unholy obsession with time, order, productivity, and efficiency that marks our age."[5] Through Taylor's scientific management approach, workers were under constant surveillance by a manager with a stopwatch—not just measuring, but also judging, prying, and intruding.[6] To the workers, the stopwatch "was a hideous invasion of privacy, an oppressive all-seeing eye that peered into their work lives, ripping at their dignity."[7]

---

† JD, MBA. Assistant Professor, University of Wyoming College of Business Department of Management and Marketing.

1. Robert Kanigel, *Taylor-Made: How the World's First Efficiency Expert Refashioned Modern Life in His Own Image,* SCI., May-June 1997, at 18.

2. *See* ROBERT KANIGEL,THE ONE BEST WAY 429-443 (1997).

3. *See id.*

4. FREDERICK W. TAYLOR, The Principles of Scientific Management 85 (Easton Press 1993) (1911).

5. Kanigel, *supra* note 1, at 7.

6. *See id.* at 466.

7. *Id.*

The concept of Taylor's all-seeing eye was expanded by the Panopticon. Originally a twelve-sided polygon prison with a central tower through which the superintendent could observe the behavior of the inmates, the Panopticon represents a means of constant, centralized observation.[8] One can always be observed within the Panopticon. In the early twenty-first century, electronics have largely replaced optics, with computer networks possibly replacing the original architecture of the Panopticon.[9]

The concept of surveillance under the Panopticon has evolved into what Jeffrey Rosen refers to as the "Omnipticon," in which the many are watching the many.[10] Everyone is under surveillance, all the time, everywhere.[11] While Taylor-based dystopian fears centered on a regimented society in which every human endeavor, from walking to eating, was strictly regimented,[12] Omnipticon-based fears are more Orwellian.[13] The issue addressed in this article is whether U.S. employers can become Big Brother, constantly monitoring employees not only at the workplace, but outside of work as well. This article explores the legal environment that arguably allows U.S. employers to extend employee monitoring and surveillance beyond the workplace.[14]

---

8. *See* Alan McKinlay & Ken Starkey, Managing Foucault: Foucault, Management and Organization Theory, in FOUCAULT, MANAGEMENT AND ORGANIZATION THEORY: FROM PANOPTICON TO TECHNOLOGIES OF SELF 2 (Alan McKinlay & Ken Starkey, eds. 1998).

9. *See* Gibson Burrell, *Modernism, Postmodernism and Organizational Analysis: The Contribution of Michel Foucault, in* FOUCAULT, MANAGEMENT AND ORGANIZATION THEORY: FROM PANOPTICON TO TECHNOLOGIES OF SELF 20 (Alan McKinlay & Ken Starkey, eds. 1998); Graham Sewell & James R. Barker, *Coercion Versus Care: Using Irony to Make Sense of Organizational Surveillance*, 31 ACAD. MGMT. REV. 934 (2006).

10. JEFFREY ROSEN, THE NAKED CROWD 11 (2004).

11. *See, e.g.*, Thomas L. Friedman, Editorial, *The Whole World is Watching*, N.Y. TIMES, June 27, 2007, at A23 (discussing the prevalence of blogs and camera cell phones making everyone a paparazzo and everyone a public figure).

12. *See* Kanigel, *supra* note 1, at 14-15; YEVGENY ZAMYATIN, WE (Natasha Randall, Modern Library 2006) (1952).

13. *See, e.g.*, Jill Yung, *Big Brother Is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163 (2005) (arguing that Global Positioning System (GPS) technology allows employers to monitor employees beyond the workplace); *see also* Gary T. Marx, *The Case of the Omniscient Organization*, HARV. BUS. REV., March-Apr. 1990, at 12 (describing in 1990, perhaps presciently, the "modern" workplace); *but see* Christopher P. Fazekas, *1984 Is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15 (2004) (arguing that current U.S. law governing electronic monitoring in the workplace is fair, particularly in light of potential employer liability for employee misconduct).

14. Although surveillance is a form of monitoring, because this article focuses extensively on forms of electronic monitoring, which is a type of surveillance, the terms monitoring and surveillance are used interchangeably herein.

Part II of this article reviews the basic surveillance techniques currently employed in the workplace and employer justifications for the surveillance. Part III provides an overview of the development of privacy law in the United States, with an emphasis on information privacy. Part IV of this article examines workplace privacy and demonstrates that, for the employee, it exists in only extreme circumstances. Part V reviews instances of employers exerting influence over employees outside the workplace, and examines the extent to which employers may have the legal right to monitor employees off-hours and off-site.

II. WORKPLACE SURVEILLANCE

As the office has replaced the factory floor, telephones, computers, e-mail, and the Internet have become the tools of the modern workplace.[15] Electronic monitoring in the workplace has become as ubiquitous as these modern office tools.[16] Most forms of workplace surveillance involve electronically monitoring Internet use and Web browsing, e-mail, and instant messaging (IM) communications, computer use, and telephone calls. A 2005 survey by the American Management Association found that over three-quarters of companies were monitoring their workers' Web site connections, with approximately fifty percent retaining and reviewing e-mail messages, computer files, and tracking time spent and numbers called on the telephone system, and approximately twenty percent of firms were taping employee telephone conversations.[17] Although employers were apparently monitoring the use of computers since their introduction into the workplace,[18] the 2005 percentages represent significant increases from a similar 2001 survey.[19]

Although employers also use video cameras to monitor the work-

15. *See* Richard S. Rosenberg, The Technological Assault on Ethics in the Modern Workplace, *in* THE ETHICS OF HUMAN RESOURCES AND INDUSTRIAL RELATIONS 141 (John W. Budd & James G. Scoville eds. 2005).

16. *See* Scott C. D'Urso, *Who's Watching Us at Work? Toward a Structural-Perceptual Model of Electronic Monitoring and Surveillance in Organizations*, 16 COMM. THEORY 281 (2006).

17. *See* American Management Association, *2005 Electronic Monitoring & Surveillance Survey*, http://www.amanet.org/research/pdfs/EMS_summary05.pdf (last visited Jan. 18, 2007).

18. *See, e.g.*, BARBARA GARSON, THE ELECTRONIC SWEATSHOP: HOW COMPUTERS ARE TRANSFORMING THE OFFICE OF THE FUTURE INTO THE FACTORY OF THE PAST 215 (1988); JON D. BIBLE & DARIEN A. MCWHIRTER, PRIVACY IN THE WORKPLACE 174-75 (1990).

19. *See 2005 Electronic Monitoring & Surveillance Survey*, *supra* note 17; *See also Employee Privacy: Computer-Use Monitoring Practices and Policies of Selected Companies*, G.A.O. REPORT TO THE RANKING MINORITY MEMBER, SUBCOMMITTEE ON 21ST CENTURY COMPETITIVENESS, COMMITTEE ON EDUCATION AND WORKFORCE, HOUSE OF REPRESENTATIVES, Sept. 2002, *available at* http://www.gao.gov/new.items/d02717.pdf.

place,[20] employers engage in other forms of workplace monitoring that are not specifically a form of surveillance. For example, under certain circumstances, employers may test employees for drug use or submit employees to polygraphs.[21]

Employers have a number of justifications for monitoring the workplace; they have valuable property rights they are attempting to protect.[22] "[E]mployers regard control of the workplace as their prerogative, including the right to protect and control their property, and the right to supervise and manage employee performance in terms of productivity, quality, training, and the recording of customer interactions."[23] One significant motivation for monitoring is performance-based, ensuring that employees are performing their work effectively and efficiently, or at all.[24] Employers also have a legitimate concern that confidential information (particularly trade secrets and strategies) are not intentionally or inadvertently disclosed through communications systems.[25]

Additionally, employers face significant legal risks associated with workplace communications systems. Of particular concern is that employees will create a hostile work environment by openly browsing pornographic Web sites or sending sexually explicit or racially insensitive e-mail messages. Title VII of the Civil Rights Act of 1964 makes it "an unlawful employment practice for an employer . . . to discriminate against any individual with respect to his compensation, terms, conditions, or privileges of employment, because of such individual's race,

---

20. *See, e.g.,* Nelson v. Salem State Coll., 845 N.E.2d 338 (Mass 2006) (involving an employer's use of video surveillance in a work area).

21. *See* Victor Schachter, *Privacy in the Workplace*, 828 PLI/PAT 153, 194-199 (2005) (discussing workplace employee drug tests and polygraphs).

22. *See* Corey A. Ciocchetti, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26, 4 (2001).

23. Patricia Findlay & Alan McKinlay, *Surveillance, Electronic Communications Technologies and Regulation*, 34 INDUS. REL. J. 305, 306 (2003) (citation omitted).

24. *See* Ciocchetti, *supra*, note 22, at 4 (listing maintaining employee productivity as one of several reasons for employer monitoring); Leonard Court & Courtney Warmington, *The Workplace Privacy Myth: Why Electronic Monitoring is Here to Stay*, 29 OKLA. CITY U. L. REV. 15, 18 (2006) (noting survey results in which employees admitted spending between a half day to two days per week shopping on the Internet at work for holiday gifts); Lee N. Jacobs, *Is What's Yours Really Mine?:* Shmueli v. Corcoran Group *and Penumbral Property Rights*, 14 J.L. & POL'Y 837, 848 (2006) (stating that Internet messaging and personal e-mails are part of the reasons computers have replaced the coffee room or talking on the telephone as the largest waste of an employee's on-the-job time); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 290 (2002) (quoting one estimate that "cyberslacking" is responsible for up to a forty percent loss in employee productivity).

25. *See* Ciocchetti, *supra* note *22*; Kesan, *supra* note 24; Anne L. Lehman, *E-Mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMMLAW CONSPECTUS 99 (1997).

color, religion, sex, or national origin."[26] The Supreme Court has made clear that this language is not limited to economic or tangible discrimination,[27] which would include discrimination related to hiring, firing, promotion, compensation, and work assignment.[28] In defining "sexual harassment," the Equal Employment Opportunity Commission (EEOC) Guidelines include actionable conduct such as "[u]nwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature."[29] The Guidelines further provide that sexual misconduct constitutes prohibited "sexual harassment," whether or not it is directly linked to the grant or denial of an economic *quid pro quo*, where "such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment."[30] A plaintiff may establish a violation of Title VII by proving that discrimination based on sex has created a hostile or abusive work environment,[31] though all protected classes (not just gender classes) are protected from hostile work environments.[32]

In *Harris v. Forklift Systems, Inc.*, the Supreme Court attempted to establish a standard that struck a balance between merely offensive conduct and conduct that causes tangible psychological injury.[33] "Conduct that is not severe or pervasive enough to create an objectively hostile or abusive work environment . . . is beyond Title VII's purview. . . . [I]f . . . the conduct has not actually altered the conditions of the victim's employment, . . . there is no Title VII violation."[34] At the same time, however, "Title VII comes into play before the harassing conduct leads to a nervous breakdown."[35] Despite recognizing in *Harris* that determining whether a hostile environment exists is not subject to a "mathematically precise test,"[36] the Court believes standards for judging hostility are sufficiently demanding to ensure that Title VII does not become a "general civility code."[37] Courts must look at all the circumstances, including the frequency of the discriminatory conduct; its severity; whether it is physi-

26. Harris v. Forklift Sys., Inc., 510 U.S. 17, 21 (1993) (quoting 42 U.S.C. § 2000e-2(a)(1) (2006)).

27. *See* Meritor Sav. Bank v. Vinson, 477 U.S. 57, 64 (1986).

28. *See* Faragher v. City of Boca Raton, 524 U.S. 775, 790 (1998).

29. 29 C.F.R. § 1604.11(a) (1985); *see generally*, *Meritor*, 477 U.S. at 65.

30. *Meritor*, 477 U.S. at 65 (quoting 29 C.F.R. § 1604.11(a)(3) (1985)).

31. *See id.* at 66.

32. *See, e.g.*, Curtis v. DiMaio, 46 F.Supp.2d 206, 212-14 (E.D.N.Y. 1999), *aff'd*, 205 F.3d 1322 (2nd Cir. 2000) (addressing hostile work environment claim based on race; holding that a single racist e-mail does not create an actionable hostile environment).

33. *Harris*, 510 U.S. at 17.

34. *Id.* at 21-22.

35. *Id.* at 22.

36. *Id.* at 23.

37. *Faragher*, 524 U.S. at 788 (citation omitted).

cally threatening or humiliating, or a mere offensive utterance; and whether it unreasonably interferes with an employee's work performance.[38]

In *Faragher*, and a companion case, *Burlington Industries, Inc. v. Ellerth*, the Supreme Court held that an employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee, though when no tangible employment action is taken, a defending employer may raise an affirmative defense: (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior; and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise.[39]

In both *Faragher* and *Burlington Industries*, Justice Thomas argued that absent an adverse employment consequence, an employer should not be held vicariously liable if a supervisor creates a hostile work environment.[40] Justice Thomas expressed his concern that "[s]exual harassment is simply not something that employers can wholly prevent without taking extraordinary measures—constant video and audio surveillance, for example—that would revolutionize the workplace in a manner incompatible with a free society."[41] Justice Thomas was echoing the rhetorical response Justice Posner had expressed in his dissent to the case's appellate court decision (which was upheld by *Burlington Industries*):

> [I]t is facile to suggest that employers are quite capable of monitoring a supervisor's actions affecting the work environment. Large companies have thousands of supervisory employees. Are they all to be put under video surveillance? Subjected to periodic lie-detector tests? Trailed on business trips by company spies?[42]

Jeffrey Rosen argues that the Supreme Court's rulings on hostile work environments provide a "strong incentive [for employers] to monitor and punish far more private speech and conduct than the law actually forbids."[43]

Employers face additional legal concerns that drive workplace monitoring. Recent amendments to the Federal Rules of Civil Procedure formalize the use of electronically stored documents in litigation.[44] One

38. *See id.* at 777-78 (citation omitted).

39. *See id.*; Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 745 (1998).

40. *Faragher*, 524 U.S. at 810 (Thomas, J., dissenting); *Burlington*, 524 U.S. at 767 (Thomas, J., dissenting).

41. *Id.* at 770 (Thomas, J., dissenting) (citation omitted).

42. Jansen v. Packaging Corp. of Am., 123 F.3d 490, 513 (7th Cir. 1997) (Posner, C. J., concurring and dissenting).

43. JEFFREY ROSEN, THE UNWANTED GAZE 13 (2000).

44. *See Federal Procedure Changes on E-Discovery, Unpublished Opinion Citations Take Effect*, 75 U.S. LAW WK. 2313 (2006).

commentator has argued that the amended rules will make systematic electronic monitoring an attractive option to

> (1) keep employees from using company networks for personal reasons, thereby reducing the amount of data captured on backup tapes; (2) detect improper employee behavior before a lawsuit is lodged against the company; and (3) prevent key players from erasing evidence from their computers once litigation is anticipated.[45]

Employers have also been held liable for harm caused to third parties by employees under the negligent retention doctrine.[46] Under the negligent retention doctrine, employers are under a duty of care in the supervision and retention of employees. If the employer is aware, or should have been aware, of any potential an employee has to cause harm to third parties (including co-workers), the employer will be liable if it does not take reasonable steps to prevent that harm.[47] However, there must be some nexus between the employer's business and the third party before liability can attach.[48]

Potential employer liability for employee communications is a principal motivation for monitoring,[49] as well as formulating electronic technology policies.[50] Employers are enforcing those policies by disciplining

---

45. Elaine K. J. Kim, *The New Electronic Discovery Rules: A Place for Employee Privacy?*, 115 YALE L.J. 1481, 1485 (2006).

46. *See* Rosanne Lienhard, *Negligent Retention of Employees: An Expanding Doctrine*, 63 DEF. COUNS. J. 389, 389 (1996) (explaining that the negligent retention doctrine is an expansion of the fellow servant rule, rather than the vicarious liability doctrine (which would hold the employer liable to harmed third parties only if the employee were acting within the scope of authority when the act occurred)).

47. *See, e.g.*, Yunker v. Honeywell, Inc., 496 N.W.2d 419 (Minn.Ct.App. 1993). Despite the fact there was a gap in the employee's (Landin's) work history with Honeywell because Landin was incarcerated for five years for killing a Honeywell coworker, the court held that Honeywell was not liable for negligent hiring for rehiring Landin, who subsequently murdered another Honeywell coworker, because Landin was rehired "as a maintenance worker whose job responsibilities entailed no exposure to the general public and required only limited contact with coemployees." *Id.* at 421, 423. The court did, however, find Honeywell liable for negligent retention due to Landin's "troubled work history and the escalation of abusive behavior" after he was rehired. *Id.* at 424.

48. *See, e.g.*, Delfino v. Agilent Techs., Inc., 52 Cal.Rptr.3d 376, 398 (Cal.Ct.App. 2006) (holding that an employer, whose employee had sent threatening e-mail messages to the plaintiff through the employer's computer system, owed no duty to the plaintiff because the plaintiff and employer had no business relationship; addressing a negligent supervision/retention claim, and stating "[i]t would be a dubious proposition indeed to suggest that a party, simply by virtue of engaging in business, owes a duty to the world for all acts taken by its employee, irrespective of whether those actions were connected with the enterprise in which the business was engaged").

49. *See* Court & Warmington, *supra* note 24, at 18-19 (citing a 2001 American Management Association survey indicating that legal liability is the primary motivation for the majority of firms that monitor employee e-mail and Internet use).

50. *See 2005 Electronic Monitoring & Surveillance Survey*, *supra* note 17.

employees who violate the policies, including termination.[51]

Courts are beginning to recognize that workplace monitoring is becoming a *de facto* standard. As noted by one court, the "community norm" within twenty-first century computer-dependent businesses is to monitor telephone calls, e-mails, Internet connections, and computer files.[52] Furthermore, businesses may find themselves liable to third parties, even beyond the negligent retention theory, if they fail to monitor employees' computer use and act on their misdeeds.[53] For example, in *Doe v. XYC Corp.*, it became known to computer technicians and supervisors that an employee was using the employer's computer system to visit pornographic Web sites while at work.[54] No action was taken, particularly because of the employer's policy against monitoring the Internet activities of employees.[55] The employee's wife later sued the employer for negligence (on behalf of her daughter) after it was discovered the employee had published nude photos of the wife's daughter on Internet Web sites using his office computer.[56] The New Jersey Superior Court reversed the lower court's granting of the employer's motion for summary judgment, holding that where an employer is on notice that one of its employees is using a workplace computer to access pornography, and possibly child pornography, that employer has a duty to investigate the employee's activities and take prompt action.[57] The court ruled there was a triable issue of fact as to whether the employer's failure to investigate and take action was a proximate cause of the harm suffered by the employee's stepdaughter.[58]

Arguably, there must be a balance between surveillance, and the ills it seeks to prevent, and civil liberties.[59] However, as discussed more fully below, the balance has been predominantly tipped in favor of the employer.

---

51. *See id.*

52. TBG Ins. Servs. Corp. v. Super. Ct., 117 Cal.Rptr.2d 155, 161-62 (Cal. Ct. App. 2002).

53. *See, e.g.,* Doe v. XYC, Corp., 887 A.2d 1156 (N.J.Super. Ct.App.Div. 2005).

54. *See id.* at 1158-60.

55. *See id.* at 1159.

56. *See id.* at 1161.

57. *See id.* at 1158.

58. *See id.* at 1169-70; *but see* Delfino, 52 Cal.Rptr.3d at 398 (holding that an employer, whose employee had sent threatening e-mail messages to the plaintiff through the employer's computer system, owed no duty to the plaintiff because the plaintiff and employer had no business relationship; addressing a negligent supervision/retention claim). *Doe* and *Delfino* may be distinguished by the fact that the employer in *Delfino* was unaware of the employee's conduct (*see* Delfino, 52 Cal.Rptr.3d at 399), whereas the employer in *Doe* knew its employee was visiting pornographic sites at work (*see* Doe, 887 A.2d at 1158-60).

59. *See generally* Sewell & Barker, *supra* note 9, at 934.

III. PRIVACY

The concept of privacy is amorphous. Commentators have referred to it as "illusive" and "ill-defined;"[60] a concept in disarray for which no one can articulate a meaning;[61] with little agreement about its source as a right.[62] In one sense, privacy protects against affronts to dignity by persons or entities who pry too deeply into our personal affairs.[63] Privacy is also considered vital to decisions of intimacy.[64] One common theme of the concept of privacy is the right to control information about oneself,[65] which also implies control of that information's dissemination, as well as protections against intrusions, such as through monitoring and surveillance.[66]

In the United States, the legal right to privacy is just as amorphous. The U.S. Constitution does not expressly guarantee a right to privacy, though the U.S. Supreme Court has recognized an implied constitutional right of privacy in certain situations. As discussed in more detail below, an individual's right to privacy is only directly protected through a hodgepodge of state and federal statutes applied to specific circumstances.

The first reported instance of a court recognizing a right of privacy arose in the late nineteenth century in the case of *De May v. Roberts*, in which a man impersonated a doctor in order to be present when a woman gave birth.[67] Although the woman sued for battery, the court recognized that she "had a legal right to privacy" while giving birth.[68]

A few years later Warren and Brandeis (the same Louis Brandeis who had earlier championed Taylorism[69]) advocated the legal recognition of a "right to be let alone."[70] It is reported that the impetus for this

60. Richard A. Posner, *An Economic Theory of Privacy, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 331, 331 (Ferdinand D. Schoeman ed. 1984).

61. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477 (2006).

62. *See* Gary L. Bostwick, *A Taxonomy of Privacy: Repose, Sanctuary, and Intimate Decision*, 64 CAL. L. REV. 1447, 1448 (1976).

63. *See* Edward J. Bloustein, *Privacy As an Aspect of Human Dignity: An Answer to Dean Prosser, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 156 (Ferdinand D. Schoeman ed. 1984).

64. *See* Robert S. Gerstein, *Intimacy and Privacy, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 265 (Ferdinand D. Schoeman ed. 1984).

65. *See* Lubor C. Velecky, *The Concept of Privacy, in* PRIVACY 13, 20 (John B. Young ed. 1978); Richard A. Wasserstrom, *Privacy: Some Arguments and Assumptions, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 317, 317 (Ferdinand D. Schoeman ed. 1984).

66. *See* Ruth Gavison, *Privacy and the Limits of Law, in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 346, 351-56 (Ferdinand D. Schoeman ed. 1984).

67. 9 N.W. 146 (Mich. 1881).

68. *Id.* at 149.

69. *See supra*, text accompanying note 3.

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

treatise was Warren's dismay at seeing details of his daughter's wedding reported in the Boston gossip pages.[71] Warren and Brandeis argued for a legal protection from "injurious disclosures as to private matters."[72] Presaging an era of technologically enhanced surveillance, Warren and Brandeis buttressed their argument by discussing new advances in photographic technology, allowing individuals to be surreptitiously photographed, compared to the older technology which required one's consent to "sit" for a photographic portrait.[73] Warren and Brandeis' main thesis was that individuals had the right to determine what information about them could be made public.[74]

Although there were a few false starts in getting courts to formally recognize a legal right to privacy,[75] on the basis of Warren and Brandeis' work, courts throughout the country began to recognize a common law right to privacy. In analyzing the various state cases involving a right to privacy, Prosser later identified four distinct types of invasions:

> (1) Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs[;] (2) Public disclosure of embarrassing private facts about the plaintiff[;] (3) Publicity which places the plaintiff in a false light in the public eye[; and] (4) Appropriation, for the defendant's advantage, of the plaintiff's name or likeness.[76]

As will be explored in more detail below, employees of private enterprises, who believe their privacy has been invaded by their employer, base their claim predominately on Prosser's first type of invasion: intrusion upon seclusion.

Contemporaneous to the development of the common law right of privacy in state courts, another related right of privacy was also developing—that against unreasonable searches and seizures. The Fourth Amendment to the U.S. Constitution grants "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . ."[77] Warrants authorizing a search or seizure must be based on probable cause and must describe with particu-

---

71. *See* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 383 (1960).

72. Warren & Brandeis, *supra* note 70, at 204.

73. *See id.* at 211.

74. *See id.* at 199.

75. *See, e.g.*, Roberson v. Rochester Folding Box Co., 64 N.E. 442, 552 (N.Y. 1902) (declaring no right of privacy exists in case involving the use of a young lady's picture to advertise flour without her consent).

76. Prosser, *supra* note 71, at 389. New York, however, does not have a common law right of privacy. *See* Chimarev v. TD Waterhouse Investor Servs., Inc., 280 F.Supp.2d 208, 216 (S.D.N.Y. 2003) (holding also that "New York's limited [statutory] right of privacy does not prohibit an employer from accessing employee e-mail and other documents produced on the company's system").

77. U.S. CONST. amend. IV.

larity the place to be searched, and the persons or things to be seized.[78] The Fourth Amendment applies to the states through the Fourteenth Amendment.[79]

In the late nineteenth century, the U.S. Supreme Court had ruled that sealed letters[80] and private papers were private,[81] and thus subject to Fourth Amendment warrant requirements. In the early twentieth century, the issue arose of whether authorities needed a warrant to surreptitiously listen to someone's telephone call.[82] This was problematic because the Fourth Amendment's language refers to seizing people or things, or searching places. Since there was no entry, no search, and no seizure, the Supreme Court initially ruled that telephone conversations were outside the Fourth Amendment's warrant requirement.[83] In his dissent, Justice Brandeis resurrected a theme from his earlier treatise with Warren,[84] that technology had transformed the nature of communications from letters to conversations over wires. Brandeis argued that if sealed letters deserved protection, so did telephone conversations.[85]

Following this theme, the Supreme Court reversed itself in *Katz v. U.S.*, rejecting a requirement of physicality in a search or seizure.[86] In *Katz,* the Court held that the Government's activities in electronically listening to and recording an individual's words violated the privacy upon which he justifiably relied while using a telephone booth, resulting in a "search and seizure" within the meaning of the Fourth Amendment.[87] The Court stated that while what a person exposes to the world is not protected by the Fourth Amendment, what a person seeks to preserve as private may be constitutionally protected, at least from an unwarranted search or seizure.[88] There is limited authority that the logic in *Katz*, as applied to telephone calls, may be applied to private e-mail messages. In *Warshak v. U.S.*, the Sixth Circuit Court of Appeals held that an individual had a reasonable expectation of privacy in e-mails sent through and stored by an Internet service provider, at least as applied to the warrant requirement under the Fourth Amendment.[89] "It goes without saying that like the telephone earlier in our history, e-mail

78. *See id.*
79. U.S. CONST. amend. XIV; *see* O'Connor v. Ortega, 480 U.S. 709, 714 (1987).
80. *Ex parte* Jackson, 96 U.S. 727 (1877).
81. Boyd v. U. S., 116 U.S. 616 (1886).
82. *See* Olmstead v. U.S., 277 U.S. 438 (1928).
83. *See id.* at 463.
84. *See supra*, text accompanying note 73.
85. *See Olmstead*, 277 U.S. at 475 (Brandeis, J., dissenting).
86. 389 U.S. 347 (1967).
87. *Id.* at 353.
88. *See id.* at 351.
89. 490 F.3d 455, 473 (6th Cir. 2007), *Rehearing en Banc Granted, Opinion Vacated* (Oct 09, 2007).

is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[90]

The Supreme Court supported a general constitutional right to privacy in *Griswold v. Connecticut*, holding there was a "penumbral" right to privacy emanating from the Constitution and its amendments.[91] In particular, the majority believed that a husband and wife were entitled to a "zone of privacy" surrounding their intimate relationship, including their physician's role in that relationship.[92] The right of privacy expressed in *Griswold* was used as the basis to overturn laws banning interracial marriages,[93] the possession of pornography in one's own home,[94] and the distribution of contraceptives;[95] as well as limits on sexual conduct of consenting adults in the privacy of their own homes.[96]

The main focus of the Supreme Court's penumbral zone of privacy is intimacy; whereas, constitutional rights relative to the collection and dissemination of information come from the Fourth Amendment. In *Katz*, the Supreme Court specifically rejected the notion that the Fourth Amendment provides a general constitutional right to privacy.[97] Instead, the Supreme Court left it up to individual states to protect the general right of privacy.[98] In *Roe v. Wade*, the Supreme Court added that the constitutional guarantee of personal privacy includes personal rights only if they are "fundamental" or "implicit in the concept of ordered liberty."[99]

Underlying any right of privacy is a person's subjective expectation of privacy in a given situation.[100] Different situations present different expectations of privacy. Someone may not be intruding into a couple's right to privacy when, from the sidewalk, he overhears a couple having a loud argument inside their home with the windows open; on the other hand, someone may be intruding into the couple's right to privacy when he uses an amplifier to listen to the couple having a quiet conversation

90. *Id.*

91. 381 U.S. 479, 484 (1965) (reversing a Connecticut law that resulted in the prosecution of Planned Parenthood of Connecticut and a doctor for dispersing contraceptives and related information to married persons).

92. *Id.* at 485.

93. Loving v. Virginia, 388 U.S. 1 (1967).

94. Stanley v. Georgia, 394 U.S. 557 (1969).

95. Eisenstadt v. Baird, 405 U.S. 438 (1972).

96. Lawrence v. Texas, 539 U.S. 558 (2003).

97. *See Katz*, 389 U.S. at 350.

98. *See id.* at 350-51.

99. 410 U.S. 113, 152 (1973) (recognizing a conditional constitutional right of privacy in a woman's abortion decision).

100. *See Katz*, 389 U.S. at 347.

inside their home with the windows closed.[101] One court held that night club dancers had no expectation of privacy when they knew club security personnel had video surveillance of their dressing room, but the dancers did have an expectation of privacy when government agents viewed the same surveillance without a warrant.[102] Similarly, loss of privacy in one context (such as undressing in one's home before an open window) does not lead to loss of privacy in other contexts (such as an unwarranted search by police of that same home for illegal drugs).[103]

What is exposed to the public, though, is not private. There is no expectation of privacy, and hence no constitutional protection, for matters open to public observation.[104] For example, the court in *Nelson v. Salem State College* found no invasion of privacy where a college employee was videotaped by a hidden camera while changing clothes in a locked office to which a number of employees had a key, primarily because the court regarded the office as an "open work area."[105] Even though the video camera was installed to thwart after-hour thefts, the court was unconcerned that the camera was recording twenty-four hours per day. The court focused instead on the employee's subjective expectation of privacy within the office, with or without the camera.[106]

The *Nelson* holding has been extended to data stored on a personal computer brought into the workplace. In *U.S. v. Barrows*, the Tenth Circuit concluded that an employee had no expectation of privacy in any files observed by co-workers when that employee connected his personal computer, located in a public work area, to his employer's computer network which allowed file sharing, left the computer running, and did not password-protect any files.[107] The court ruled that while the employee may have had "a subjective expectation of privacy, his failure to take affirmative measures to limit other employees' access made that expectation unreasonable."[108]

Someone invoking Fourth Amendment protection from government action must claim a "justifiable," a "reasonable," or a "legitimate expectation of privacy." The Supreme Court uses a two-part analysis to make this determination: (1) whether the individual, by his or her conduct, exhibited a subjective expectation of privacy; and (2) and whether that sub-

101. *See* Judith J. Thomson, *The Right to Privacy*, 4 Phil. & Pub. Aff. 295, 296 (1975).

102. *See* Bevan v. Smartt, 316 F.Supp.2d 1153, 1160-61 (D.Utah 2004).

103. *See id.* at 1161.

104. *See* Bond v. United States, 529 U.S. 334, 337 (2000).

105. 845 N.E.2d at 343.

106. *See id.* at 347.

107. *See* 481 F.3d 1246, 1249 (10th Cir. 2007).

108. *Id.* (citations omitted). "Those who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably expect their personal materials to remain private." *Id.*

jective expectation of privacy is reasonable, or objectively justifiable under the circumstances.[109] Applying this analysis, the Supreme Court ruled that the state of Maryland did not need a warrant to install a pen register that recorded numbers dialed from a person's home telephone line, noting that the pen register did not record actual conversations that took place. The Court concluded phone customers have no legitimate expectation of privacy in the phone numbers they dial because that information is transmitted to the phone company, which uses and records that information for a number of legitimate business purposes.[110] At least one court, following *Smith v. Maryland*, has ruled that using a "mirror port" (analogous to a pen register) to obtain from a criminal suspect's Internet Service Provider account to and from addresses of e-mail messages, the Internet protocol ("IP") addresses of websites visited, and the total volume of information transmitted to or from the account, is not a Fourth Amendment search.[111]

As stated succinctly by Jeffrey Rosen, "as advances in the technology of monitoring and searching have made ever more intrusive surveillance possible, expectations of privacy have naturally diminished, with a corresponding reduction in constitutional protection."[112] Justice Marshall recognized a similar dilemma when he dissented in *Smith v. Maryland*—the government could control the level of privacy expectation, and therefore the extent of protected privacy, simply by announcing an intent to monitor certain communications, such as phone calls and mail.[113] Similarly, employers (public or private) can control the expectations of their workforce, and, hence, the level of protected privacy, simply by notifying employees of the possibility of monitoring and surveillance.[114] Where

109. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979).

110. *See id.* at 743.

111. *See* United States v. Forrester, 495 F.3d 1041, 1048 (9th Cir. 2007).

112. Rosen, *supra* note 43, at 60-61.

113. *See Smith*, 442 U.S. at 749-50 (Marshall, J., dissenting).

114. *See, e.g.*, United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding employer's Internet policy "placed employees on notice that they could not reasonably expect that their Internet activity would be private.") (footnote omitted); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (holding that since the employer had announced that it could inspect laptop computers furnished for the use of its employees, this destroyed any reasonable expectation of privacy those employees might have had); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) ("University policies and procedures prevent its employees from reasonably expecting privacy in data downloaded from the Internet onto University computers."); *TBG Ins. Servs. Corp.*, 117 Cal.Rptr.2d at 162 ("[E]mployers can diminish an individual employee's expectation of privacy by clearly stating in the policy that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee Internet or e-mail usage."); Kelleher v. City of Reading, 2002 WL 1067442, *8 (E.D.Pa. 2002) (holding employee had no expectation of privacy in e-mails because City's guidelines explicitly informed employees that there was no such expectation of privacy).

employees were unaware of monitoring, at least one court found an expectation of privacy on the part of employees due to the frank nature of their conversations.[115] After all, the court reasoned, "no reasonable employee would harshly criticize the boss if the employee thought that the boss was listening."[116] Such is the nature of privacy. Individuals generally do not disclose intimate facts or perform intimate acts unless the individuals believe they are acting in private. Hence, private activities are only done when there is a reasonable belief that the activities are private, and individuals refrain from doing private things when they do not have an expectation of privacy.[117]

A. Specific Federal Privacy-Related Laws

Primarily in response to the growing collection of information about individuals in computer databases, the U.S. Congress began passing a series of privacy laws in the latter half of the twentieth century.[118] The majority of the federal privacy-related laws focus on consumer protection and protection from government intrusion, and only a few have direct application to the workplace.[119]

One of the first federal privacy-related laws passed by Congress is the Fair Credit Reporting Act of 1970,[120] which provides mechanisms for individuals to review their credit records and correct inaccuracies. In relation to the workplace, the Fair Credit Reporting Act requires that employers notify job applicants in writing if a credit report is to be obtained as part of the employer's consideration of the candidate,[121] and employers must notify an applicant if a credit report is used in making an adverse decision, such as a decision not to hire the applicant.[122]

---

115. *See* Dorris v. Absher, 179 F.3d 420 (6th Cir. 1999).

116. *See id.* at 425. *See also*, Restuccia v. Burk Tech., Inc., 1996 WL 1329386, *1, *3 (Mass.Super. 1996) (declining to grant summary judgment against employees' invasion of privacy claim where employer had no stated policy regarding use or monitoring of employee e-mails).

117. *See* Wasserstrom, *supra* note 65, at 321.

118. *See* Harry Henderson, Privacy in the Information Age (2006); Daniel J. Solove, *A Brief History of Information Privacy Law*, *Proskauer on Privacy*, Practicing Law Institute (2006), *available at* http://ssrn.com/abstract=914271.

119. *See infra*, notes 120-155 and accompanying text.

120. 15 U.S.C. § 1681 (2007).

121. *See id.* at § 1681d.

122. *See id.* at § 1681m. However, employers are not required to notify employees if credit reports are used as part of an investigation of work-related misconduct. The Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), Pub. L. No. 108-159, 117 Stat. 1952 (Dec. 4, 2003), amended the FCRA to remove employer investigations of employment-related misconduct or enforcement of company policies. *See* Schachter, *supra* note 21, at 181-85.

Congress also enacted the Freedom of Information Act of 1966 ("FOIA"), which allows citizens to request records maintained by an executive agency.[123] To protect privacy interests, though, personnel and medical files, as well as certain law enforcement information, cannot be disclosed under FOIA.[124] In 1974, Congress passed the Privacy Act, which regulates the collection and use of records by federal agencies, and affords individuals the right to access and correct their personal information.[125] In the same year, Congress enacted The Family Educational Rights and Privacy Act,[126] which limits the accessibility of student records. The Bank Secrecy Act of 1970[127] requires banks to retain records and create reports to help law enforcement investigations, while the Right to Financial Privacy Act of 1978 requires government officials to obtain a warrant or subpoena to obtain financial information.[128] The Right to Financial Privacy Act was enacted in direct response to the U.S. Supreme Court's decision in *U.S. v. Miller*,[129] where the Supreme Court held customers had no expectation of privacy in records kept by their banks and other financial institutions.[130] Congress also passed the Privacy Protection Act of 1980, which restricts the search or seizures of work product materials in the possession of third parties,[131] and the Computer Matching and Privacy Protection Act of 1988, which regulates the federal government's practice of comparing individual information stored across different agency computer databases.[132] The majority of other privacy-related federal laws are focused on consumer protection.[133]

Federal laws that can have an impact on the workplace include Sec-

123. 5 U.S.C. § 552(a)(3)(A) (2007).
124. *See id.* at § 552(b).
125. 5 U.S.C. § 552a (2007).
126. 20 U.S.C. § 1232g (2007).
127. Pub. L. No. 91-508.
128. Pub. L. No. 95-630.
129. 425 U.S. 435 (1976).
130. *See* Solove, *supra* note 118.
131. 42 U.S.C. § 2000aa (2007).
132. Pub. L. No. 100-503.
133. For example, the Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2794, codified at 42 U.S.C. § 551, restricts disclosure of the viewing habits of cable customers; Video Privacy Protection Act of 1988, 18 U.S.C. §§ 2710-11 (2007), prohibits video rental stores from disclosing customer video rental and purchase information; the Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-25 (2007), prohibits states from selling driver's license information without prior consent; the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, regulates the disclosure of health information; and the Gramm-Leach-Bliley Act of 1999, 15 U.S.C. §§ 6801-09 (2007), limits information sharing by financial institutions with third parties without prior consent by customers. *See* Solove, *supra* note 118. The Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) jointly promulgated regulations to create a "no call list" of telephone subscribers which telemarketers are prohibited from contacting. 16 C.F.R. § 310.4(b)(1)(iii)(B) (FTC rule); 47 C.F.R. § 64.1200(c)(2) (FCC rule). The rules were

tion 7 of the National Labor Relations Act ("NLRA"),[134] the Employee Polygraph Protection Act of 1988,[135] and the Electronic Communications Privacy Act of 1986.[136] Although the NLRA does not expressly protect employee privacy rights, it does limit an employer's ability to discipline or fire employees as a result of certain communications.[137] Section 7 of the NLRA "guarantees employees the right to engage in 'concerted activities' not only for self-organization but also 'for the purpose of . . . mutual aid or protection[.]'"[138] Section 8(a)(1) of the NLRA makes it an unfair labor practice for an employer to interfere with, restrain, or coerce employees in the exercise of the rights guaranteed in Section 7.[139] "[A]n employer violates Section 8(a)(1) by discharging an employee for engaging in concerted activities protected by the Act."[140] For example, an employer violated the NLRA when it fired an employee after the employee sent an e-mail message on behalf of fellow employees to management complaining about a new incentive compensation plan.[141]

The Employee Polygraph Protection Act[142] restricts employers' use of polygraphs. It prohibits private employers engaged in interstate commerce from using polygraphs to screen job applicants unless the employment relates to certain security functions or the manufacture, distribution, or sale of controlled substances.[143] The Act does not apply to public employers.[144]

A 1986 amendment to the Omnibus Crime Control and Safe Streets Act of 1968,[145] the Electronic Communications Privacy Act (ECPA),[146] protects against unwarranted interception or retrieval of electronic com-

---

promulgated to protect personal privacy. *See* Mainstream Mktg. Servs., Inc. v. F.T.C., 358 F.3d 1228 (10th Cir. 2004).

134. 29 U.S.C. § 157 (2007).

135. 29 U.S.C. §§ 2001-09 (2007).

136. 18 U.S.C. §§ 2510-22, 2701-11 (2007).

137. *See* 29 U.S.C. § 157 (2007).

138. Citizens Inv. Servs. Corp. v. N.L.R.B., 430 F.3d 1195, 1197 (D.C. Cir. 2005). Section 7 applies to non-unionized workers; since they have no bargaining representative, they must speak for themselves. *See id.*

139. 29 U.S.C. § 158(a)(1) (2007).

140. *Citizens*, 430 F.3d at 1197 (citation omitted).

141. *See id.* at 1199 (rejecting the Company's defense that the employee was discharged because he was a "troublemaker" and "not a team player"). *See also* Timekeeping Systems, Inc., 323 N.L.R.B. 244 (1997) (explaining that an e-mail message sent by employee to fellow employees criticizing new vacation policy was protected concerted activity).

142. 29 U.S.C. §§ 2001-09 (2007).

143. *See id.* at § 2006(e) & (f).

144. *See id.* at § 2006(a).

145. Pub.L. 90-351, Title III, § 802, 82 Stat. 212 (June 19, 1968).

146. 18 U.S.C. §§ 2510-22, 2701-11 (2007).

munications.[147] Title I of the ECPA restricts the use of wiretaps.[148] On its face, Title I would have an impact on an employer's ability to monitor employee telephone calls.[149] As discussed below, the statute provides minimal employee privacy protection,[150] particularly because of a "business use" exception in Title I.[151] Title II of the ECPA, the Stored Communications Act (SCA),[152] makes it illegal to access stored electronic communications without authorization.[153] The SCA, on its face, would appear to provide protection for workplace e-mails, but as will be discussed in more detail below, courts have interpreted the language of the SCA very strictly, holding employers' access of employee Web pages and personal e-mail accounts did not violate the SCA.[154] Overall, the ECPA provides little, if any, employee privacy protection.[155]

B. Specific State Privacy-Related Laws

States have enacted various laws directed at protecting individual rights of privacy. California's state constitution expressly includes privacy as a protected right.[156] Massachusetts' Right of Privacy statute provides: "A person shall have a right against unreasonable, substantial

147. *See* Ira David, *Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is it Big Brother or Just Business?*, 5 Nev. L.J. 319, 327 (2004).

148. 18 U.S.C. §§ 2510-2521 (2007).

149. Because Title I of the ECPA prohibits the interception of electronic communications, it has been interpreted as not applying when an employer accesses stored e-mail messages. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113-14 (3rd Cir. 2004) (providing an analysis of cases which have interpreted same).

150. *See infra,* text accompanying notes 206-210.

151. *See* 18 U.S.C. § 2510(5)(a) (2007).

152. 18 U.S.C. §§ 2701-2711 (2002).

153. *See* David, *supra* note 147, at 328.

154. *See* Konop v. Hawaii Airlines, Inc., 302 F.3d 868, 880 (9th Cir. 2002), *cert. denied,* 537 U.S. 1193 (2003) (holding that employers' access to employee Web site did violate SCA because employee Web site was held not "readily accessible;" employee required a user to enter an employee member's name and certify that user was not the employer before viewing the site); *but see* Snow v. DirecTV, 450 F.3d 1314, 1321 (finding Web site was readily accessible under the ECPA even though owner required users to acknowledge privilege before viewing the site); Fischer v. Mt. Olive Lutheran Church, 207 F.Supp.2d 914, 926 (W.D. Wis. 2002) (holding that employer's intentional access of employee's personal e-mail account alone is not enough to violate the SCA; employee must also show that employer obtained, altered or prevented employee's authorized access to his email account); *see infra,* text accompanying notes 229-237, for a more detailed discussion of the SCA to off-site employee conduct.

155. *See* Ray Lewis, *Employee E-Mail Privacy Still Unemployed: What the United States Can Learn From the United Kingdom*, 67 La. L. Rev. 959, 962 (2007) ("[T]he Electronic Communications Privacy Act . fails to protect the employee because it is confusing, poorly drafted, and riddled with holes and exceptions.") (footnote omitted).

156. Cal. Const. art. I, § 1.

or serious interference with his privacy."[157] A number of states have enacted statutes similar to the Electronic Communications Privacy Act, meaning they do not provide any additional levels of privacy protection.[158] One notable exception is the state of Connecticut, which requires employers to notify employees in writing if workplace electronic monitoring takes place.[159] Of course, the statute does not prohibit the act of electronic monitoring.

One area of privacy that a few states have addressed is the installation of two-way mirrors or cameras in dressing rooms, restrooms, shower areas, and/or motel rooms.[160] Many of these statutes expressly prohibit merchants from conducting such surveillance, implying the statutes protect only customers, though they do provide exemptions where there is conspicuous notice that dressing rooms are under surveillance.[161] A few of these statutes, however, also apply to employers. California prohibits the use of cameras in bathrooms without an express limitation to merchants.[162] New York's statute is not limited in language to merchants and expressly prohibits installing or maintaining a two-way mirror or other viewing device by owners and managers.[163] Louisiana's voyeurism statute is included because it is broad enough to encompass anyone, including an employer, who surreptitiously videotapes someone in a bathroom.[164]

A number of states have also passed legislation that prohibits employers from making adverse employment decisions based on employees' off-duty conduct.[165] Most of these statutes, however, are limited to protecting employee use of tobacco or the consumption of a "lawful prod-

157. Mass. Ann. Laws ch. 214, § 1B (2007); *but see* French v. United Parcel Serv., Inc., 2 F.Supp.2d 128, 131 (1998) (holding employer did not violate ch. 214, § 1B by questioning employee about co-worker's excessive drinking in employee's home).

158. *See* David, *supra* note 147, at 329.

159. Conn. Gen. Stat. § 31-48d (2007).

160. *See* Cal. Penal Code § 647(k)(1) (West 2007); Cal. Penal Code § 653n (West 2007) (prohibiting the installation of two-way mirrors); Fla. Stat. Ann. § 877.26 (West 2007); La. Rev. Stat. Ann. ch. 14, § 283 (West 2006); Mass. Gen. Laws ch. 93 § 89 (2007); N.Y. Gen. Bus. Law § 395-b (McKinney 2007); R.I. Gen. Laws § 11-41-26 (2006).

161. *See, e.g.*, N.Y. Gen. Bus. Law § 395-b (McKinney 2007).

162. *See* Cal. Penal Code § 647(k)(1); Cal. Penal Code § 653n; *see also* Cramer v. Consol. Freightways, Inc., 255 F.3d 683, 695-97 (2001), *cert. denied* 534 U.S. 1078 (2002) (holding that collective bargaining agreement that permitted installation of video cameras behind two-way bathroom mirrors violated § 653n).

163. *See* N.Y. Gen. Bus. Law § 395-b(2).

164. *See* La. Rev. Stat. Ann., ch. 14, § 283.

165. *See*, Marisa A. Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. Pa. J. Lab. & Emp. L. 625 (2004) (analyzing the content and application of the various state statutes protecting employee off-duty conduct).

uct."[166] A few of these "off-duty" statutes are more expansive,[167] and represent, on their face, an attempt by the states to protect employee privacy outside of work; however, as discussed below in Part IV, these statutes are quite limited in their application.[168] Beyond the bathroom, states do not provide substantial employee privacy protections apart from the limited federal laws or common law.[169]

IV. WORKPLACE SURVEILLANCE AND EMPLOYEE EXPECTATIONS OF PRIVACY

Employee privacy becomes an employment issue when an employee is disciplined, or, in particular, fired, based on information obtained by the employer through what the employee considers an invasion of privacy. This creates the possibility of a wrongful discharge action by the now former employee against the employer.[170] Most employers hire employees without agreeing to the specific length of employment, standards for continued employment, or conditions for termination. These employment relationships are subject to the employment-at-will doctrine.[171] Under the employment-at-will doctrine, both the employer and the employee may terminate the employment relationship at any time, with or without cause. All states and the District of Columbia, except Montana, have adopted the employment-at-will doctrine.[172] Taken to its extreme, the employment-at-will doctrine means that employers can dismiss employees for arbitrary or irrational reasons: "office politics, nepotism, preference for left-handedness, astrological sign, or their choice of favorite

166. *See id.* at 641.

167. *See id.* at 646-70 (discussing more expansive state statutes that broadly protect off duty conduct).

168. *See infra*, text accompanying notes 245-267.

169. *See, e.g.*, Lewis, *supra* note 155, at 962 ("State constitutional protections rarely apply to private employers, and state statutes either parallel the flawed ECPA or are inapplicable to private employers. In essence, the privacy rights of employees vanish the moment they come in contact with their workplace or employer.") (footnote omitted).

170. Other actions are possible, such as intentional infliction of emotional distress. *See, e.g.*, Johnson v. K-mart Corp., 723 N.E.2d 1192 (2000).

171. *See, e.g.*, Kenneth A. Sprang, *Beware the Toothless Tiger: A Critique of the Model Employment Termination Act*, 43 Am. U. L. Rev. 849, 850 (1994) (citing statistics indicating that two-thirds of private-sector employees are subject to the employment-at-will doctrine); Charles B. Craver, *Privacy Issues Affecting Employers, Employees, and Labor Organizations*, 66 La. L. Rev. 1057, 1057-58 (2006) (noting more recent studies indicating that over ninety percent of private sector employees are not covered under collective bargaining agreements, and are therefore at-will employees).

172. Montana has, by statute, limited employers' ability to discharge employees and preempted common law employment-at-will actions. *See* Mont. Code Ann § 39-2-904(1) (2005).

sports team."[173]

Over time, however, courts have fashioned limits to the application of the employment-at-will doctrine. An employer cannot terminate an at-will employee in violation of public policy, such as violating an employee's right of privacy, or in violation of an employment-related law, such as Title VII of the Civil Rights Act of 1964, which prevents employment discrimination against certain protected classes of individuals,[174] or the National Labor Relations Act.[175] Employees have lower expectations of privacy in the workplace than they do in the home.[176] As discussed previously, employers have compelling reasons to monitor workers in the workplace.[177] Almost as soon as e-mail became an office tool, employees were fired for using it inappropriately.[178] One of the earliest cases involving an inappropriate e-mail is *Bourke v. Nissan Motor Corp., U.S.A.*, in which two employees were fired after their e-mail correspondence, which contained sexual material, was randomly chosen for display during a computer training session.[179] Although the plaintiffs claimed they had a subjective expectation of privacy in their e-mail messages because they were given passwords to access the computer system, the court held they had no objective expectation of privacy in e-mail messages that could be read by others.[180]

The Fourth Amendment protects individuals against warrantless searches or seizures by the government when the individual searched or subject to the seizure has a legitimate expectation of privacy. Legitimate expectations of privacy include government-employer workplaces.[181] Fourth Amendment protections do not directly apply to privately owned entities; therefore private-sector employees have no Fourth Amendment-based privacy protections from their employers. Private-sector employees, however, do have protection through the tort of intrusion upon seclusion. This tort prohibits intentional intrusion upon the private affairs of

173. Robert C. Bird, *Rethinking Wrongful Discharge: A Continuum Approach*, 73 U. Cin. L. Rev. 517, 551, 554 (2004). *But see* Agis v. Howard Johnson Co., 355 N.E.2d 315 (Mass. 1976), for an example of behavior that was so outrageous the employer was liable for the tort of intentional infliction of emotional distress, though not wrongful discharge. In *Agis*, the employer began firing employees in alphabetical order during an investigation of employee theft.

174. *See Harris*, 510 U.S. at 21, *supra* note 26 and accompanying text.

175. *See supra* notes 141- 143, 147 and accompanying text.

176. Vega-Rodriguez v. Puerto Rico Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997).

177. *See infra*, text accompanying notes 23-58.

178. *See, e.g.*, Janice C. Sipior & Burke T. Ward, *The Dark Side of Employee Email*, 42 Comm. ACM 88, 89 (July 1999) (reporting the rise during the 1990s in the use of e-mail to sexually harass someone at work).

179. Bourke v. Nissan Motor Corp., No. B068705 (Cal.Ct.App. 2nd Dist. 1993) (unpublished decision), *available at* http://www.loundy.com/CASES/Bourke_v_Nissan.html.

180. *See id.*

181. *O'Connor*, 480 U.S. at 715.

another "if the intrusion would be highly offensive to a reasonable person."[182]

The tort of intrusion upon seclusion of an employee is similar to the test under the Fourth Amendment's right to privacy. Both require (1) a reasonable expectation of privacy on the part of the employee, and (2) a legitimate purpose for the search on the part of the employer. The tort of intrusion upon seclusion, though, has the additional requirement that the intrusion—by the privately-owned employer—must be highly offensive to a reasonable person.

The most crucial step in determining employee privacy is whether the employee has a reasonable expectation of privacy. The factors in determining workplace expectations of privacy are no different whether the employer is public or private. Though specifically considering public-employer workplace privacy, the U.S. Supreme Court has admitted there is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."[183] Employees' expectations of privacy must be assessed in the context of the employment relationship, and must be addressed on a case-by-case basis.[184]

One justification for a minimized expectation of privacy in the workplace is simply because employees are using the employer's property. The telephones, computer system, desks, and other equipment are all owned or controlled by the employer.[185] There can only be an expectation of privacy in the workplace when it relates to private property the employee is allowed to bring to work, or in any form of seclusion granted to the employee by the employer. For example, the U.S. Supreme Court, in a public-employer scenario, did recognize a legitimate expectation of privacy on the part of an employee in personal effects he was allowed to keep in his desk and file cabinet drawers in an office to which he had exclusive access for seventeen years.[186]

In the private sector, courts have also recognized possible expectations of privacy in a briefcase brought into work by an employee,[187] and in personal contents stored in an employer-provided locker secured by the employee's own lock.[188] However, even where there is a legitimate

182. Restatement (Second) of Torts § 652B (1965). *See also supra,* note 76 and accompanying text.

183. *O'Connor*, 480 U.S. at 715.

184. *See id.* at 717, 718.

185. *See* Findlay & McKinlay, *supra* note 23, at 307 ("The workplace can be considered as a wholly public domain in which any notion of personal privacy is irrelevant and where employers' property rights predominate.").

186. *See O'Connor*, 480 U.S. at 718.

187. *See* Branan v. Mac Tools, No. 03AP-1096, 2004 WL 2361568 at *11 (Ohio Ct. App. 2004).

188. *See* K-mart Corp. v. Trotti, 677 S.W.2d 632, 638 (Tex.Ct.App. 1984).

expectation of privacy, an intrusion by a private employer is not actionable unless the intrusion is also highly offensive to a reasonable person.[189] For example, although the court in *Kmart Corporation v. Trotti* believed the employee had a reasonable expectation of privacy in her personal items she secured with her own lock in an employer-provided locker, the court left it to the fact-finder to determine whether the employer's search of those personal belongings was highly offensive.[190]

The analogy to a secured locker does not necessarily apply, though, to e-mail messages stored in a password-protected personal folder on a work computer. For example, in *McLaren v. Microsoft Corp.*, McLaren claimed his privacy had been invaded when Microsoft employees—as part of an investigation of sexual harassment and "inventory questions"—retrieved e-mail messages McLaren had stored in a password-protected folder located on the hard drive in his office computer.[191] However, McLaren was not storing personal items, but work-related messages. The court also believed a physical locker that stores personal belongings is discreet, unlike an e-mail system where messages are transmitted over a network and which, at some point, are accessible by others.[192] The fact that e-mail messages can be forwarded to anyone with an Internet accessible e-mail address can also defeat any notion of an expectation of privacy in those communications.[193] Expressly following the earlier case of *Smyth v. Pillsbury Co.*,[194] the *McLaren* court concluded that even if McLaren had a reasonable expectation of privacy in the e-mail messages he had stored on his computer, Microsoft's "interest in preventing inappropriate and unprofessional comments, or even illegal activity, over its e-mail system would outweigh McLaren's claimed privacy interest in those communications."[195]

If there is a recognized, legitimate expectation of privacy on the part of the employee, it must be balanced against the reasonableness of the intrusion. In other words, even if the affected employee has a reasonable expectation of privacy in the circumstances involved, the employer may still be justified in intruding upon privacy. Turning back to Fourth Amendment protections (which apply to public employees and help inform the analysis for private workplace actions), employers are not held to the same probable cause standards as for criminal investigations—

189. *See supra*, note 182 and accompanying text.

190. *K-mart*, 677 S.W.2d at 637.

191. McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 at *1 (Tex.App. 1999).

192. *See id.* at *4.

193. *See* Garrity v. John Hancock Mut. Life Ins. Co., 2002 WL 974676 at *1 (D. Mass. May 7, 2002).

194. Smyth v. Pillsbury Co., 914 F.Supp. 97 (E.D. Pa., 1996).

195. *McLaren*, 1999 WL 339015, at *5.

after all, the employer's motivation is the efficient operation of an office, not apprehending criminals.[196] There need merely be a legitimate, reasonable, work-related purpose behind the workplace search.[197] It is in situations in which there is no legitimate business purpose, coupled with an expectation of privacy, that there can be an invasion of privacy. For example, in *Soroka v. Dayton Hudson Corp.*, the court ruled the prospective employer violated applicants' privacy with a 704-question psychological test that asked questions pertaining to religious beliefs and sexual orientation, concluding these issues had no bearing on the requirements of the applied-for job.[198]

Frequently, particularly in the private sector, courts have given deference to the employer's legitimate business needs over any expectations of privacy on the part of employees. One striking example is *Smyth v. Pillsbury Co.*[199] Although Pillsbury assured its employees that their e-mail messages would remain confidential and privileged and employees would not be discharged as a result of their e-mail communications, Smyth was fired because he sent "inappropriate and unprofessional" e-mail messages to his supervisor (criticizing employees in a different department) from his home computer over the company's e-mail system.[200] First, the court found no expectation of privacy in an e-mail message voluntarily sent on the company e-mail system, regardless of the employer's assurances such communications would not be intercepted by management.[201] Secondly, the court concluded, even if Smyth had a legitimate expectation of privacy in his e-mail messages, Pillsbury'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."[202]

The same standards should apply to employer monitoring of Internet use. For example, in *Coniglio v. City of Berwyn*, the court ruled against the defendant-employer's motion to dismiss the plaintiff's sexual harassment claim where a supervisor would purposely display and comment on pornographic Web sites on his office computer when his secretary was present.[203] Therefore, employers have a legitimate business

196. *See O'Connor*, 480 U.S. at 724 (addressing a public employer situation).

197. *See id.* at 725.

198. *See* Soroka v. Dayton Hudson Co. 1 Cal. Rptr. 2d 77, 79, 86 (Cal.App. 4th, 1991). *See also* Johnson, 723 N.E.2d at 1196-97 (reversing summary judgment granted in favor of defendant-employer as to plaintiffs' intrusion upon seclusion claims; holding employer's investigation concerning workplace thefts, vandalism, and drug use went too deeply into personal lives of employees, beyond any business purpose).

199. Smyth v. Pillsbury Co., 914 F.Supp. 97 (E.D. Pa., 1996).

200. *Id.* at 98.

201. *See id.* at 101.

202. *Id.*

203. *See* Coniglio v. City of Berwyn, No. 99 C 4475, 1999 WL 1212190 (N.D. Ill. 1999).

interest in preventing the display of pornographic Web sites in the workplace.

Even when an employee may have an expectation of privacy in the contents of his computer, the employer may still consent to its search by law enforcement officials. For example, in *U.S. v. Ziegler*, the Ninth Circuit Court of Appeals concluded an employee had a reasonable expectation of privacy in his locked office he did not share.[204] However, the court concluded the employee's privacy was not invaded, for Fourth Amendment purposes, when the employer consented to the search of the employee's computer by government agents, "because the computer is the type of workplace property that remains within the control of the employer 'even if the employee has placed personal items in [it].'"[205]

When it comes to monitoring telephone conversations, employees potentially have an additional privacy protection under Title I of the ECPA, which prohibits the intentional interception of a wire or electronic communication (which would include a telephone call).[206] However, there is no violation of Title I if one of the parties to the communication gives prior consent to the interception. Further, there is also what is known as the "business use" exemption under the Act where employers are permitted to intercept phone calls on telephone equipment used in the ordinary course of business.[207]

Courts have determined that employees have an expectation of privacy in personal telephone calls where the employer has made provisions for (or expressly allowed) such calls.[208] But the extent of that expectation of privacy is not absolute—it can still be tied back to the employer's legitimate business interest in monitoring employee conversations. In both *Fischer v. Mt. Olive Lutheran Church* and *Watkins v. L.M. Berry Co.*, applying Title I, the employees' privacy was not invaded simply because the employer monitored a personal phone call after the employer had expressly permitted such calls, rather the invasions occurred when the employers continued to monitor the conversations after it became obvious they were personal. In other words, there was no legitimate business purpose in continuing to monitor the phone calls.[209] Courts have also found invasions of privacy under Title I where employers could not justify with a legitimate business purpose the continuous monitoring of employee telephone calls twenty-four hours a day, seven days per

204. United States v. Ziegler, 474 F.3d 1184, 1189-90 (9th Cir. 2007).

205. *Id.* at 1191 (quoting *O'Connor*, 480 U.S. at 716).

206. 18 U.S.C. §§ 2510-2520 (2007).

207. Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994).

208. *See, e.g. Fischer*, 207 F.Supp.2d 914; *see also* Watkins v. L.M. Berry Co., 704 F.2d 577 (11th Cir. 1983).

209. *See Fischer*, 207 F. Supp. 2d at 923; *Watkins*, 704 F.2d at 583-84.

week.[210]

Title I, because of its specificity, offers greater privacy protection for employee telephone calls versus video surveillance. Recall that in *Nelson v. Salem State College*, the court was unconcerned with why the employer was video recording an office twenty-four hours per day when the purpose of the video surveillance was to thwart after-hours thefts.[211] In particular, courts have rejected the argument that electronic surveillance should be limited to what management can see with the naked eye; constant video surveillance of an open work area is permissible.[212]

There have been a few instances where courts have recognized a possible expectation of privacy in an employee's personal information accessed by an employer. For example, in *Campbell v. Woodard Photographic,* the court held that if the employee (suspected of stealing equipment from the employer) could establish that the employer had accessed the employee's personal e-Bay account (using the employee's employer-provided computer), or had reviewed the employee's e-Bay transactions by searching his briefcase, he could establish an actionable invasion of privacy claim.[213] In a public employer environment, one court held that a government employee had a reasonable expectation of privacy in personal information stored on an employer-owned computer where the employee had exclusive access to the computer in an exclusive office, and computer maintenance personnel had only previously accessed the computer on an as-need maintenance basis.[214]

In addition, courts and legislatures appear ready to draw a line when it comes to video surveillance of bathrooms. Not accounting for a handful of state statutes that may be applicable to employers,[215] at least one court has held that bathroom surveillance, despite being incorporated into a collective bargaining agreement, constituted an invasion of privacy.[216]

---

210. *See, e.g.* Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992); *Sanders*, 38 F.3d 736.

211. Webb v. Edwards, 845 N.E.2d at 535; *see also supra* notes 105-106 and accompanying text.

212. *Vega-Rodriguez*, 110 F.3d at 180.

213. *See* Campbell v. Woodard Photographic Inc., 433 F. Supp. 2d 857, 861 (N.D. Ohio 2006).

214. *See* Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001).

215. *See id. at*, notes 160-164 and accompanying text.

216. *See Cramer*, 255 F.3d at 695-97 (holding terms of collective bargaining agreement allowing employer to install cameras behind two-way bathroom mirrors violated California's law prohibiting use of two-way mirrors, Cal. Penal Code § 653n); *see also* Michael Selmi, PRIVACY FOR THE WORKING CLASS: PUBLIC WORK AND PRIVATE LIVES, 66 La. L. Rev. 1035, 1049 (2006) (suggesting that bathrooms remain a core area of privacy protection).

V. EMPLOYER MONITORING AND EMPLOYEE EXPECTATIONS OF PRIVACY OUTSIDE THE WORKPLACE

Initially, although it was accepted that there was essentially no privacy in the workplace, it was assumed there was still at least privacy at home.[217] Commentators now fear, however, that the home/work dichotomy is disappearing. Technology has facilitated the broadening of the definition of "on the job" to include areas far beyond the traditional confines of office space.[218]

> Developments in the nature of work and organization are . . . blurring the boundary between work and home, between public and private. It is becoming more difficult to distinguish clear and unambiguous boundaries between work and private life as people work longer hours, work from home on computers owned by their employer, and work on call.[219]

The commingling of home and work also results from the growth in telecommuting (also referred to as teleworking).[220] A growing number of employees now work in a virtual workplace, not in the office, but on the road or at home.[221] Since there is less face-to-face interaction among

---

217. *See* Garson, *supra* note 18, at 220-21.

218. *See* JILL A. FRASER, WHITE-COLLAR SWEATSHOP 75 (W.W. Norton & Co. 2001).

219. Findlay & McKinlay, *supra* note 23, at 307; *see also* Rosen, *supra* note 43, at 84 ("The Internet has blurred the distinction between the home and the office, as Americans are spending more time at the office and are using company-owned computers and Internet servers to do their work from home."); Carol Hymowitz, *Personal Boundaries Shrink as Companies Punish Bad Behavior*, WALL ST. J., June 18, 2007, at B1 (noting that one reason companies are taking more interest in their workers' personal behavior is because of "the increasingly blurred line between work and home"); Rachel Konrad, *IBM Rules Govern Workers in Virtual Worlds*, MSNBC.com, July 26, 2007, http://www.msnbc.msn.com/id/19982107/ (discussing reaction to IBM instituting rules for its employees who use Second Life, an online virtual community; although the employees use Second Life for business purposes, concern was expressed that since Second Life users have multiple personas (avatars), there is the propensity for confusion between personal and professional use); Rob Pegoraro, *Friend? Not? It's One or the Other*, WASH. POST, July 19, 2007, at D1 (discussing the rise in the use by companies of social networking sites, resulting in workers having difficulty differentiating between their private and professional personas on such sites); *Bosses Do Not Always Make Best Online Pals*, Interview with Lucy Kellaway, Columnist, Fin. Times, Natl. Pub. Radio Morning Ed., July 25, 2007, *available at* http://www.npr.org/templates/story/story.php?storyId-12218559 (transcript on file with author) (discussing use of Facebook social networking site by employers to communicate with employees, merging the workplace with personal online use; stating that "we actually may reach the situation where we're all much more tolerant about what people get up to in their private lives, because everyone's doing it").

220. *See* Michelle A. Travis, *Equality in the Virtual Workplace*, 24 BERKELEY J. EMPL. & LAB. L. 283, 289-90 (2003) (describing telecommuting and telework).

221. *See id.* at 292 (noting that by the end of the twentieth century, nearly 10% of the U.S. workforce were telecommuters); Joan T.A. Gabel & Nancy R. Mansfield, *The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyber-*

workers, there is a greater reliance on electronic communications.[222]

Do employees have any legally recognized privacy interests in a company-provided computer that is used at home? Not at Harvard. In 1998, the dean of the Harvard Divinity School resigned after a technician performing routine maintenance on a university-owned computer located in the dean's residence discovered pornographic images stored on the computer.[223] Similarly, the court in *TBG Insurance Services Corp. v. Superior Court* found no reasonable expectation of privacy on the part of an employee in an employer-provided computer used for business and personal purposes in the employee's home.[224] Indeed, the court stated that in light of the employee's agreement to be bound by the employer's electronics policy statement, and in light of the fact that the home computer belonged to the employer, the employee "could not *seriously* claim that he had a reasonable expectation of privacy when he used it for personal matters."[225] Just as courts have recognized that electronic communications are not necessarily discreet,[226] one court has held that an employer-sponsored electronic bulletin board not physically located at the workplace can nonetheless be an extension of the workplace.[227]

If an employee were to maintain a personal Web site that restricted access to authorized users, one would expect a reasonable expectation of privacy on the part of the employee as to his or her employer. The Stored Communications Act (SCA), which protects stored electronic communications from unauthorized access, would appear to support that expectation of privacy.[228] In *Konop v. Hawaiian Airlines, Inc.*, the plaintiff, a pilot employed by the defendant, maintained a Web site that contained commentary critical of the defendant's management practices.[229] Konop's Web site required users to have an assigned username and password in order to access the site, and Konop maintained a list of authorized users, which consisted primarily of other Hawaiian Airline employees.[230] A Hawaiian Airlines senior manager (a vice president who did not have authorized access to the Web site) used other pilots' usernames and passwords (with their permission) to access the Web

---

space Workplace, 40 AM. BUS. L.J. 301, 302 (2003) (noting estimates that the number of people working from home would rise to 40 million by 2004).

222. *See* Wayne F. Cascio, *Managing a Virtual Workplace*, 14 ACAD. MGMT. EXECUTIVE 81 (2000).

223. *See* Fox Butterfield, *Pornography Cited in Ouster at Harvard*, N.Y. TIMES, May 20, 1999, at A21.

224. *See* TBG Ins. Servs. Corp. v. Super. Ct., 117 Cal. Rptr. 2d at 160.

225. *Id.* at 158 (emphasis added).

226. *See supra* note 192 and accompanying text.

227. *See* Blakey v. Cont'l Airlines, Inc., 751 A.2d 538, 543 (N.J. 2000).

228. *See supra* notes 152-154 and accompanying text.

229. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872 (9th Cir., 2002).

230. *See id.*

site.[231] Because the manager had used other authorized users' accounts, with their permission, to access the Web site, it would appear the manager had not violated the SCA.[232] However, the court concluded the manager did violate the SCA, but only because the authorized user accounts used by the manager had never been actually used by the authorized users—therefore, under a strict reading of the statute, the manager did not have the permission of an authorized "user."[233]

The SCA also does not appear to protect an employee's personal e-mail account from a prying employer. In *Fischer v. Mt. Olive Lutheran Church Inc.*, Fischer's employer, during an investigation into possible misconduct by Fischer, accessed his personal Microsoft Hotmail account without authorization.[234] The court concluded, however, that the employer did not violate the SCA merely by its unauthorized access. The "[p]laintiff must also show that defendants obtained, altered or prevented his authorized access to his email account."[235]

In addition, the SCA exempts seizures by providers of electronic communications services.[236] Two courts have interpreted this language to exempt employers who provided the e-mail system from which the messages were retrieved.[237]

An employee may also reasonably believe that an employer could not take adverse employment actions against the employee based on a personal phone call occurring in her home. In *Karch v. Baybank FSB*, neighbors overheard a telephone conversation on their radio scanner between Karch and her friend, a co-worker, which took place on a Saturday evening, during non-work hours, involving mostly personal matters; however, some work-related comments were overheard.[238] The neighbors turned over a recording of the conversation to Karch's employer, and Karch was initially reprimanded and had a note inserted into her personnel file admonishing her to "'limit her conversations regarding personal situations with [bank] personnel as well as customers.'"[239] Karch ultimately resigned, claiming her workplace became hostile.[240]

---

231. *See id.* at 873.

232. *See id.* at 880.

233. *See id.*

234. *See S.E.C. v. Bennett & Co.*, 207 F.Supp. at 920 (Although Fischer did access his Hotmail account through the employer's Internet service provider, that fact did not appear to influence the court's conclusions.).

235. *Id.* at 926. *But see*, *supra* notes 89-90 and accompanying text.

236. *See* 18 U.S.C. § 2701(c)(1) (2001).

237. *See* Bohach v. City of Reno, 932 F.Supp. 1232, 1236 (D. Nev. 1996) (applying interpretation to public employer); Fraser, 352 F.3d at 114-15 (applying interpretation to private employer).

238. *See* Karch v. Baybank, 794 A.2d 763, 768 (N.H. 2002).

239. *Id.* at 769.

240. *See id.*

The Supreme Court of New Hampshire upheld the lower court's dismissal of Karch's claim against her employer for invasion of seclusion, ruling that it was the neighbors who had potentially intruded upon Karch's seclusion, not the Bank (and particularly the officer) who had received the information and then acted upon it.[241]

Employers have also been found to have not invaded employee privacy when they inquire into off-duty conduct among co-workers. For example, in *French v. United Parcel Service, Inc.*, the court ruled the employer had not violated an employee's privacy by questioning the employee about a co-worker's excessive drinking in the employee's home.[242] The court held "there are circumstances in which it is legitimate for an employer to know some 'personal' information about its employees, so long as the information reasonably bears upon the employees' fitness for, or discharge of, their employment responsibilities."[243] The court concluded that the employer had "articulated legitimate business reasons for seeking information about the [drinking] incident, including concerns about the soundness of judgment exercised by its supervisory employees in regard to alcohol abuse generally as well as in a particular setting where all participants were . . . employees."[244]

These cases exemplify how off-duty conduct by employees may still be subject to some form of monitoring by their employers. State legislatures have addressed the notion that employees' off-site, off-hours conduct should be free from employer scrutiny. Most of this legislation protects employees' consumption of lawful products, particularly tobacco.[245] Typical language contained in the broader of these "consumption" statues is exemplified by Montana's statute, which provides that an employer "may not discriminate against an individual with respect to compensation, promotion, or the terms, conditions, or privileges of employment because the individual legally uses a lawful product off the employer's premises during nonworking hours."[246] Arguably, for example, an employer in Minnesota could not take an adverse employment action against an employee because of the employee's off-duty legal consump-

241. *See id.* at 773.

242. *See* French v. United Parcel Serv., Inc., 2 F. Supp. 2d 128, 131 (D. Mass, 1998) (applying Mass. Ann. Laws ch. 214, § 1B).

243. *Id.* (citation omitted).

244. *Id.*

245. *See generally* Pagnattaro, *supra* note 165 (discussing and analyzing "off-duty" statutes); *See also* Jason Bosch, *None of Your Business (Interest): The Argument for Protecting All Employee Behavior With No Business Impact*, 76 S. CAL. L. REV. 639, 654-58 (2003) (describing the nature and benefits of "lifestyle protection statutes.")

246. Mont. Code Ann. § 39-2-313(2) (2007). For an example of a tobacco-specific statute, *see* Wyo. Stat. Ann. § 27-9-105(a)(iv) (Michie 2007) (prohibiting, in part, employers from requiring "as a condition of employment that any employee or prospective employee use or refrain from using tobacco products outside the course of his employment. . . .")

tion of alcohol, because Minnesota's statute specifically includes alcoholic beverages as a "lawful consumable product."[247]

A few of these "off-duty" statutes (in California, Colorado, Connecticut, New York, and North Dakota) go beyond just lawful consumable products and protect off-duty conduct in general. However, despite the broad language of these statutes, their actual application reveals their limitations.

In California, section 96(k) of the California Labor Code authorizes the Labor Commissioner to take assignments of "[c]laims for loss of wages as the result of demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer's premises."[248] A plain reading of California's "lawful conduct" statute indicates there is no limitation to the type of lawful conduct protected. In *Barbee v. Household Automotive Finance Corp.*,[249] the California Court of Appeal rejected an employee's claim that his employer violated his (state) constitutional right of privacy[250] when the employer discharged him as a result of his intimate relationship with a co-worker.[251] The court concluded the employee had no reasonable expectation of privacy as to the relationship because he was on notice of the employer's policy discouraging such relationships and the employer was aware of the relationship.[252] The employee in *Barbee* claimed that his employer's conduct violated section 96(k) because the intimate relationship with the co-worker took place during nonworking hours away from the employer's premises.[253] The court rejected this claim, holding that section 96(k) "does not set forth an independent public policy that provides employees with any substantive rights, but rather, merely establishes a procedure by which the Labor Commissioner may assert, on behalf of employees, recognized constitutional rights."[254] With no expectation of privacy, the employee had no invasion of privacy claim, and hence no claim, despite the action involving allegedly lawful conduct occurring during nonworking hours away from the employer's premises.

Colorado has enacted legislation that also prohibits an employer from terminating "the employment of any employee due to that employee's engaging in any lawful activity off the premises of the employer

247. Minn. Stat. Ann. § 181.938(2) (West 2007). *see also* Pagnattaro, *supra* note 165, at 643.

248. Cal. Lab. Code § 96(k) (West 2007).

249. Barbee v. Household Auto. Fin. Corp., 6 Cal. Rptr. 3d 406 (Cal.Ct.App. 2003).

250. *See supra* note 156 (the *Barbee* court stated that California's constitutional privacy provision applies to private, as well as public, actions), *see* Barbee 6 Cal. Rptr. 3d at 410.

251. *See id.* at 411.

252. *See id.* at 411-12.

253. *See id.* at 412.

254. *Id.*

during nonworking hours . . . ."[255] However, Colorado's "lawful activity" restriction does not apply if the activity "[r]elates to a bona fide occupational requirement or is reasonably and rationally related to the employment activities and responsibilities of a particular employee . . . ."[256] Therefore, in *Marsh v. Delta Air Lines, Inc.*, the U.S. District Court ruled that an employer did not violate Colorado's statute when it dismissed an employee who had written a letter critical of management that was published in a newspaper.[257] The court held that the employee owed his employer a duty of loyalty, which the employee breached by trying to settle publicly a private dispute with management.[258]

Connecticut's "off-duty" statute is limited to protecting employees who exercise state or federal first amendment rights.[259] At least as applied to free speech rights, courts have limited application of Connecticut's statute to speech relating to matters of public concern, and "internal employment policies are not a matter of public concern."[260]

The state of New York has adopted legislation that prohibits employers from discriminating against employees on the basis of their legal political activities, legal use of consumable products, and legal recreational activities—all off-site, outside of work hours without the use of the employer's equipment or other property.[261] The statute specifically excludes, however, any activity which "creates a material conflict of interest related to the employer's trade secrets, proprietary information or other proprietary or business interest. . . ."[262] To date, the majority of cases dealing with the "recreational activities" portion of the statute have defined recreational activities as not including romantic relationships or extramarital affairs,[263] although the Supreme Court, Appellate Division has ruled that an employee who was terminated as a result of a discussion during recreational activities (dinner at a restaurant) outside of the workplace in which her political affiliations became an issue, stated a cause of action for a violation of the state's statute.[264]

---

255. Colo. Rev. Stat. Ann. § 24-34-402.5(1) (West, Westlaw through 2008 legislation).

256. *Id.* at § 24-34-402.5(1)(a).

257. *See* Marsh v. Delta Air Lines, Inc., 952 F.Supp. 1458, 1462 (D.Colo. 1997).

258. *See id.* at 1463.

259. Conn. Gen. Stat. Ann. § 31-51q (West 2007); *see also* Pagnattaro, *supra* note 165, at 669.

260. *See, e.g.* Daley v. Aetna Life & Cas. Co., 734 A.2d 112, 112-13 (Conn. 1999).

261. *See* N.Y. Lab. Law § 201-d(2)(d) (McKinney 2007).

262. *Id.* at § 201-d(3)(a).

263. *See, e.g.* State v. Wal-Mart Stores, Inc., 621 N.Y.S.2d 158 (N.Y. App. Div. 1995) (finding that legislative history of statute forbidding employer discrimination against employees excluded dating relationships from the definition of leisure activities); McCavitt v. Swiss Reinsurance Am. Corp., 237 F.3d 166 (2d Cir. 2001) (finding same).

264. *See* Cavanaugh v. Doherty, 675 N.Y.S.2d 143 (N.Y. App. Div. 1998).

North Dakota's statute prohibits discrimination by an employer, in part, based on an employee's "participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer."[265] In the only case interpreting this language, the Supreme Court of North Dakota ruled it was a disputed issue of fact whether a chaplain who was discovered engaging in unseemly behavior in a Sears store bathroom was terminated for participating in lawful activity off the employer's premises during nonworking hours.[266]

An important theme running throughout the "lawful product" and "off-duty conduct" statutes is that the products or activities must be completely divorced from the employer—they must take place (or be consumed) off-site, during non-working hours, and have no relationship to the employer's interests. In other words, the statutes do not apply if a legitimate business interest of the employer is involved. This is similar to the analysis used in intrusion upon seclusion cases: even if an employee has a reasonable expectation of privacy, it can be overridden by legitimate employer interests.[267] It is arguable, therefore, that as long as the employer can establish a legitimate business interest in offsite monitoring, it will defeat any claim of invasion of privacy.

If one examines the cases in which employers have been found to have (at least potentially) invaded an employee's privacy, it is usually because the employer has pried into the employee's private life far beyond a legitimate business need. Recall that in cases involving an invasion of privacy when an employer listened to an employee's allowed personal call, the intrusion occurred when the employer continued to listen to the call after the employer knew it was a personal call,[268] or simply could not justify continuous monitoring with a legitimate business need.[269]

With the merger of office and home life,[270] employers can more easily argue for a business need in monitoring employee conduct offsite. Even before considering the employer's legitimate need for monitoring, the employee still must first have a reasonable expectation of privacy. Commentators believe individuals are living more and more within the Omnipticon,[271] under constant surveillance from a number of sources. Not only may our actions be recorded and posted on the Internet by any-

265. N.D. Cent. Code § 14-02.4-03 (2005).

266. *See* Hougum v. Valley Mem'l Homes, 574 N.W.2d 812, 820 (N.D. 1998).

267. *See, e.g. Smyth*, 914 F.Supp. at 101.

268. *See supra* note 209 and accompanying text.

269. *See supra* note 210 and accompanying text.

270. *See supra* notes 218-222 and accompanying text.

271. *See supra* notes 10-11 and accompanying text.

one with a camera phone we happen to come across,[272] we are also under increasingly more formal surveillance.[273]

There has been some pushback. For example, people expressed concern when Google introduced a new photo mapping service with digital images so clear users could discern details inside windows of homes located near photographed intersections.[274] Internet search services have been bowing to privacy concerns by limiting the amount of information they collect from user searches.[275]

But the technological trends are promising increased surveillance. Global Positioning System (GPS) technology allows employers "to watch everybody all the time and scrutinize every movement."[276] Many cell phones are GPS-enabled, allowing employers to track the whereabouts of the phones they provide to employees, as well as the employees carrying those phones.[277] The same can be said for company-provided cars that include a GPS tracking device.[278] Employers may soon be using radio frequency identification (RFID) chips to constantly monitor the whereabouts of their employees, whether at home or in the office.[279]

VI. CONCLUSION

Determining whether an employer has invaded an employee's privacy involves a balancing between the employee's reasonable expectation of privacy and the employer's legitimate business need for the intrusion (plus the added requirement under the tort of intrusion upon seclusion that the intrusion must be highly offensive to a reasonable person). Historically, courts have considered employees to have minimal expectations of privacy in the workplace, particularly when the employer publishes policies pertaining to workplace monitoring and surveillance.

---

272. *See supra* note 11 and accompanying text.

273. *See, e.g.* Cara Buckley, *Police Plan Web of Surveillance for Downtown*, N.Y. TIMES, July 9, 2007, at A1 (discussing a planned 3,000 camera-based surveillance system in New York City, including the ability to read automobile license plates); Electronic Privacy Info. Center, Spotlight on Surveillance, May 2005, http://www.epic.org/privacy/surveillance/spotlight/0505/ (discussing Department of Homeland Security grants to various cities used to install camera surveillance networks).

274. *See* Miguel Helft, *Google Zooms in Too Close for Some*, N.Y. TIMES, June 1, 2007, at C1.

275. *See* Ellen Nakashima, *Search Engines Tighten Privacy*, WASH. POST, July 24, 2007, at D1.

276. Yung, *supra* note 13 at 165.

277. *See id.* at 173.

278. *See id.*

279. *See, e.g.* Todd Lewan, *Chips: High Tech Aids or Tracking Tools?*, ABC News, July 24, 2007, http://www.abc.news.go.com/Technology/wireStory?id=3402044 (discussing two employees of a provider of surveillance equipment injecting RFID tags into themselves to demonstrate "chipping" as a surveillance technique).

Even when courts have acknowledged a reasonable expectation of privacy, they have deferred to the legitimate business interests of the employer. As home and work life have merged, compounded by technological advancements that permit ever-greater levels of continuous surveillance, minimized work-related expectations of privacy are invading employees' lives outside the traditional workplace. Even when state legislatures have attempted to extend employee privacy protection to off-hours and off-site activities, those laws invariably defer to legitimate business interests. As long as an employer can assert some form of legitimate business interest, the current legal environment in the U.S. is conducive to allowing employers to monitor more and more of their employees' offsite, personal activities.