2009

Workplace Privacy: We'll Be Watching You

Lisa Smith-Butler, *Charleston School of Law*

Ohio Northern University
Law Review

Articles

Workplace Privacy: We'll Be Watching You

LISA SMITH-BUTLER*

I. INTRODUCTION

Privacy and information dominate conversations today. Individuals bemoan the lack of privacy resulting from intrusive camera cell phones and self publication via blogs.[1] Today it seems as though everyone is a writer, thinker or photographer.[2] People post their photos, thoughts and beliefs on the Internet, making formerly private information available to anyone in the world.[3] Despite this self publication and promotion, people are often surprised when prospective employers, current employers, friends, lovers, and others view the information, making decisions, sometimes adverse, and acting upon these decisions.[4]

---

* Lisa Smith-Butler is the Assistant Dean and Director & Associate Professor of Law, Law Library & Technology Center, Nova Southeastern University, Shepard Broad Law Center, Ft. Lauderdale, FL. A draft of this paper was presented on Nov. 3, 2007 at the Stetson University School of Law Junior Faculty Forum in Gulfport, FL. Many thanks to all colleagues there who listened and offered suggestions.

1. Thomas L. Friedman, *The Whole World is Watching*, N.Y. TIMES, June 27, 2007, at A23.
2. *Id.*
3. *See id.*
4. Harry A. Valetk, *Off the Clock: Should Your Personal Online Chronicles Jeopardize Your Career*, LAW.COM, Feb. 5, 2008, http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1202136231178; *see* PEW INTERNET & AMERICAN LIFE PROJECT, DIGITAL FOOTPRINTS: ONLINE IDENTITY MANAGEMENT AND SEARCH IN THE AGE OF TRANSPARENCY (Dec. 16, 2007), *available at* http://www.pewinternet.org/pdfs/PIP_Digital_Footprints.pdf. This report indicates that 60% of "internet users say they are not worried about how much information is available about them online." *Id.* at ii. Despite this optimism, the evolution of negative online information has resulted in the creation of a new product or service that helps defend online reputations. *See* Reputation Defender, http://www.reputationdefender.com (last visited Sept. 17, 2008).

Employees and employers also share concerns about sensitive employer and employee information. Reports of laptops lost by employees, containing confidential employee information, such as social security numbers, are numerous.[5] These data losses place employees at risk for identity theft. Employers then worry that employees will disseminate confidential or propriety information as well as render the employer liable for comments made via e-mail or other computer abuses.[6]

Individuals and organizations are reeling from information overload, worried about identity theft, and trying to probe the boundaries of privacy in the Information Age. Employee expectations of privacy in the workplace, as well as employee concern about employer-collected information, pervade the workplace today.[7]

To understand these concerns, an examination of the definition and etymology of *privacy* and *information* is necessary. In the Information Age, privacy and information are closely intertwined concepts. According to the Oxford English Dictionary, one definition of *privacy* is "[t]he state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; freedom from interference or intrusion."[8] The entry's etymology indicates that the word first entered the English language around 1450.[9] Shakespeare introduced it to Elizabethan audiences in 1598 in

---

5. For a review of public reports of employee or perspective employee data loss in the U.S. since Jan. 10, 2005, see the Privacy Rights Clearinghouse list of data breaches. Privacy Rights Clearinghouse, *A Chronology of Data Breaches*, *available at* http://www.privacyrights.org/ar/ChronDataBreaches.htm# Total (last visited Sept. 17, 2008). According to this site as of September 15, 2008, there have been 244,829,751 breaches of an individual's data since January 10, 2005. *See id.* The problem is not limited to the U.S. *See* Rosalie Marshall, *MoD Breach Puts More Data At Risk*, IT WEEK, Feb 12, 2008, *available at* http://www.itweek.co.uk/itweek/news/2209452/personal-details-potentially (last visited Sept. 17, 2008). In the United Kingdom, Britain's Ministry of Defense (MoD) recently lost the personal details of more than 200 UK soldiers. *See id.*

6. *See* Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super Ct. App. Div. 2005). Jane Doe sued a corporation, alleging that the corporation was negligent for failing to monitor her ex-husband's e-mail and Internet usage. Jane Doe's ex-husband was an XYC Corp. employee. According to Ms. Doe, had XYC Corp. monitored her ex-husband as their office policy actually stated, her ex-husband would have been unable to send nude pictures of his then ten year old step-daughter over the Internet to pedophilia sites. *Id.* at 1158. Ms. Doe also argued that XYC Corp. was aware that her ex-husband was viewing pornography on his work computer prior to his arrest for child molestation. *Id.* at 1159. Given these facts, Ms. Doe argued that XYC Corp. breached its duty to her which resulted in harm to her daughter. *XYC Corp.*, 887 A.2d at 1158. While the Court did not hold XYC Corp. liable, it did reverse the lower court's summary judgment for XYC Corp., remanding to the lower court to resolve the issue of "harm proximately caused by defendant's breach of duty." *Id.* at 1170.

7. *See, e.g.*, *Personal Data Privacy Ordinance: A Draft Code of Practice on Monitoring and Personal Data Privacy at Work*, OFFICE OF THE PRIVACY COMM'R FOR PERS. DATA, H.K., *available at* www.pcpd.org.hk/english/ordinance/files/consult_paper.doc (last visited Oct. 26, 2008).

8. OXFORD ENGLISH DICTIONARY 515 (2d ed. 1989), *available at* http://dictionary.oed.com.

9. *Id.*

The Merry Wives of Windsor.[10] The word *information* first appeared in the English language via literature.[11] Geoffrey Chaucer used the word in 1386 in his *Canterbury Tales.*[12] Today the Oxford English Dictionary defines *information* as "[t]he action of informing . . . 'news' of some fact or occurrence; the action of telling or fact of being told something."[13]

While privacy concerns itself with containment and isolation, information fosters the dissemination of knowledge, events, or facts among many. These two concepts frequently clash today; the conflict is exacerbated by modern technology. In the workplace, the mixture can be explosive.[14] As individuals, organizations, institutions, and governments ponder the crossroads of privacy, information and technology, former Sun Microsoft Systems CEO, Scott McNealy, has words for everyone: "You have zero privacy. Get over it."[15]

While dealing with privacy concerns, individuals and institutions are also dealing with information overload.[16] Improved technologies have made the collection, collation and dissemination of data on individuals and organizations easy to manage, quick to obtain, and cheap to acquire.[17] Massive amounts of data are collected, stored and transferred among networks.[18] To ascertain relevancy, someone must then sift through this data. Consequently, individuals worry about the data being collected by companies, businesses, employers, neighbors, and the government. What is being collected? Why is it being collected? How is it being used?[19]

Thus information, its generation, collection, and dissemination, plays an enormous role in the Twenty-first Century. Just as the Gutenberg Press helped usher in the Industrial Revolution,[20] the Internet is playing a large role

---

10. *Id.*

11. *See id.* at 944.

12. *Id.* at 944.

13. *See* OXFORD ENGLISH DICTIONARY, *supra* note 8, at 944.

14. *Privacy under Siege: Electronic Monitoring in the Workplace*, Nat'l Working Rights Institute, (2008) http://www.workrights.org/issue_electronic/NWI_EM_Report.pdf.

15. A. Michael Froomkin, *Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy*, 52 STAN. L. REV. 1461, 1462 (2000) (quoting Sun Microsoft Systems, Inc. CEO, Scott McNealy).

16. Stephen J. Adler, *A Businessweek for a Busier World*, BUS. WK., Oct. 22, 2007 at 8.

17. Danielle Kent Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. CAL. L. REV. 241, 246-49 (2007).

18. *See id.*

19. Information that is collected by the federal government is governed by the PRIVACY ACT OF 1974, 5 U.S.C. § 552(a) (2007). Consumer privacy involving banking is governed by the privacy provisions of the GRAMM-LEACH-BLILEY ACT, 12 U.S.C. § 1811 (2007).

20. BARBARA J. SHAPRIO, A CULTURE OF FACT: ENGLAND-1550-1720 86-89 (Cornell Univ. Press 2000).

in the development of the Information Revolution.[21] Why is the Information Revolution so important? The Information Revolution[22] impacts global economies, world governments, multi-national conglomerates, and ultimately individuals and their personal decisions.[23] How does it create such an impact? Access to information informs and drives decisions. Today access to information has been democratized, making it easy and relatively inexpensive for anyone to obtain.[24] As an example, Richard Saul Wurman reflected in his groundbreaking work, *Information Anxiety*, that a person receives and accesses more information today than a Seventeenth Century individual received in his or her entire lifetime.[25]

Because of its importance, the collection, storage, and retrieval of information generates concerns and raises the following questions:

- Who will access this information?
- How much access will be available to others?
- Will there be restrictions?
- If so, how will the restrictions be decided and enforced?
- How will the information be safely stored?
- How will the information be retrieved?
- Can the information be safely transferred?
- What technologies will be employed to acquire the information?
- Will the employee be aware that data is being gathered?
- How will this information be used?[26]

Concerns about information collection, retrieval and dissemination are plentiful in the employment sector on both the part of the employee and the employer.[27] Important private information, such as medical records, work

---

21. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION 18-20 (Yale Univ. Press 2007).

22. *See* Jessica T. Mathews, *The Information Revolution*, 119 FOREIGN POL'Y 63, 63-65 (2000) (defining Information Revolution).

23. *See* THOMAS C. FRIEDMAN, THE WORLD IS FLAT (Farrar, Strauss & Giroux 2005) (discussing information and its impact on society); *see also* Joan T. Gabel & Nancy R. Mansfield, *The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace*, 40 AM. BUS. L.J. 301, 301-04 (2003) (discussing the impact of the Information Revolution on the work force).

24. ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 183-186 (Harper Collins 1994).

25. *See* RICHARD SAUL WURMAN, INFORMATION ANXIETY 34-36 (Doubleday 1989).

26. BARBARA S. MAGILL, WORKPLACE PRIVACY: REAL ANSWERS AND PRACTICAL SOLUTIONS 135-162 (2d ed. Thompson 2007); *see* Victor Schachter & Shawna Swanson, *Workplace Privacy and Monitoring: New Developments Affecting the Rights of Employers and Employees in* PRACTICING LAW INSTITUTE'S 7TH ANNUAL INSTITUTE ON PRIVACY LAW: EVOLVING LAWS AND PRACTICES IN A SECURITY DRIVEN WORLD 135, 142, 159-170 (2006), *available at* 866 PLI/PAT 135 (Westlaw).

27. *See, e.g.*, Schachter & Swanson, *supra* note 26, at 142, 159-70.

history, salary history, performance evaluations, individual disabilities, drug and alcohol screen results, garnishments, tax withholdings, names of dependents, social security numbers and other very private information is often stored in an individual's personnel file at work.[28] Employees are very concerned about the protection of this type of data.[29] Employers too have concerns. They trust employees with confidential information, such as trade secrets and financial information. Employers also provide employees with access to tools, such as e-mail, the Internet, telephones, or vehicles, that can create liability if handled incorrectly or improperly by an employee. To avoid liability and ensure employee productivity, Employers often monitor employees in the workplace arena with a variety of technologies.[30]

Consequently, workplace privacy and data security is a global issue.[31] In Europe, the European Union has the 1996 Data Protection Directive,[32] which provides for comprehensive as opposed to patchwork "protection of personal information maintained by a broad range of entities."[33] In Europe, privacy is treated as an aspect of a fundamental right, i.e. human dignity, which is collectively owned by the community and bestowed by the community upon individuals;[34] whereas in the United States, privacy is treated as an individual right that can be bargained away in employment negotiations.[35] Not only do the philosophical origins differ. Comprehensiveness of legislation differs as does the approach of balancing the rights of employees and employers. While Europe has comprehensive coverage, the United States has a patchwork of

---

28. *Id.* at 116-17, 125-26.

29. DAVID M. SAFON, WORKPLACE PRIVACY: REAL ANSWERS AND PRACTICAL SOLUTIONS 115-21 (Thompson 2001).

30. Leonard Court, *The Workplace Privacy Myth: Why Electronic Monitoring Is Here to Stay*, 29 OKLA. CITY U.L. REV. 15, 15-18 (2004); *see also* Matthew E. Swaya & Stacey R. Eisenstein, *Emerging Technology in the Workplace*, 21 LAB. LAW. 1, 9-10 (2005).

31. *See, e.g.*, Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC). This directive was updated in 2002. Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

32. Council Directive 1995/46, 1995 O.J. (L 281) 31 (EC). This directive was updated in 2002. Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

33. Daniel J. Solove, *The Origins and Growth of Information Privacy Law in* PRACTICING LAW INSTITUTE'S 6TH ANNUAL INSTITUTE ON PRIVACY LAW: DATA PROTECTION—THE CONVERGENCE OF PRIVACY AND SECURITY 64 (2005) *available at* 828 PLI/PAT 23 (Westlaw).

34. Marsha Copa Huie, Stephen F. Laribee, & Stephen D. Hogan, *The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues*, 9 TULSA J. COMP. & INT'L L. 391, 456-59 (2002). According to the authors, this concept was developed and extracted from decisions by the European Court of Justice. *See* Stauder v. City of Ulm, 1969 E.C.R. 419 and Internationale Handelsgesellschaft GmbH v. Einfuhr-under Vorrafsstelle st., 1970 E.C.R. 1125.

35. Gail Lasprogata, Nancy J. King, & Sukanya Pillay, *Regulation of Electronic Monitoring: Identifying Fundamental Principles of Employee Privacy Through a Comparative Study of Data Privacy Legislation in the European Union, United States, and Canada*, 2004 STAN. TECH. L. REV. 4, 4-6 (2004).

state and federal legislation, constitutional provisions, and case law.[36] In order to understand the development of the law in the United States on the topic, a review of the historical and legal aspects of privacy is appropriate.

II. HISTORICAL ASPECTS

Officially, the word "privacy" traces its entry into the English language back to 1598.[37] Shakespeare spread its dissemination to Elizabethan audiences with some of his later plays such as the *Merry Wives of Windsor*.[38] While privacy was elusive in Elizabethan England,[39] it was recognized by courts as early as 1604 in *Semayne's Case*.[40] In this decision, the Court stated "[t]hat the house of every one is to him as his . . . castle and fortress[.]"[41] This concept continued expanding. In 1769, Sir William Blackstone stated that

> *Eaves-droppers*, or fuch as liften under walls or windows, or the eaves of a houfe, to hearken after difcourfe, and thereupon to frame flanderous and mifchievous tales, are a common nufance and prefentable at the court-leet: or are indictable at the feffions, and punifhable by fine and finding funreties for the good behavior.[42]

This concept of privacy crossed the Atlantic with the American colonists,[43] and was enshrined in the Constitution with the Fourth Amendment, which guaranteed "[t]he right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures," as well as requiring "probable cause" for "warrants" to be issued and "supported by Oath or Affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[44]

---

36. *See* U.S. CONST. amend. IV, amend. XIV (noting potential federal constitutional protections that are applicable to public employers). Several pieces of enacted legislation also provides a patchwork quilt of protection. *See* Electronic Communication Privacy Act of 1986, 18 U.S.C. § 2511 (2007); Employee Polygraph Protection Act, 29 U.S.C. § 2002 (2002) Fair Credit Reporting Act, 15 U.S.C. § 1681k (2001); Federal Wiretap Act of 1968, 18 U.S.C. § 2510 (2007), *amended by* Electronic Communication Privacy Act of 1986; National Labor Relations Act, 29 U.S.C. § 151 (2002); Privacy Act of 1974, 5 U.S.C. § 552(a) (2007); Stored Communications Act, 18 U.S.C. § 2701 (2007); and Video Voyeurism Act of 2004, 18 U.S.C. § 1801 (2007). State constitutions and legislation as well as the common law tort theory of privacy may also offer protection. *See* SAFON, *supra* note 29, at 40-47.

37. *See* OXFORD ENGLISH DICTIONARY, *supra* note 8, at 515.

38. *Id.*

39. *See* SARAH GRISTWOOD, ELIZABETH AND LEICESTER: POWER, PASSION, POLITICS 118 (Viking Penguin 2007).

40. *Semayne's Case*, (1604) 77 Eng. Rep. 194 (K. B.).

41. *Id.* at 195.

42. SIR WILLIAM BLACKSTONE, 4 COMMENTARIES 169 (1769).

43. *See* Solove, *supra* note 33, at 23, 27-28.

44. U.S. CONST. amend. IV.

Spaciousness in the new colonies made privacy a reality for many of the new settlers.[45] Over time, the evolution of new technologies, particularly print newspapers, made the invasion of privacy real and problematic.[46] Yellow journalism, as it was known, purported to report upon the activities of community leaders, their spouses and acquaintances.[47] Gossip, in print format, became permanent, creating archives with information about individuals.[48]

In the Nineteenth Century, new inventions such as the telegraph[49] and camera[50] created additional privacy concerns, particularly when paired with burgeoning newspaper publications. Samuel D. Warren and Louis D. Brandeis were so concerned about the new technologies and the potential impact upon an individual's "right to be let alone" that they penned *The Right to Privacy*.[51] Their article began the development of a tort theory of the right to privacy.[52] Its impact was profound.[53] This tort theory was further expanded by William Prosser in the 1960s.[54] After carefully examining cases on the topic, Prosser concluded that four distinct privacy torts were recognized.[55] The theories were: "(1) intrusion upon seclusion; (2) public disclosure of private facts; (3) false light or "publicity"; and (4) appropriation."[56] As case law developed in this area, federal legislation also developed and later expanded, offering a variety of piecemeal privacy protections.[57]

As a result of this, individual expectations regarding privacy exist. An employer also has concerns that result in the monitoring of employees, enabled by technology. This article will consider several questions about workplace privacy, such as:

- Whether employees have an expectation of privacy in the workplace?

---

45. ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 16-18 (Sheridan Books 2000).

46. *See* SOLOVE, *supra* note 21, at 106-09.

47. *Id.*

48. *See* MORRIS L. ERNST AND ALAN U. SCHWARTZ, PRIVACY: THE RIGHT TO BE LET ALONE 5-44 (Greenwood Pub. 1962).

49. Library of Congress, *American Memory, Samuel F.B. Morse Papers*, http://memory.loc.gov/ammem/sfbmhtml/sfbmhome.html (last visited Sept. 17, 2008). Morse is credited with sending the first electronic telegraph on May 24, 1844. It said: "What hath God wrought?" *Id.*

50. *See* Solove, *supra* note 33, at 34. The film roll as well as the hand held camera is considered to be inventions of George Eastman of Eastman Kodak Co. *Id.*

51. Samuel D. Warren and Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1891).

52. *See id.*

53. *See* Solove, *supra* note 33, at 34-36.

54. *Id.* at 37.

55. *Id.*

56. *Id.*

57. *See* U.S. Const. amend. IV and XIV.

- Whether such an expectation is reasonable?
- Whether employers monitor employee behaviors in the workplace?
- If so, what tools are used to monitor?
- When and where does monitoring occur?
- Whether there is legislation available to address workplace privacy rights when an employee believes that an employer has violated his or her privacy?
- What analysis should be used to determine a breach of privacy in the workplace?

III. THE EMPLOYEE'S PERSPECTIVE: DO THEY HAVE AN EXPECTATION OF PRIVACY?

Employees frequently believe, albeit mistakenly, that the Constitution's guarantee that individuals "be secure in their persons, houses, papers and effects, against unreasonable searches and seizures"[58] is applicable to the workplace.[59] Unless the employer is a public sector employer, neither the Fourth Amendment nor the Fourteenth Amendment is applicable to a private employer's behavior because both amendments require "state action."[60]

Using various forms of technology, employers monitor employee behaviors in the workplace.[61] Electronic surveillance of Internet access and e-mail is common as is video surveillance of workplace areas.[62] In addition, office and cubicle searches are not unknown.[63] While the Fourth and Fourteenth Amendments provide public sector employees with some privacy protections, this protection is limited as was discussed by the U.S. Supreme Court in *O'Connor v. Ortega*.[64]

In *Ortega*, the Court confronted two issues: (1) whether a public employee has a reasonable expectation of privacy in his or her office, desk and filing cabinets[65]; and (2) if so, what is the appropriate Fourth Amendment

---

58. U.S. Const. amend. IV.

59. Alan F. Westin, *The Kenneth M. Piper Lecture: Privacy in the Workplace: How Well Does American Law Reflect American Values?*, 72 CHI.-KENT L. REV. 271, 274-75 (1996).

60. S. Elizabeth Wiborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 826-27 (1998).

61. *See* 2005 Electronic Monitoring & Surveillance Survey: *Many Companies Monitoring, Recording, Videotaping—and Firing—Employees*, AM. MGMT ASS'N, May 18, 2005, *available at* http://www.amanet.org/press/amanews/ems05.htm.

62. *Id.*

63. MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 239-252 (2d ed., Bureau of National Affairs 2003).

64. O'Connor v. Ortega, 480 U.S. 709 (1987).

65. *Id.* at 711-12.

standard to be applied to a search conducted by a public employer in an area where a public employee has a reasonable expectation of privacy?[66]

Ortega, a psychiatrist, was in charge of the Napa State Hospital's psychiatric residency training program.[67] Complaints from residents about his personnel management led to the hospital's placing Dr. Ortega on administrative leave as they investigated allegations of sexual harassment, financial impropriety and inappropriate disciplinary actions.[68] As part of the investigation, hospital personnel entered Dr. Ortega's office and searched his desk and file cabinets.[69] This search resulted in the seizure of several personal items of Dr. Ortega's.[70] Shortly thereafter, Dr. Ortega was terminated by the hospital.[71] He then sued, arguing that Napa State's search of his office, desk and cabinets violated his reasonable expectation of privacy.[72]

As the Court considered Ortega's claims, they concluded that within the public employment sector, "the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."[73]The Court recognized that an employee's need for privacy in the workplace must be balanced against the employer's need to manage and control the workplace.[74] While the Court in *Ortega* acknowledged that public employer searches and seizures are subject to the restraints and restrictions of the Fourth Amendment, the Court held that probable cause is not required for such a workplace search.[75] Rather a standard of reasonableness, using a balancing act, is determinative.[76] According to this divided Court,[77] an employee's expectations of privacy within the workplace are dependent upon context.

The Court stated:

> [i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer. The operational realities of the workplace, however, may make *some*

---

66. *Id.* at 712.
67. *Id.*
68. *Id.*
69. *O'Connor*, 480 U.S. at 713.
70. *Id.*
71. *Id.* at 713-14.
72. *Id.* at 714.
73. *Id.* at 718.
74. *O'Connor*, 480 U.S. at 719.
75. *Id.* at 723.
76. *See generally id.*
77. *Id.* at 710. Justice O'Connor authored the opinion and was joined by Chief Justice Rehnquist along with Justices White and Powell. *See id.* Justice Scalia concurred, writing a separate concurring opinion. Justice Blackmun drafted a dissenting opinion in which Justices Brennan, Marshall and Stevens joined. *O'Connor*, 480 U.S. at 709.

> employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official. Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.[78]

Generally, courts have upheld and allowed an employer's surveillance of its employees.[79] To date, attempts to enact federal legislation, protecting workplace privacy rights for employees, have failed.[80]

In addition to these limited federal constitutional and legislative protections, employees also sometimes receive protection via state constitutions and legislation.[81] The common law tort of privacy also provides some protection.

Justice Louis Brandeis and Samuel Warren began arguing for a right of privacy in the late 1800s as the emergence of then new technologies such as photography, telephones and telegraphs began changing perceptions of privacy, space and time.[82] In the early 1960s, William Prosser further explored their concept and articulated four causes of actions under a tort of privacy.[83] According to Prosser, tort privacy theory allowed actions based upon an intrusion upon seclusion; public disclosure of embarrassing private facts; casting in a false light; or the appropriation of one's image or likeness without permission.[84]

These four similar theories of invasion of privacy are actually four different torts.[85] Each theory differs slightly in the elements of proof.[86] To prevail under the first theory, intrusion upon seclusion, a plaintiff would need to demonstrate an intrusion into "something which would be offensive or objectionable to a reasonable man."[87]

The public disclosure of embarrassing public facts requires that a plaintiff demonstrate:

---

78. *Id.* at 717.

79. *See* FINKIN, *supra* note 63, at xxiii-xxx; *see also* Smyth v. Pillsbury, 914 F. SUPP. 97 (E.D. Pa 1996); San Diego v. Roe, 543 U.S. 77 (2004).

80. *See* Privacy for Consumers and Workers Act, H.R. REP. NO. 102-1024 (1992); Notice of Electronic Monitoring Act, S. 2898, 106th Cong. (2000). Both bills stalled in Committee.

81. For a comprehensive discussion of state legislation pertaining to employee privacy rights in the workplace, *see* FINKIN, *supra* note 63, at 429-822.

82. *See generally* Warren & Brandeis, *supra* note 51.

83. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

84. *Id.*

85. *Id.* at 389.

86. *Id.*

87. *Id.* at 390-391.

- the public, rather than private, disclosure of facts, i.e. publicity;
- the facts disclosed are private facts; and
- the private fact that is publically disclosed "would be offensive and objectionable to a reasonable man of ordinary sensibilities."[88]

To demonstrate that a defendant has cast a plaintiff in a "false light in the public eye," the plaintiff must show:

- that the defendant's action case the plaintiff in a false light, although not necessarily a "defamatory one[;]" and
- this casting is something that "would be objectionable to the ordinary reasonable man under the circumstances[.]"[89]

Last, a plaintiff may allege a violation of privacy when a defendant appropriates his or her "likeness" without permission. To establish this theory of invasion of privacy, a plaintiff must establish:

- that there was an "appropriation of an aspect of the plaintiff's identity[;]" and
- that the defendant appropriated this "likeness for his own advantage."[90]

While these tort theories of privacy are separate and distinct, they do share common features.[91]

An employee's expectations regarding privacy in the workplace depend upon the specific context and circumstances and must always be "reasonable."[92]

IV. THE EMPLOYER'S PERSPECTIVE

Employees are not the only group in the workplace with privacy concerns. Employers are concerned with workplace privacy for a variety of reasons, including lost productivity and the imposition of liability for employee comments and behavior.[93] Thus, employers monitor employees both inside, and sometimes outside of the workplace.[94]

---

88. Prosser, *supra* note 83, at 393-97.

89. *Id.* at 400. There is frequent overlap between this tort and the tort of defamation.

90. *Id.* at 403-406.

91. *Id.* at 407-409.

92. *See O'Connor v. Ortega*, 480 U.S. at 725-26; *see also* 18 A.L.R.6th 1 (2006) (analyzing the reasonableness standard).

93. *See, e.g.*, Victor Schachter, *Privacy in the Workplace in* PRACTICING LAW INSTITUTE'S 6TH ANNUAL INSTITUTE ON PRIVACY LAW: DATA PROTECTION—THE CONVERGENCE OF PRIVACY AND SECURITY 153, 214-17, 220-35 (2006) *available at* 828 PLI/PAT 153 (Westlaw).

94. *Id.*

A. Why Do Employers Monitor?

Employers monitor employee conduct in the workplace for several reasons. Studies indicate that employees spend a significant portion of their working hours managing personal business, resulting in a loss of productivity.[95] Employee "internet abuse" includes activities such as surfing non-work related sites (including pornographic sites), online shopping, checking stocks, and making personal travel arrangements.[96] Employer liability can also become an issue with employee misuse of employment related tools such as the Internet, email, and bulletin boards.[97] Employees can send emails defaming or libeling co-workers and others as well as sending inappropriate emails that result in claims of sexual harassment or discrimination.[98] Employees can breach employer and co-worker confidences by inappropriately sharing trade secrets or company financial data.[99] These are some of the reasons why employers monitor employee behavior.

Employers use a variety of tools to monitor employee behavior. These include: tracking Internet usage and reviewing sites visited; monitoring e-mail communications; listening in on telephone conversations; video surveillance; keystroke logging; screening and blocking software; and using GPS (global positioning) software.[100]

Employers monitor employees at different stages of the employer-employee relationship.[101] Often such monitoring starts at the beginning of the relationship with pre-employment screening.[102] Credit and criminal background investigations are conducted while references are checked.[103] Drug and alcohol tests may also be done and medical examinations may be required.[104]

---

95. Court, *supra* note 30, at 18.

96. *Id.* at 16-18.

97. *See* Blakely v. Continental Airlines, 751 A.2d 538 (N.J. 2000.) In this decision, the court held that an employer could be held liable under Title VII of the Civil Rights Act of 1964 for remarks made against a female employee by other employees on an electronic bulletin board on which work assignments were posted, and remanded the case to resolve a fact-based jurisdictional issue. *Id.* at 543.

98. Curtis v. DiMaio, 46 F. Supp. 2d 206 (E.D.N.Y. 1999.) This case involved the dissemination of Polish and Ebonic jokes sent over the company's e-mail system, and held that multiple offenses can result in action against an employer; however, "a single offensive e-mail does not create a hostile work environment." *Id.* at 213.

99. Christopher Pearson Fazekas, *1984 is Still Fiction: Electronic Monitoring in the Workplace and U.S. Privacy Law*, 2004 DUKE L. & TECH. REV. 15, 15-17 (2004).

100. *See* Swaya & Eisenstein, *supra*, note 30, 9-11.

101. *See, e.g.*, FINKIN, *supra* note 63, at 160-73.

102. *Id.*

103. *Id.* at 170-75.

104. *Id.*

Once hired and on the job, an employee's conduct may be monitored while at work as well as while *off duty*. Telephone calls may be monitored for *quality assurance*. Keystroke logging and blocking software can track employee productivity while eliminating access to non-work related sites. Emails may be monitored and searched to ensure productivity and compliance with employer policies. Video cameras could be installed in work areas overseeing work-related activities. Global Positioning Systems ("GPS") are used to monitor employees outside of the building and often drivers are monitored with GPS technology.[105]

Workplace monitoring sometimes extends beyond the workplace. Dating policies, designed to ensure compliance with Title VII of the Civil Rights Act,[106] prohibit supervisor/subordinate dating.[107] A few workplaces, deciding to promote healthy lifestyles, have banned after hours smoking and do drug tests to ensure compliance.[108] Blogging, if it includes comments about an employer, can result in terminations even if done after hours, at home and on the employee's own computer.[109]

Employers monitor for productivity and liability reasons, using a variety of tools. Monitoring often begins early in the relationship and frequently lasts until the relationship ends. Does an employee have any workplace privacy protections? To answer this question, primary sources of federal and state law must be examined.

V. U.S. LAW: CONSTITUTIONS, CASES & LEGISLATION MONITORING

A. Pre-employment Screening

Employers can monitor behavior before the employment relationship is formally created, beginning the job application process with pre-employment inquiries.[110] In order to hire wisely and avoid future litigation, employers often investigate the background of a job applicant whom they wish to

---

105. National Work Rights Institute, *On Your Tracks: GPS Tracking in the Workplace*, *available at* http://www.workrights.org/issue_electronic/NWI_GPS_Report.pdf (last visited Oct. 5, 2008).

106. 42 U.S.C. § 2000(e) (2008).

107. *See* Ruth Ann Strickland, *Sexual Harrassment: A Legal Perspective for Public Administrators*, 25 PUB. PERS. MGMT., Vol. 25 (1995), *available at* http://www.questia.com/googleScholar.qst;jsessionid=JFNL53TcrFZZH3QTlLd1vL13zklpvKx2qqJPXf49kkhcTLCX0r19!1407480681?docId=5001654617.

108. *See, e.g.*, Jeremy W. Peters, *Company's Smoking Ban Means Off-Hours, Too*, N.Y. TIMES, Feb. 8, 2005, at C5, *available at* ERLINK"http://www.nytimes.com/2005/02/08/business/08smoking.html" http://www.nytimes.com/2005/02/08/business/08smoking.html (last visited Oct. 23, 2008).

109. Thomas J. Benedict & Timothy M. Rusche, *Internet Law: Employee Blogs Pose Potential Problems for Businesses*, INTERNET BUS. LAW SERV., Mar. 6, 2007, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1629.

110. *See* FINKIN, *supra* Note 63, at 158-83.

employ.[111] If the employer delegates this background investigation to a third party consumer reporting agency, the Fair Credit Reporting Act takes effect.[112] According to the Act, the employer must:

> disclose to the job applicant or employee that the employer will be retaining a consumer reporting agency to prepare a consumer report on the individual. This disclosure must be on a standalone document and not part of an employment application. The employer must receive the individual's signed consent to the preparation of such a report prior to requesting the report from the consumer reporting agency.
>
> If the employer uses information contained in the consumer report for an "adverse action," the employer must notify the subject of the report prior to taking the adverse action. This pre-adverse action notice must include a copy of the report and an explanation of the individual's rights under the FCRA[.]
>
> . . . .
>
> After the adverse action occurs, the employer must provide the individual subject to the adverse action with an adverse action notice. This notice would include the name, address, and phone number of the consumer reporting agency that prepared the report and statements that (1) the employer, and not the agency, made the adverse decision regarding the individual, (2) the individual has the right to a free copy of the report, and (3) the individual has the right to dispute the accuracy or completeness of the information contained in the consumer report.[113]

In addition to investigating a job applicant's credit report, employers also conduct pre-employment investigations into other aspects of an applicant's life.[114] Criminal background checks occur as do requests to view school records, occupational licenses and drug screening.[115]

B. Workplace Surveillance

In the United States, job applicants who survive the initial investigation and become employees continue to face employer scrutiny of their behavior.[116]

---

111. *See id.*

112. 15 U.S.C. § 1681(k) (2008).

113. Lisa J. Sotto & Elisabeth M. McCarthy, *An Employer's Guide to U.S. Workplace Privacy Issues*, THE COMPUTER & INTERNET LAWYER, Jan. 2007, at 2.

114. FINKIN, *supra* note 63, at 173-83.

115. *Id.*

116. *See* Court, *supra* note 30, at 16-18.

As discussed earlier, employers use several forms of technology to monitor the behavior of employees in the workplace.[117] E-mail and Internet usage together with telephone use are behaviors that are frequently monitored.[118]

Two federal statutes apply to the monitoring of e-mail and the telephone. They are the Electronic Communications Privacy Act of 1986 ("ECPA")[119] and the Stored Communications Act.[120] Enacted in 1986 by Congress, the stated purpose of the ECPA is to protect electronic communications.[121] Since the ECPA was designed to prevent the unauthorized access to oral, wire and electronic communications, it would appear that employees would find a shield for their privacy concerns with the ECPA. Three exceptions render the ECPA almost meaningless in the work place.

The ECPA prohibits the "[i]nterception and disclosure of wire, oral, or electronic communications."[122] Section 2(a)(i) of the Act states that "[i]t shall not be unlawful . . . for an operator of a switchboard, or an officer, employee, or agent of a provider of wire or electronic communication service . . . to intercept, disclose, or use that communication in the normal course of his employment."[123] Section 2(c) provides that such an interception is not unlawful "where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[124]

Given the above language the statute provides a large loophole for employers. According to the Act, the following exceptions are applicable: consent, provider or service, or ordinary course of business.[125] The consent exception requires only that an individual who is a party to the communication consent to its interception and access.[126] Since providers of communication systems are not subject to the requirements of the ECPA, employers who own and provide their own e-mail systems are exempt from the ECPA's requirements.[127] Last, if the interception occurs in the ordinary course of business, the ECPA is not applicable.[128]

---

117. *Id.*

118. *Id.*

119. 18 U.S.C. § 2510 (2007).

120. *Id.* § 2701 (2001).

121. *See* Schachter & Swanson, *supra* note 26, at 147-54. The ECPA amended the earlier Federal Wiretap Act of 1968 which protected wire and oral communications by adding "electronic communications" to the type of communications protected. *See id.*

122. 18 U.S.C. § 2511.

123. § 2511(2)(a)(i).

124. § 2511(2)(c).

125. *See generally id.*

126. *Id.*

127. *See generally id.*

128. Court, *supra* note 30, at 25-33. According to Court, the "ordinary course of business exception" has been applied only to telephone monitoring. *Id.* Courts have not yet had to decide this exception's

While the ECPA prohibits the unauthorized access to electronic communications, the Stored Communication Act prohibits the unauthorized interception of electronic communications.[129] Courts have held for an interception to be unauthorized and violate the SCA, it must "be contemporaneous with the transmission or transfer of information from the sender to the recipient."[130]

While the ECPA and the SCA appear to protect employees' e-mail privacy, they generally do not. Employee claims that an employer invaded their privacy when the employer accessed their workplace e-mails typically do not prevail in court.[131] Courts appear to favor employers when the e-mail system involved is owned and operated by the employer as is the computer hardware that is used by the employee.[132]

As early as 1996 in *Smyth v. Pillsbury*, the U.S. District Court for the Eastern District of Pennsylvania concluded that an employee did not have a reasonable expectation of privacy in a company's e-mail system despite company assurances that e-mails would "remain confidential and privileged."[133] Using the company's e-mail system from his home, Pillsbury's employee, Smyth, responded to his supervisor via e-mail to queries about the company's sales management team.[134] Displeased with the sales management team, Smyth threatened to "kill the backstabbing bastards" and indicated a desire to turn the holiday party into a "Jim Jones Koolaid affair."[135] Pillsbury terminated Smyth for sending "unprofessional" and "inappropriate" e-mails.[136] Despite Smyth's allegations that Pillsbury violated his right to privacy, the court did not "find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management."[137]

Almost a decade later, a similar result was reached in the U.S. District Court for the District of Oregon.[138] In *Thygeson v. U.S. Bancorp*, Thygeson, an eighteen-year employee of U.S. Bancorp was terminated for violating

---

application to e-mail. *See* FINKIN, *supra* note 63, at 261-97.

129. See Swaya & Eisenstein, *supra* note 30, at 11.

130. See Frazer v. Nationwide Mutual Insurance Co., 135 F. Supp. 2d 623, 634 (E.D. Pa 2001).

131. *See, e.g., id.*

132. Meir S. Hornung, *Think Before You Type: A Look at E-mail Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 154 (2005).

133. Smyth v. Pillsbury, 914 F. Supp. 97, 98 (E.D.Pa 1996).

134. *Id.*

135. *Id.* at 99 n.1.

136. *Id.* at 98-99.

137. *Id.* at 101.

138. Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 U.S. Dist. Lexis 18863 (D. Or Sept. 15, 2004).

company policy regarding computer and Internet usage.[139] U.S. Bancorp's company policy handbook explicitly stated that "[o]ur . . . personal computers, . . . including e-mail, . . . are intended for Company business only."[140] The policy further provided: "[d]o not use U.S. Bancorp computer resources for personal business" and "[d]o not access inappropriate internet sites and do not send e-mails which may be perceived as offensive, intimidating or hostile[.]"[141] Thygeson acknowledged receipt of these policies in writing.[142] After co-workers complained about receiving offensive e-mails from Thygeson as well as complaining that he spent time sleeping on the job, his manager decided an investigation was required.[143] He asked the network administrator to examine the network drive to review Thygeson's e-mail and Internet usage.[144] The administrator learned, without ever entering Thygeson's office, that Thygeson was spending over four hours a day visiting non-work related Internet sites, and sending sexually explicit e-mail messages.[145] When terminated, Thygeson argued that Bancorp violated his privacy by accessing his e-mail account and viewing his data on the network drive.[146] Bancorp denied that Thygeson's privacy was violated.[147] Disputing this, Thygeson argued that his folders were clearly marked "personal" and that this entitled him to an expectation of privacy.[148] The court denied Thygeson's claim, holding that "when, as here, an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy."[149]

As earlier decisions indicate, an employee's "reasonable expectation of privacy" in e-mail is particularly important when analyzing and understanding employee claims of invasion of privacy. The U.S. District Court for the District of Massachusetts elaborated on an employee's "reasonable expectation of privacy" in e-mail correspondence when it held in *Garrity v. John Hancock* that the plaintiff-employee, Nancy Garrity, had no reasonable expectation of privacy.[150] John Hancock had an e-mail policy that prohibited employees from using the company's e-mail system to send sexually sugges-

139. *Id.* at *2.
140. *Id.* at *14.
141. *Id.*
142. *Id.*
143. *Thygeson*, 2004 U.S. Dist. Lexis 18863, at **7-8.
144. *Id.*
145. *Id.* at **8-9.
146. *See generally id.*
147. *Id.* at **71-72.
148. *Thygeson*, 2004 U.S. Dist. Lexis 18863, at *71-72.
149. *Id.*
150. Garrity v. John Hancock, No. 00-12143-RWZ, 2002 WL 974676 (D. Mass. 2002).

tive messages.[151] The policy further stated that e-mail would be periodically reviewed.[152] Consequently when a co-worker complained that Garrity was sending sexually explicit e-mails that were perceived as sexual harassment, the company conducted an investigation.[153] The investigation revealed the existence of sexually explicit e-mail messages on Garrity's work computer.[154] Garrity did not dispute the existence of such e-mail but insisted that she had an expectation that her e-mail would be private.[155] The court denied Garrity's claim, stating that "[a]ny reasonable expectation on the part of the plaintiffs is belied by the record and plaintiffs' own statements."[156]

Do an employee's e-mail messages to his or her attorney, when sent over an employer's e-mail system, retain their attorney-client/work product privilege? Recently, in *Scott v. Beth Israel Medical* Center, a New York court said "no."[157] In this decision, Dr. Scott was terminated by his employer, Beth Israel Medical Center.[158] After the termination, Beth Israel's attorneys sent counsel for Dr. Scott a letter informing them that the hospital was in possession of e-mail messages exchanged between Dr. Scott and his attorneys.[159] The letter stated that the hospital believed that the attorney-client work product privilege was waived as Dr. Scott used the hospital's e-mail system to send and receive these e-mails, all in violation of the hospital's e-mail policy.[160] Dr. Scott disagreed, arguing that the privilege was not waived.[161] The court rejected Dr. Scott's argument, and invoked a four part test to determine privilege based on the following factors: (1) whether the employer has a "no personal use" e-mail policy; (2) whether the employer enforces this policy by monitoring employee e-mail; (3) whether third parties have the right to access an employee's computer and e-mail; and (4) whether an employee has notice of the e-mail policy and potential for monitoring.[162]

Announcing that the third factor was irrelevant to the case before it, the court concluded that the employer clearly had a "no personal use" e-mail policy that it enforced via monitoring.[163] Employees, including Dr. Scott,

---

151. *Id.*
152. *Id.*
153. *Id.*
154. *Id.*
155. *Garrity*, 2002 WL 974676.
156. *Id.*
157. Scott v. Beth Israel Med. Ctr., 847 N.Y.S.2d 436 (2007).
158. *Id.* at 438.
159. *Id.* at 935-36.
160. *Id.* at 438-39.
161. *Id.*
162. *Scott*, 847 N.Y.S.2d at 439-43; *see also* Kelly D. Talcott, *The Office: One More Privacy-Free Zone*, N.Y. L.J., Dec. 18, 2007, at 5, col. 1.
163. *Scott*, 847 N.Y.S.2d 436, at 443.

were aware of this.[164] The court also held that "[u]nder New York State law, work product is waived when it is disclosed in a manner that materially increases the likelihood that an adversary will obtain the information."[165] Citing the New York State Bar Association's Opinion 782,[166] the *Smith* Court held that "a lawyer who uses technology to communicate with clients must use reasonable care with respect to such communication, and therefore must assess the risks attendant to the use of that technology and determine if the mode of transmission is appropriate under the circumstances."[167] Since Beth Israel clearly made its e-mail and monitoring policy known to its employees Dr. Scott was unable to invoke the privilege.[168]

While courts appear to afford sexually explicit e-mails and personal e-mails little protection, employee e-mails sent over the employer's e-mail system that advocate and urge a change to improve employee working conditions may receive protection under the National Labor Relations Act.[169] If an employer strictly enforces a non-business use e-mail policy, any such e-mail messages would likely not be acceptable. If, however, the policy is not enforced, employers cannot selectively enforce and then forbid employee e-mail messages that argue for the existence of a union.[170]

Besides monitoring e-mail, employers may also monitor computer usage.[171] Keystroke logging software is used to keep track of productivity, and blocking software prevents employees from accessing non-work related Internet sites.[172]

Other employee monitoring may include video surveillance which the Electronic Communications Privacy Act and the Federal Wiretap Act of

---

164. *Id.* at 443.

165. *Id.*

166. N. Y. STATE BAR ASSOC., COMM. ON PROF'L ETHICS, *E-mailing Documents That May Contain Hidden Data Reflecting Client Confidences and Secrets*, Op. N. 782, 2004, 2004 WL 3021157 (Dec. 8, 2004), *available at* http://www.nysba.org/AM/Template.cfm?Section=Home&CONTENTID=6871&TEMPLATE=/CM/ContentDisplay.cfm.

167. *Smith*, 847 N.Y.S.2d 436, at 444 (quoting N. Y. STATE BAR ASSOC.,*supra* note 169.

168. *Id.* Although the New York Supreme Court, Appellate Division, First Department reversed the lower's court's decision the reversal affected only the issue of breach of an employment contract. *See Scott v. Beth Israel*, 850 N.Y.S.2d 81 (2008.).

169. 29 U.S.C. § 151 (2008); *see* FINKIN, *supra* note 63, at 289-93 (discussing National Labor Relations Act and company e-mail). A recent Board decision, *Register-Guard Pub. Co.*, 351 N.L.R.B. No. 70, (Dec. 16, 2007), indicated that "absent discrimination, employees have no statutory right to use an employer's equipment or media for Section 7 communications." *Id.* While the decision was not unanimous, it does appear that the majority of the Board concluded that employees, looking to unionize, have no right to use the employer's e-mail system to further this goal. *See id.*

170. The NLRB decision in *Register-Guard Pub. Co.* does throw this principle into some doubt.

171. *See, e.g.*, Jay P. Kesan, *Cyber-Working or Cyber-Shirking? A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289 (2002).

172. *Id.* at 331-32.

1968[173] do not address. These statutes prohibit the unauthorized interception of oral, wire, and electronic communications, and making audio surveillance without consent.[174] They do not address, however, video surveillance. Frequently employers place cameras throughout the workplace area to visually monitor employee productivity without using sound. Employers should limit this surveillance to video only. For instance, installation of a video camera in an employee break room could create issues with the National Labor Relations Act[175] if employees use the break room to discuss unionizing as means of improving the terms and conditions of employment.[176] Video surveillance in bathrooms is likely to run afoul of both the Video Voyeurism Act[177] as well as an employee's reasonable expectation of privacy (i.e. an intrusion upon what should be secluded).[178] The Video Voyeurism Act prohibits the capture, without a person's consent, of the "private area of an individual . . . under circumstances in which that individual has a reasonable expectation of privacy[.]"[179]

In addition to monitoring e-mail, tracking Internet sites and watching employee behavior at work via video surveillance, employers may also need to investigate an employee's honesty when there are allegations of fraud or abuse. When an investigation is ongoing involving allegations of deceit, fraud, or lies, can an employer use a polygraph test to determine truthfulness? Use of polygraphs is governed by the Employee Polygraph Protection Act which generally prohibits the use of polygraph examinations by employers.[180] Section 2006of the Act provides six exceptions to this general rule.[181] Employer polygraphs of employees may be permitted if the employee is a governmental employee at the federal, state or local level.[182] Experts or consultants and the companies that they work for may be subjected to polygraph tests if the company meets either the "National defense and security exemption" or the "FBI exemption."[183] Under the national defense exemption, experts, consultants and companies handling national security issues and contracting with the National Security Agency, the Defense Intelligence

---

173. The Federal Wiretap Act of 1968, 18 U.S.C. § 2510 (2008) *amended by* the Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2511 (2008).

174. *See id.*

175. 29 U.S.C. § 151 (2008).

176. FINKIN, *supra* note 63, at 235-37; *see also* MAGILL, *supra* note 26, at 63-64.

177. 18 U.S.C. § 1801 (2008).

178. MAGILL, *supra* note 26, at 63-64.

179. 18 U.S.C. § 1801(a).

180. 29 U.S.C. § 2002 (2008).

181. *Id.* § 2006.

182. *Id.* § 2006(a).

183. *Id.* § 2006(b), (c).

Agency, the National Geospatial-Intelligence Agency, and the Central Intelligence Agency may use polygraphs on their employees.[184] The FBI exemption provides a similar exception. Employees or contractors with the Federal Bureau of Investigation or the Department of Justice who are involved with counterintelligence may also be subject to polygraph tests.[185] The statute also reserves an exception for an employer involved in an ongoing investigation that involves "theft, embezzlement, misappropriation or an act of unlawful industrial espionage or sabotage[.]"[186] In order to fit within this limited exemption, the following must be satisfied:

> (1) the test is administered in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage;
> (2) the employee had access to the property that is the subject of the investigation;
> (3) the employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation; and
> (4) the employer executes a statement, provided to the examinee before the test, that—
> (A) sets forth with particularity the specific incident or activity being investigated and the basis for testing particular employees,
> (B) is signed by a person (other than a polygraph examiner) authorized to legally bind the employer,
> (C) is retained by the employer for at least 3 years, and
> (D) contains at a minimum—
> (i) an identification of the specific economic loss or injury to the business of the employer;
> (ii) a statement indicating that the employee had access to the property that is the subject of the investigation; and
> (iii) a statement describing the basis of the employer's reasonable suspicion that the employee was involved in the incident or activity under investigation.[187]

---

184. *Id.* § 2006(b)(2)(A)(i).
185. 29 U.S.C. § 2006(c).
186. *Id.* § 2006(d).
187. *Id.* In addition to the four exemptions mentioned, the statute also provides exemptions for security services and for drug security, drug theft, or drug diversion investigations. *See. id.* § 2006(e)-(f).

Besides monitoring employee behavior within the workplace, employers are implementing new tools and technologies to follow up on employees performing work outside of the workplace.[188] GPS and radio frequency identification tags ("RFID") as well as cell phones are examples of new technologies being used in the workplace.[189] With these tracking devices, employers are checking up on drivers and other employees who handle their jobs outside the traditional office area.[190] While employers claim it permits them to ascertain productivity, employees may disagree.

C. Surveillance After Hours

The distinctions between work and "off-duty" behaviors are harder to establish in today's world because existing technologies, such as cell phones, PDAs, and laptops, blur the line between on the clock and off. Employers can, however, exert some control over off-duty employee behaviors.[191] Four years ago the United States Supreme Court directly addressed the "after hours" activities issue, as it relates to employee termination, with its decision in *San Diego v. Roe.*[192] A police officer, John Roe, was terminated by the San Diego Police, for his behavior while off duty.[193] Because John Roe was an employee for the City of San Diego, some of his arguments (i.e. that the City was violating his First Amendment freedom of speech rights) would not be available to non-public employees.[194]

John Roe had made a video of himself wearing a police uniform then stripping it off and masturbating.[195] He then sold this video on eBay, using the moniker and e-mail contact of code3stud@aol.com.[196] While he was not

---

188. *See, e.g.*, William A. Herbert, *No Direction Home: Will the Law Keep Pace with Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery*, 2 J. L. & POL'Y FOR INFO SOC'Y. 409 (2006); *see also* Kelly D. Talcott, *Cutting Out Privacy in the Office*, N.Y. L.J., Dec. 19, 2007, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1198010085253 (discussing New York case law on employee privacy in the workplace).

189. *See* Herbert, *supra* note 188, at 455; *see also* Talcott, *supra* note 188 (discussing New York case law on employee privacy in the workplace).

190. Herbert, *supra* note 188.

191. FINKIN, *supra* note 63, at 421-26; *see also* Marisa Anne Pagnattaro, *What Do You Do When You Are Not At Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L 625, 641-46 (2004) (discussing various state law provisions regarding employer limitations on employee off-duty conduct); Jill Schachner Chanen, *The Boss Is Watching: And Employees Are Finding They Have Fewer Places to Hide*, 9 A.B.A. J. 48 (2008) (discussing employer monitoring practices).

192. San Diego v. Roe, 543 U.S. 77 (2004).

193. *Id.* at 78.

194. Wiborn, *supra* note 60, at 828.

195. Roe, 543 U.S. at 78.

196. *Id.*

wearing a San Diego Police Department uniform, he was wearing a police uniform.[197] When Roe's immediate supervisor was browsing eBay, he noticed that several items of official San Diego Police Department clothing were for sale by someone listed as code3stud@aol.com.[198] Further browsing led him to the Roe's adult video listings.[199] Recognizing Roe's picture, the supervisor turned the information over to a higher ranking department official, which in turn lead to an internal investigation.[200]

During the investigation, Roe sold to an undercover officer a video depicting himself issuing a ticket then disrobing and masturbating.[201] When confronted by the police department, Roe freely admitted his behavior.[202] He was told to remove the offending items from eBay.[203] While Roe removed the list of videos from eBay, he did not amend his seller's profile; which included a listing of the objectionable videos.[204] When his employer discovered this, it began termination proceedings on the basis that Roe failed "to follow its orders."[205]

Roe then sued, arguing that the termination proceeding violated his First Amendment right to free speech.[206] While the U.S. Supreme Court acknowledged that "[a] government employee does not relinquish all First Amendment rights otherwise enjoyed by citizens just by reason of his or her employment[,]"[207] it also noted that "a governmental employer may impose certain restraints on the speech of its employees, restraints that would be unconstitutional if applied to the general public."[208] When weighing a government employee's right to engage in free speech against an employer's right to protect its mission, the Court referred to the balancing test set forth in *Pickering v. Board of Education Township High School District 205.*[209] According to *Pickering*, a court must balance "the interests of the [employee], as a citizen, in commenting upon matters of public concern and the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees."[210] Applying the *Pickering* principles to the facts of

197. *Id.*
198. *Id.*
199. *Id.*
200. Roe, 543 U.S. at 78-79.
201. *Id.* at 79.
202. *Id.*
203. *Id.*
204. *Id.*
205. Roe, 543 U.S. at 79.
206. *Id.*
207. Roe, 543 U.S. at 80.
208. *Id.*
209. *Id.* at 82.
210. Pickering v. Bd. of Ed. Twp. High Sch. Dist. 205, Will County, 391 U.S. 563, 568 (1968).

Roe, the Court had no difficulty concluding that Roe's behavior did not "qualify as a matter of public concern under any view of the public concern test."[211] Therefore, Roe did not satisfy the *Pickering* threshold and thus his after hours behavior did not receive constitutional protection.[212]

Employers often prohibit other "after hours" personal behavior by employees to avoid liability or reduce costs. To avoid claims of sexual harassment under Title VII of the Civil Rights Act, employers often have non-fraternization policies, disallowing dating between supervisors and the individuals supervised by the supervisor.[213] In addition to dating, some employers extend off duty control to other lawful activities such as smoking.[214] For example, a Michigan insurance company banned employee smoking.[215] Under the new policy, employees were not allowed to smoke either at work or after work, and random breathalyzer tests were used to enforce the ban.[216] Employees who failed the breathalyzer tests were suspended, and fired in the event of a second violation.[217] While some states have enacted legislation prohibiting adverse employment decisions made regarding an employee's lawful consumption of products such as tobacco,[218] some employers have successfully banned such after hours consumption in the absence of lifestyle protection legislation.[219]

---

211. Roe, 543 U.S. at 84.

212. *Id.* at 84-85.

213. MAGILL, *supra* note 26, at 77-81.

214. Dick Dahl, *Employers Take Action to Control "Unhealthy" Employee Lifestyles*, LAW. USA, Feb. 12, 2007.

215. *Id.*

216. *Id.*

217. *Id.*; *see also* Peters, *supra* note 108.

218. Some states have enacted legislation specifically addressed at an employee's lawful consumption of tobacco after office hours and prohibit employers from taking adverse actions based on the employee's consumption. *See* CONN. GEN. STAT. ANN. § 31-40s(a) (West 2008); D.C. CODE § 7-1703.03(a) (2008); KY. REV. STAT. ANN. § 344.040(3) (West 2008); ME. REV. STAT. ANN. tit. 26, § 597 (2008); MISS. CODE ANN. 71-7-33 (West 2008); MO. ANN..STAT. § 290.145 (West 2008); N.J. STAT. ANN. § 34:6B-1 (West 2008);, N.M. STAT. ANN. § 50-11-3(A)(1) (West 2008);OKLA. STAT. tit. 40, § 500 (2008); OR. REV. STAT. ANN. § 659A.315 (West 2008); S.C. CODE ANN. § 41-1-85 (2008); S.D. CODIFIED LAWS § 60-4-11 (2008); VA. CODE ANN. § 15.2-1504 (West 2008); W. VA. CODE ANN. § 21-3-19 (West 2008); WYO. STAT. ANN. § 27-9-105(a)(iv) (2008). Other states have enacted legislation that prohibits employers from taking adverse actions against an employee who consumes lawful products after office hours. *See* CAL. LAB. CODE § 98.6 (West 2008); COLO. REV. STAT. ANN. § 24-34-402.5 (West 2008.); 820 ILL. COMP. STAT. ANN. 55/5(a) (West 2008); MINN. STAT. ANN. § 181.938 (West 2008); MONT. CODE ANN. § 39-2-313 (2008); N.C. GEN. STAT. ANN. § 95-28.2 (West 2008); N.D. CENT. CODE § 14-02.4-03 (2008); NEV. REV. STAT. ANN. § 613.333 (West 2008); N.Y. LAB. LAW § 201-d (2)(b) (McKinney 2008); TENN. CODE ANN. § 50-1-304(e) (West 2008); WIS. STAT. ANN. § 111.31 (West 2008).

219. *See* Stephen D. Sugarman, *"Lifestyle" Discrimination in Employment*, 24 BERKELEY J. EMP. & LAB. L. 377, 398-402 (2003.)

A new and popular after hours issue that sometimes results in adverse employment decisions is blogging. Can an employer fire an employee for blogging about work or mentioning anything about work in the blog? There are several well known and successful terminations involving blogging.[220] A former Delta Airlines flight attendant says she was terminated for her blog, *Diary of A Flight Attendant*.[221] Posing in her Delta uniform in an empty plane, Ellen Simonetti says she was initially suspended, then terminated, by Delta for placing "inappropriate" pictures on the Web.[222] Since then, Simonetti, now blogging as Queen of the Sky, continues to blog about her life at *Diary of A Fired Flight Attendant*.[223]

High profile terminations involving blogging exist, as do rank and file terminations.[224] Joyce Park states on her blog, *Fishy Thoughts*, that she was fired in 2004 by her employer, Friendster, for blogging.[225] In her blog, Park says that she finds it ironic that Friendster terminated her for blogging since Friendster "is a company that is all about getting people to reveal information about themselves."[226] Mark Jen, author of the then blog, *NinetyNineZeros*, told an interviewer that he was fired by Google after posting criticisms of Google on his blog.[227] Specifically, Jen compared Google's salary structure and benefit package with Microsoft's, and indicated that Google's package was less than the Microsoft package.[228]

Michael Hanscom, a temporary Microsoft employee, was fired in 2003 by Microsoft for photos posted on his blog, *eclecticism*. At the site, Hanscom took a picture of several Apple G5 notebooks being unloaded on a loading

---

220. *See, e.g.*, Ellen Simonetti, It's Over, http://queenofsky.journalspace.com/?m=10&y=2004 (Oct. 29, 2004, 14:37 CST).

221. *Id.*

222. Ellen Simonetti, *Perspective: I was fired for blogging*, CNET NEWS, http://news.cnet.com/I-was-fired-for-blogging/2010-1030_3-549086.html?tag_nefd.ac&tag=nl.e540-2.

223. *See generally* Ellen Simonetti, Diary of A Fired Flight Attendant, at http://queenofsky.journalspace.com. Simonetti has also authored an autobiography about the subject. *See* ELLEN SIMONETTI, DIARY OF A DYSFUNCTIONAL FLIGHT ATTENDANT: QUEEN OF THE SKY BLOG (Blog Based Books) (2006).

224. *See* Jon Darrow & Steve Lichtenstein, *Employment Termination for Employee Blogging: Number One Tech Trend for 2005 and Beyond, or a Recipe for Getting Dooced*, 2006 UCLA J.L. TECH. 4 (2006).

225. Joyce Park, Shitcanned, http://troutgirl.wordpress.com/2004/08/30/shitcanned/ (Aug. 30, 2004, 21:29 PST).

226. *Id.*

227. Evan Hansen & Stefanie Olsen, *Google Blogger Reappears, Redacted*, CNET NEWS, http://news.cnet.1com/Google-blogger-reappears,-redacted/2100-1038_3-5552022.html (Jan. 26, 2005, 3:19 PST).

228. *Id.*

dock. Above the picture, he included the caption: "It looks like somebody over in Microsoftland [sic] is getting some new toy."[229]

Rachel Mosteller, a journalist, blogged under a pseudonym, *Sarcastic Journalist*.[230] While employed by the Durham, North Carolina *Herald Sun*, Mosteller wrote:

> I really hate my place of employment. Seriously. Okay, first off. They have these stupid little awards that are supposed to boost company morale. So you go and do something 'spectacular' (most likely, you're doing your JOB) and then someone says 'Why golly, that was spectacular.' Then they sign your name on some paper, they bring you chocolate and some balloons.
> Okay two people in the newsroom just got it. FOR DOING THEIR JOB.[231]

Mosteller was fired the day after she posted this on her blog.[232] While her former employer refused to comment, Mosteller was convinced she was "dooced," or fired by her employer for blogging about work.[233]

A high profile Washington, D.C. blogging termination involved Jessica Cutler, then a staff assistant to Senator Mike DeWine.[234] Cutler was terminated after blogging about her sexual exploits with various Washington politicians.[235] While the men were not named in her blog, her use of their initials plus other comments made her partners easy to identify.[236] Jessica was terminated for "misusing an office computer."[237]

Blogging employees might find limited protections in certain situations.[238] Some federal statutory protections may be available. If an

---

229. Michael Hanscom, Even Microsoft Wants G5s, http://www.michaelhanscom.com/eclecticism/2003/10/23/even-microsoft-wants-g5s (Oct. 23, 2003). For more information about his termination, see Michael Hanscom, Fifteen Minutes of Fame, http://www.michaelhanscom.com/eclecticism/2003/10/29/fifteen-minutes-of-fame (Oct. 29, 2003).

230. Amy Joyce, Free *Expression Can Be Costly When Bloggers Bad-Mouth Job*, WASH. POST, Feb. 11, 2005, at A1.

231. *Id.*

232. *Id.*

233. *Id.* To be 'dooced' is to be fired for blogging about one's job. Lichtenstein & Darrow, *supra* note 224, at ¶ 2. While the Oxford English Dictionary does not define "dooced," the Urban Dictionary defines dooced as "to lose one's job because of one's website." URBAN DICTIONARY, *Dooced*, http://www.urbandictionary.com (visited Feb. 15, 2008).

234. April Witt, *Blog Interrupted*, WASH. POST, Apr. 15, 2004, at W12.

235. *Id.*

236. *Id.*

237. *Id.*

238. *See* Robert Sprague, *Fired for Blogging: Are There Legal Protections for Employees Who Blog?*, 9 U. PA. J. LAB. & EMP. L. 355, 360-76 (2007).

employer's behavior has a disparate impact upon a protected class of employees, or employees are treated differently, i.e. subjected to disparate treatment, Title VII of the Civil Rights Act is applicable.[239] Blogs advocating employee activity to improve terms and conditions of employment might also be protected under the National Labor Relations Act.[240] It is difficult to prevail under a tort theory of privacy since blogs are posted online for anyone to view. Thus absent, any federal or state statutory protections, employers can terminate, at will, employees whose blogs they dislike.[241]

D. Analysis

Employers can and do monitor employee behavior and activities. When an employee believes an employer has gone too far and invaded his or her privacy, what analysis should be used? If an employee believes an employer has violated his or her privacy, what remedies are available? The employee must first ascertain what his or her privacy rights are at both the state and federal level. Constitutional protections and legislation should be reviewed. If none of these are applicable or fail to provide relief, the employee should next consider the tort of privacy.

When analyzing an employee allegation of violation of workplace privacy, consider the following:

- Is the employer a public sector, i.e. government, employer at either the state or federal level?
- If so, using the balancing test articulated by the Supreme Court in *Ortega*,[242] was it reasonable, balancing the interests of the employer and the employee, for the employer to conduct the search alleged to have violated the employee's privacy?
- If no federal constitutional protections are available, is any federal legislation applicable?
- Was audio, e-mail, the Internet, or some kind of electronic monitoring involved? If so, is either the Electronic Communica-

239. *See* Civil Rights Act, *supra* note 97.

240. National Labor Relations Act, *supra* note 36.

241. *See* Sprague, *supra* note 237, at 359-78. The employment-at-will doctrine prevails in most states. *Id.* According to Sprague, "[t]he employment-at-will doctrine provides that, for an employment relationship of an indefinite term, both the employer and employee may terminate the relationship at any time, with or without cause, as along as the termination does not violate a contract or employment-related statute." *Id.* at 358.

242. *Ortega*, 480 U.S. at 719-20.

tion Privacy Act[243] or the Stored Communications Privacy Act[244] applicable?

- Is a polygraph exam involved? If so, does the Employee Polygraph Protection Act[245] apply?
- Was a pre-employment background check completed? If so, are the provisions of the Fair Credit Reporting Act[246] going to apply?
- Was video surveillance used? If so, will it bring into play the provisions of the Video Voyeurism Act?[247]
- Does a state's constitution provide any privacy rights?[248]
- If there is no federal legislation that provides protection, is there state legislation that will provide protection? Remember to check out "lawful consumption" and "lifestyle discrimination" statutes at the state level.[249]
- Does the employee have a right to privacy under one of the tort privacy theories? Before reviewing the four tort theories of privacy, remember to ask:
- Did the employee have an expectation of privacy?
- If so, was the privacy invaded?
- Was the matter such that a reasonable person would understand it was private?[250]
- If so, which of the four privacy tort theories available?
- Was there an intrusion upon the employee's seclusion?
- Was a private fact about the employee publically disclosed by the employer?
- Did the employer cast the employee in a false light? or
- Did the employer appropriate and use the employee's likeness or image without the employee's consent?[251]

Answering these questions will help determine if an employer has wrongfully invaded an employee's privacy.

---

243. Electronic Communication Privacy Act, *supra* note 36.
244. Stored Communications Privacy Act, *supra* note 36.
245. Employee Polygraph Protection Act, *supra* note 36.
246. Fair Credit Reporting Act, *supra* note 36.
247. Video Voyeurism Act, *supra* note 36.
248. Florida is an example of a state that provides for privacy rights in its constitution. FLA. CONST. art. 1, § 23.
249. For examples, see the various statutory provisions, *supra* note 36.
250. Warren & Brandeis, *supra* note 51.
251. Prosser, *supra* note 83.

VI. BEST PRACTICES FOR EMPLOYERS & CONCLUSION

As evidenced by the research presented in this article, employees in the United States have very limited expectations of privacy within the workplace. A patchwork quilt of privacy rights is stitched together with limited constitutional, legislative and judicial protections. Despite this, employees often believe personal e-mail, Internet usage and other behavior is protected from employer monitoring. Employers ignore this expectation, monitoring to see that employee productivity is acceptable as well as limiting its liability for employee behaviors.

To ensure best practices about employer monitoring, employers should: have a clearly defined policy in place, explaining that e-mail, Internet usage, keystroke logging, and instant messaging are all monitored; ask the employee to sign a form, indicating that they are aware of this electronic monitoring and give their consent to it; broadly define the network, including e-mail, as well as hardware and software equipment, as employer property that is subject to the employer's control and monitoring; discuss and enumerate in writing expectations about employee blogging and define unacceptable practices; check legislation to determine if lifestyle or lawful consumption statutes exist in a state that provide employees with protection, prohibiting employer discrimination against an employee engaging in such protected acts; alert employees of any video surveillance occurring within their work areas and ensure that cameras do not intrude in areas where a reasonable expectation of privacy exists, i.e. bathrooms or break rooms; alert employees of the use of any tracking devices, such as GPS or RFID; and explain the reasons for the monitoring to employees.

Adhering to these best practices will provide clear communications about privacy expectations, improve employee morale, and provide protection for employers.