INTRUSIVE MONITORING: EMPLOYEE PRIVACY EXPECTATIONS ARE REASONABLE IN EUROPE, DESTROYED IN THE UNITED STATES

Lothar Determann[†] *& Robert Sprague*[††]

TABLE OF CONTENTS

I. **INTRODUCTION** 980

II. **EMPLOYER MONITORING AND EMPLOYEE PRIVACY—U.S. PERSPECTIVE** 981

A. WORK-RELATED EMPLOYER MONITORING 981
B. WORK-RELATED EMPLOYEE PRIVACY 986
1. *Work-Related Rights to Privacy Under the Constitution* 986
2. *Work-Related Rights to Privacy Under the Common Law* 990
3. *Statutory Rights to Privacy* 993
a) The Electronic Communications Privacy Act 995
C. INTRUSIVE WORKPLACE MONITORING AND EMPLOYEE PRIVACY 1001
1. *Employer Access to Personal Web-Based Applications* 1007
2. *Webcams* 1009
3. *GPS* 1012
D. WORKPLACE PRIVACY TRENDS IN THE UNITED STATES 1016

III. **EMPLOYER MONITORING AND EMPLOYEE PRIVACY—EUROPEAN PERSPECTIVE** 1018

A. LAWS IN EUROPE—OVERVIEW 1019
B. CIVIL RIGHTS PROTECTIONS FOR PRIVACY AT THE EUROPEAN LEVEL 1019

---

† Dr. iur habil, Privatdozent, Freie Universität Berlin; Adjunct Professor, University of California, Berkeley School of Law and Hastings College of the Law, and Stanford Law School; Partner, Baker & McKenzie, San Francisco, California.

†† J.D., M.B.A. Associate Professor, University of Wyoming College of Business Management & Marketing.

The authors thank Aaron J. Lyttle, J.D. 2010, University of Wyoming College of Law, for his excellent research assistance for this Article, and for contributions from Charles W. Weinroth, J.D. Candidate 2011, University of California, Hastings College of the Law, and Benjamin Bäuerle, Associate, Baker & McKenzie, Munich, Germany.

C. THE EC'S DATA PROTECTION DIRECTIVE 1023
1. *Necessity Under Contract* 1027
2. *Consent* 1027
3. *Statutory Obligations* 1028
4. *Balancing Test* 1029
D. NATIONAL WIRETAP LAWS IN EUROPE (CASE STUDY: GERMANY) 1030
E. WORK-RELATED ELECTRONIC MONITORING 1031
IV. **DIFFERENCES IN POLICY, LAW, AND PRACTICE—AND THE IMPACT ON GLOBAL EMPLOYERS AND EMPLOYEES** 1034

I. INTRODUCTION

An increasingly global workforce communicates, collaborates, and connects in multinational enterprises and worldwide marketplaces with web- and cloud-based technologies across geographies and territorial borders. Globalization has leveled many historic differences, in the workplace and elsewhere. But, the law on workplace privacy could hardly be more different in the United States and the European Union. This difference raises significant challenges for the global employer who manages and monitors worldwide human resources with global processes and technologies. Additionally, this difference raises fundamental questions as to its origins in workplace privacy standards and why these differences resist convergence so stubbornly.

This Article examines the contrasting policy and legal frameworks relating to data privacy in the United States and the European Union, with a particular focus on workplace privacy and intrusive surveillance technologies and practices. Part II of this Article examines the U.S. perspective on modern work-related employer monitoring practices, the laws giving rise to possible employee privacy rights, and specific types of employer monitoring that may lead to actionable invasions of employee privacy rights. Part III then addresses the issue of employee privacy from the EU perspective, beginning with an overview of the formation of authority to protect individual privacy rights, followed by an analysis of the principal areas of protection and their application. Part IV then provides comparison and conclusions regarding the fundamental differences between the United States and the European Union in employee privacy protection.

II. EMPLOYER MONITORING AND EMPLOYEE PRIVACY—U.S. PERSPECTIVE

U.S. employers engage in a variety of work-related monitoring practices for a range of legitimate business purposes. In general, the right to privacy in the United States is conditioned on a "reasonable expectation of privacy," which is determined by the surrounding circumstances and society's[1] or a "reasonable person['s]"[2] views. Employees in the United States tend to have minimal expectations of privacy in the workplace at the outset. Employers usually destroy any remaining limited expectations via notices and warnings regarding monitoring in employee handbooks, computer log-on splash screens, electronic systems use policies, and privacy statements. Yet, there are new and ever-evolving types of monitoring that can catch employees by surprise and challenge employers' efforts in keeping their workforce aware of advances in technology. This challenge threatens employers' efforts to prevent any development of privacy expectations that could lead to privacy rights and their violation through intrusive surveillance.

A. WORK-RELATED EMPLOYER MONITORING

In the modern office, internet access and e-mail have become ubiquitous.[3] Wireless communications, global positioning systems (GPS), and radio frequency identification (RFID) chips are now common business tools.[4] Along with increased use of computers and communications systems at work comes increased computer and communications monitoring. Typical

---

1. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring). *See also* TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 160 (Ct. App. 2002) ("When affirmative relief is sought to prevent a constitutionally prohibited invasion of privacy, the plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.") (citation and internal quotation marks omitted) (applying CAL. CONST. art. I, § 1).

2. *Katz*, 389 U.S. at 363 (White, J., concurring).

3. Qinyu Liao et al., *Workplace Management and Employee Misuse: Does Punishment Matter?*, 50 J. COMPUTER INFO. SYS. 49, 49 (2009). According to a 2008 Pew Internet & American Life Project survey, nearly one-third of American adults use e-mail or the Internet in their work. *See* MARY MADDEN & SYDNEY JONES, PEW/INTERNET, NETWORKED WORKERS, at i (2008), http://www.pewinternet.org/~/media//Files/Reports/2008/PIP_Networked_Workers_FINAL.pdf.pdf (reporting that of the 53% of American adults employed full- or part-time, 62% use e-mail or the Internet at work).

4. *See, e.g.*, NAT'L TELECOMM. & INFO. ADMIN. (NTIA) AND ECON. & STATISTICS ADMIN. (ESA), U.S. DEP'T OF COMMERCE, A NATION ONLINE: HOW AMERICANS ARE EXPANDING THEIR USE OF THE INTERNET 57–64 (2002) [hereinafter A NATION ONLINE]; Marisa Anne Pagnattaro, *Getting Under Your Skin—Literally: RFID in the Employment Context*, 2008 J.L. TECH. & POL'Y 237, 238 (2008); William P. Smith & Filiz Tabak, *Monitoring Employee E-mails: Is There Any Room for Privacy?*, 23 ACAD. MGMT. PERSP. 33, 33 (2009).

work-related monitoring includes scanning of sent and received e-mails by anti-virus and anti-spam software. This software monitors websites accessed by employees, as well as scans messages and attachments to block code that is considered harmful and content that is presumed inappropriate. Some employers use more intrusive methods: tracking a worker's every keystroke and mouse click; capturing screen shots to monitor communications via remote computing platforms outside the control of the employer's networks (such as webmail and blogging); storing copies of e-mail messages sent and received on servers where individual workers cannot access or delete the messages; logging information on actions performed by workers, including the applications used and the files accessed and printed; monitoring internet access, online sessions, and electronic chat conversations; and remotely viewing what the worker is doing in real time.[5] This monitoring is not restricted to the "workplace" per se, as a substantial number of people use computers in their homes and on the road to perform work on company-owned devices or even privately-owned devices which can be scanned while they are connected to the company network.[6] The latest widely-cited survey of workplace monitoring reveals that significant percentages of employers monitor employee internet usage (66%), e-mail (43%), and time spent on the phone and numbers called (45%), while 16% of employers record phone calls and 9% record voice mail messages.[7]

Employers in the United States monitor employees for three primary reasons: protecting information and other intellectual property assets; increasing productivity; and avoiding liability, including exposure associated with copyright infringement by employees, other improper uses of

5. *See* H. Joseph Wen, Dana Schwieger & Pam Gershuny, *Internet Usage Monitoring in the Workplace: Its Legal Challenges and Implementation Strategies*, 24 INFO. SYS. MGMT. 185, 186 (2007).

6. *See, e.g.*, A NATION ONLINE, *supra* note 4, at 62 ("[A]pproximately 24 million of the 65 million employed adults who use a computer at work also do work on a computer at home . . . ."); MADDEN & JONES, *supra* note 3, at v (reporting that 50% of employed e-mail users check their work e-mail on weekends); Laura Merritt, *Factor Gadgets into Remote-Access Policies*, N.Y. L.J., Apr. 27, 2010, at 5, *available at* http://www.law.com/jsp/nylj/PubArticleNY.jsp?id=1202453204420&The_Mobile_Workforce (noting that employers make available remote access and mobile devices to both high and low level employees who must then respond to e-mails and make calls on cell phones outside the workplace); Smith & Tabak, *supra* note 4, at 33 (noting that new communications devices are at least partially responsible for the blurring of work-life boundaries).

7. AM. MGMT. ASS'N (AMA) & EPOLICY INST., 2007 ELECTRONIC MONITORING AND SURVEILLANCE SURVEY 1–3 (2007), *available at* http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillanceSurvey.pdf.

computers by employees, or hostile work environments.[8] All employers want to ensure that confidential and proprietary information is not purposely or inadvertently disclosed by employees, or improperly accessed by individuals outside the firm.[9] Employers are also concerned about "junk computing"[10] and "cyberloafing."[11] Various surveys reveal that employees spend a significant amount of time at work surfing the Internet for non-work-related purposes and sending and reading personal e-mail messages.[12] One recent

8. Employers also justify monitoring and surveillance based on the argument that the organization owns the computers and equipment that employees use to do their jobs, so the organization has "both a right and an interest in policing the use of those facilities." JEFFREY M. STANTON & KATHRYN R. STAM, THE VISIBLE EMPLOYEE 116 (2006).

9. *See, e.g.*, William G. Porter II & Michael C. Griffaton, *Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace*, 70 DEF. COUNS. J. 65, 66 (2003); Marian K. Riedy & Joseph H. Wen, *Electronic Surveillance of Internet Access in the American Workplace: Implications for Management*, 19 INFO. & COMM. TECH. L. 87, 91 (2010); Smith & Tabak, *supra* note 4, at 34; *see also* United States v. Martin, 228 F.3d 1 (1st Cir. 2000) (upholding conviction of theft of trade secrets based on defendant's e-mail correspondence with competitor's employee); PROOFPOINT, OUTBOUND EMAIL AND DATA LOSS PREVENTION IN TODAY'S ENTERPRISE, 2010, at 4 (2010), http://www.proofpoint.com/id/outbound/index.php (reporting survey data revealing percentages of surveyed firms reporting it is common or very common for outbound e-mail messages to contain valuable intellectual property or trade secrets which should not leave the organization (23%) or confidential or proprietary business information about the organization (21%)). *See generally* Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829, 838 (2005) (discussing the need for employers to monitor employee communications to prevent the loss of intellectual property rights).

10. *See, e.g.*, Ruth Guthrie & Paul Gray, *Junk Computing: Is It Bad for an Organization?*, 13 INFO. SYS. MGMT. 23 (1996) (defining "junk computing" as "the use of information systems in a way that does not directly advance organizational goals" and including examples of unnecessarily sending e-mail messages to multiple recipients and playing computer games).

11. *See, e.g.*, Vivien K. G. Lim, *The IT Way of Loafing on the Job: Cyberloafing, Neutralizing and Organizational Justice*, 23 J. ORG. BEHAV. 675, 677 (2002) (defining "cyberloafing" as "any voluntary act of employees using their companies' internet access during office hours to surf non-job-related Web sites for personal purposes and to check (including receiving and sending) personal e-mail"); *see also* Murugan Anandarajan, *Internet Abuse in the Workplace*, 45 COMM. ACM 53, 53 (2002) (characterizing the world wide web as providing "employees access to the world's biggest playground").

12. *See* Lim, *supra* note 11, at 676 (summarizing several surveys revealing various degrees to which employees use employers' computers and communications systems for personal uses). *But see* Riedy & Wen, *supra* note 9, at 90 (arguing personal use of the Internet and e-mail could make employees more productive and asserting that there is no direct evidence of decreased employee productivity by their sending an e-mail message rather than chatting with a colleague in the break room). *See also* Weber v. Univs. Research Ass'n, 621 F.3d 589, 590–92 (7th Cir. 2010) (affirming the granting of the defendant employer's motion for summary judgment in a case arising from the dismissal of an employee where monitoring revealed that the plaintiff employee had spent some sixteen hours in one week accessing non-work-related websites and frequently accessed personal e-mail accounts associated with the plaintiff's outside business).

survey indicates that over one-quarter of employers have fired employees for internet and e-mail abuse.[13] In fact, public companies in the United States are required to implement whistleblower hotlines and investigate inappropriate conduct as part of their overall obligation to avoid material weaknesses in their processes to ensure compliance with applicable law.[14]

Employers engage in work-related monitoring also in an effort to limit potential liability. There is concern some employees may be downloading music, movies, and other materials in violation of copyright laws, which could result in the employer facing vicarious liability through the doctrine of respondeat superior.[15] There are other improper uses of company computers that can possibly put employers at risk. For example, in one case, an employer was found potentially liable to the wife of an employee who had published nude pictures of the wife's daughter on the Internet using the employer's computer system.[16] Additionally, employers have concerns regarding the content of e-mail messages revealed in litigation-related discovery.[17]

---

13. AMA & EPOLICY INST., *supra* note 7, at 1.

14. *See* Cynthia Jackson, *A Global Whistle-Stop Tour*, DAILY J., Feb. 19, 2009, at 7, *available at* http://www.bakermckenzie.com/files/Publication/b3442009-d314-4585-a396-f1ec419acc6e/Presentation/PublicationAttachment/4840fa55-490c-448a-983f-fbdb28b9f7f5/ar_sfpa_DJ8GlobalWhistleStopTour_feb09.pdf.

15. Smith & Tabak, *supra* note 4, at 34; *see RIAA Collects $1 Million from Company Running Internal Server Offering Thousands of Songs*, RIAA (Apr. 9, 2002), http://www.riaa.com/newsitem.php?news_month_filter=4&news_year_filter=2002&resultpage=2&id=E9996E0C-D33C-CA18-851A-19690EE763FA (announcing settlement of copyright infringement claims against a company that allegedly permitted its employees to access and distribute thousands of infringing music files over its computer network).

16. Doe v. XYC, Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005). In *Doe*, computer technicians and supervisors were aware the employee was using the employer's computer system to visit pornographic websites while at work, but no action was taken due to the employer's policy to not monitor the internet activities of its employees. *Id.* at 1158–60. The court held:

> [A]n employer who is on notice that one of its employees is using a workplace computer to access pornography, possibly child pornography, has a duty to investigate the employee's activities and to take prompt and effective action to stop the unauthorized activity, lest it result in harm to innocent third-parties.

Id. at 1158.

17. *See* AMA & EPOLICY INST., *supra* note 7, at 2 ("Workers' e-mail and other electronically stored information create written business records that are the electronic equivalent of DNA evidence. As a result, 24% of employers have had e-mail subpoenaed by courts and regulators and another 15% have battled workplace lawsuits triggered by employee e-mail . . . ."); Linda Sandler, *"Stupid" Lehman E-Mails Didn't Stay "Just Between Us,"* BLOOMBERG (June 11, 2010, 7:06 AM), http://www.bloomberg.com/news/2010-06-11/lehman-probe-lesson-avoid-big-trouble-by-shunning-stupid-e-mail-terms.html

Employers are also concerned inappropriate e-mail and text messages and internet use could spur hostile work environment complaints.[18] In *Burlington Industries, Inc. v. Ellerth*, and its companion case *Faragher v. City of Boca Raton*, the U.S. Supreme Court held that an employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor.[19] However, when no tangible employment action is taken, an employer may raise as a defense that it exercised reasonable care to prevent and correct promptly any sexually harassing behavior.[20] As a result of this defense's requirements, employers are under greater pressure to take steps to prevent their computer and communications systems from being used to create a hostile work

(describing techniques investigators used to search thirty-four million pages of Lehman Brothers Holdings Inc. e-mails and reports).

18. A hostile work environment is created when "[u]nwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature . . . unreasonably interfere[s] with an individual's work performance or creat[es] an intimidating, hostile, or offensive working environment." 29 C.F.R. § 1604.11(a) (2010) (cited with approval in Meritor Sav. Bank, FSB v. Vinson, 477 U.S. 57, 65 (1986)). Additional protected classes, particularly race, are also protected from hostile work environments. *See, e.g.*, Curtis v. DiMaio, 46 F. Supp. 2d 206, 212–14 (E.D.N.Y. 1999), *aff'd*, 205 F.3d 1322 (2d Cir. 2000); Daniels v. WorldCom, Inc., No. CIV.A.3:97-CV-0721-P, 1998 WL 91261 (N.D. Tex. Feb. 23, 1998) (holding distribution of four racist e-mail messages within the company's e-mail system did not create an actionable hostile environment where the employer had taken prompt remedial action); Owens v. Morgan Stanley & Co., No. 96 CIV. 9747(DLC), 1997 WL 793004 (S.D.N.Y. Dec. 24, 1997) (addressing a hostile work environment claim based on race and holding that a single racist e-mail message does not create an actionable hostile environment).

19. Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 765 (1998); Faragher v. City of Boca Raton, 524 U.S. 775, 807 (1998).

20. Specifically, when no tangible employment action is taken, a defending employer may raise an affirmative defense to liability or damages comprised of two necessary elements: "(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." *Burlington*, 524 U.S. at 765; *Faragher*, 524 U.S. at 807.

environment.[21] Today, employers cite efforts to prevent hostile work environments as a primary motivation for workplace surveillance.[22]

B. WORK-RELATED EMPLOYEE PRIVACY

There are three primary sources of privacy protection in the United States: the Constitution, common law, and statutes. While constitutional and common law rights to privacy have different origins and apply to different actors, they share many commonalities. As shown in Section II.B.1, *infra*, constitutional requirements for a recognized right to privacy often lay the foundation for common law privacy rights. While there are a variety of privacy-related statutes in the United States, they offer only marginal protections for employees.

1. Work-Related Rights to Privacy Under the Constitution

The U.S. Constitution provides for civil rights of individuals against actions of state actors, i.e., state and federal governments, including government employers, but not against actions of private employers.[23] The Constitution does not mention privacy expressly, but a right to privacy has

---

21. *See, e.g.*, *Burlington*, 524 U.S. at 770 (Thomas, J., dissenting) ("Sexual 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.") (citation omitted); Ellerth v. Burlington Indus., Inc., 123 F.3d 490, 513 (7th Cir. 1997) (Posner, C.J., dissenting), *aff'd*, 524 U.S. 742 (1998) ("It 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?").

22. *See* Marc A. Sherman, *Webmail at Work: The Case for Protecting Against Employer Monitoring*, 23 TOURO L. REV. 647, 657 (2007). In a recent workplace surveillance survey, of the twenty-eight percent of employers reporting they had fired an employee for misuse of e-mail, sixty-two percent did so because of offensive or inappropriate language or content; and of the thirty percent of employers reporting they had fired an employee for misuse of the Internet, eighty-four percent did so because of viewing, downloading, or uploading inappropriate or offensive content. AMA & EPOLICY INST., *supra* note 7, at 8–9; *see* Forrester v. Rauland-Borg Corp., 556 F. Supp. 2d 850, 851 (N.D. Ill. 2005), *aff'd*, 453 F.3d 416 (7th Cir. 2006) (upholding dismissal of employee for engaging in sexual harassment based, in part, on sending obscene e-mail messages to harassment victims); *see also* PROOFPOINT, *supra* note 9, at 3 (reporting survey data revealing that 18% of surveyed firms report it is common or very common for outbound e-mail messages to contain adult, obscene, or potentially offensive content).

23. In contrast, the California Constitution protects a right to privacy expressly and expands this protection also to relations between individuals, California private-sector employers, and their employees. CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.").

been inferred relative to searches and seizures permissible under the Fourth Amendment.[24] In circumstances in which a person has a reasonable expectation of privacy, an invasion of that area of privacy by a government entity is presumptively unreasonable in the absence of a search warrant.[25] This Fourth Amendment implied right to privacy in limited circumstances lays the foundation for potential privacy rights for public-sector employees.[26]

As most recently reaffirmed by the U.S. Supreme Court in *City of Ontario, California v. Quon*, the starting point for determining work-related privacy for public-sector employees is found in the plurality opinion in *O'Connor v. Ortega*.[27] "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."[28] "Searches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment."[29]

The subject of a warrantless search must first have a reasonable expectation of privacy in the item or area searched before the search can be deemed unconstitutional.[30] In the public workplace, however, even if the employee has a reasonable expectation of privacy, a warrantless search may

---

24. The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV; *see* Katz v. United States, 389 U.S. 347, 351 (1967) (holding that what a person seeks to preserve as private may be protected under the Fourth Amendment).

25. *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

26. As of December 2008, the federal government employed approximately 2.5 million people. *Federal Government Civilian Employment by Function: December 2008*, U.S. CENSUS BUREAU (2009), http://www2.census.gov/govs/apes/08fedfun.pdf (representing approximately 1.5% of the employed U.S. workforce). As of March 2008, the states employed nearly 4.4 million people on a full-time equivalent basis. *State Government Employment Data: March 2008*, U.S. CENSUS BUREAU (2009), http://www2.census.gov/govs/apes/08stus.txt (representing approximately 3% of the employed U.S. workforce); *see also Table 588. Employed Civilians and Weekly Hours: 1980 to 2008*, U.S. CENSUS BUREAU (2009), http://www.census.gov/compendia/statab/2010/tables/10s0588.pdf (reporting just over 145 million civilian employees in 2008).

27. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010); O'Connor v. Ortega, 480 U.S. 709 (1987) (involving the search of a medical doctor's office by hospital administrators for disputed purposes).

28. *O'Connor*, 480 U.S. at 717.

29. *Id.* at 715.

30. *Id.*; *Katz*, 389 U.S. at 360–61 (Harlan, J., concurring).

still be reasonable and not in violation of the Fourth Amendment.[31] As such, the Supreme Court believes public employers must be given wide latitude when conducting work-related, non-investigatory searches, as well as for investigations of employee misconduct.[32] Whether a warrantless search by a government-employer that violates the reasonable expectations of privacy of an employee is permissible depends on the reasonableness of the intrusion,[33] which is determined by a two-step process: first, whether the action was justified at its inception; and second, whether the search as actually conducted was reasonably related in scope to the circumstances which justified the intrusion in the first place.[34]

As noted above, the Supreme Court reaffirmed the *O'Connor v. Ortega* plurality in *City of Ontario, California v. Quon*.[35] In *Quon*, the City of Ontario, California issued pagers to its SWAT officers, including Jeff Quon, to help them mobilize and respond to emergency situations.[36] The City had a "Computer Usage, Internet and E-Mail Policy," which stated employees should not have an expectation of privacy in e-mail messages. Although the Policy did not explicitly mention text messages,[37] the record indicates Quon was informed that the City considered text messages to be just like e-mail messages.[38]

---

31. *See O'Connor*, 480 U.S. at 719–20 ("In the case of searches conducted by a public employer, [courts] must balance the invasion of the employees' legitimate expectations of privacy against the government's need for supervision, control, and the efficient operation of the workplace.").

32. *Id.* at 723–24. The primary justification for this approach is that "in contrast to law enforcement officials . . . public employers are not enforcers of the criminal law; instead, public employers have a direct and overriding interest in ensuring that the work of the agency is conducted in a proper and efficient manner." *Id.* at 724. *But cf.* U.S. v. Warshak, 631 F.3d 266, 274, 283–89 (6th Cir. 2010) (holding that warrantless government seizure of defendant's e-mail messages during criminal investigation violated his Fourth Amendment rights).

33. *O'Connor*, 480 U.S. at 726.

34. *Id.* ("Ordinarily, a search of an employee's office by a supervisor will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file. . . . The search will be permissible in its scope when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the nature of the misconduct.") (citation, internal quotation marks, and alterations omitted).

35. 130 S. Ct. 2619 (2010).

36. *Id.* at 2625.

37. The type of electronic messages that could be sent and received through the City-provided pagers.

38. *Id.* at 2625.

The City provided the pagers through an outside vendor, Arch Wireless, which charged the City a monthly base rate, plus additional fees for usage in excess of a set number of alphanumeric characters.[39] Quon, along with a few additional officers, quickly exceeded the monthly base usage allotment for their individual pagers.[40] The SWAT team's supervisor, Lieutenant Duke, told Quon and the other SWAT officers that as long as they paid the overage fees, he would not audit their pager text messages.[41] Over the next few months, Quon and other SWAT officers exceeded their monthly base allotment of characters sent and received and paid the overage charges for their individual pagers.[42] Over time Duke grew tired, as he put it, of "being a bill collector."[43] The Chief of Police then decided to audit the pager messages, ostensibly "to determine whether the existing character limit was too low—that is, whether officers such as Quon were having to pay fees for sending work-related messages—or if the overages were for personal messages."[44] An audit of text messages sent and received by Quon revealed that in one month alone, Quon sent or received 456 messages during work hours, of which no more than fifty-seven were work related.[45] As a result, Quon was "allegedly" disciplined.[46]

Quon, along with some of those with whom he communicated via his City-provided pager, sued the City and Arch Wireless for, inter alia, violation of their Fourth Amendment rights. Although the District Court agreed Quon had a reasonable expectation of privacy in the pager messages, it ruled that if a jury found the purpose of the audit was to determine the efficacy of the pager text limits, the City did not violate Quon's Fourth Amendment rights.[47]

---

39. *Id.*

40. *Id.* at 2625–26.

41. *Id.* at 2625.

42. *Id.* at 2625–26.

43. *Id.* at 2626.

44. *Id.*

45. *Id.*

46. *Id.* None of the court opinions specify whether Quon was directly disciplined as a result of his personal pager messages, though his personal use of the pagers resulted in an internal affairs investigation. *See, e.g.*, Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1127 (C.D. Cal. 2006), *aff'd in part, rev'd in part*, 529 F.3d 892, 898 (9th Cir. 2008), *rev'd sub nom.* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010). The District Court did explain one possible indirect negative impact for Quon as a result of the review of his pager messages: many of the messages were between Quon and his then-mistress, who had earlier been dismissed as a dispatcher for the City of Ontario due to improper conduct; Quon's then-wife believed she was denied a job with a different police force when Quon's messages with his mistress came to light. *Arch Wireless*, 445 F. Supp. 2d at 1127–28.

47. *Id.* at 1146. The District Court granted Arch Wireless's motion for summary judgment. *Id.* at 1138.

The Ninth Circuit Court of Appeals reversed, in part, agreeing Quon had a reasonable expectation of privacy, but ruling the search was unreasonable because it was not conducted in the least intrusive manner possible.[48]

In a nearly unanimous decision, the Supreme Court reversed the Ninth Circuit.[49] The Court held that even assuming Quon had a reasonable expectation of privacy in his text messages and that the City's review of those messages constituted a search within the meaning of the Fourth Amendment,[50] because the search was motivated by a legitimate work-related purpose, and because the measures were not excessive in scope given this purpose, it was reasonable under the *O'Connor* plurality.[51]

As such, although the U.S. Supreme Court recognizes that public employees may have limited, reasonable expectations of privacy in the workplace, the public employer is still free to search employees' offices, communications, and private property as long as the search is not overly intrusive—i.e., as long as it has a rational work-related justification and is limited in scope to that work-related justification. As discussed more fully in Section II.C, *infra*, the Supreme Court did not provide much helpful guidance for when an employee has a reasonable expectation of privacy in the workplace, as well as what constitutes an overly intrusive search that can impermissibly invade an employee's right to privacy.

2. *Work-Related Rights to Privacy Under the Common Law*

Private-sector employees do not enjoy any Fourth Amendment rights vis-à-vis searches or surveillance by their employers under the U.S. Constitution.[52] Any work-related privacy rights that private employees may have are derived from a common law right to privacy developed among the states during the twentieth century. These common law rights to privacy consist of four categories: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false

48. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 908–09 (9th Cir. 2008), *reh'g denied en banc*, 554 F.3d 769 (2009), *rev'd sub nom.* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 (2010). The Ninth Circuit also reversed the granting of Arch Wireless's motion for summary judgment. *Id.* at 903.

49. Justice Scalia joined in all but Section III.A of the majority opinion. *Quon*, 130 S. Ct. at 2624.

50. *Id.* at 2630.

51. *Id.* at 2632.

52. Georgia v. Randolph, 547 U.S. 103, 146 (2006) (Thomas, J., dissenting) ("[O]nly the action of an agent of the government can constitute a search within the meaning of the Fourth Amendment . . . .") (citation omitted); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 614 (1989) ("[T]he Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative . . . .").

light in the public eye; and (4) commercial appropriation of a person's name or likeness.[53] Of these four types of common law rights to privacy, intrusion upon seclusion is the most common tort that private-sector employees allege when they believe their privacy has been invaded by their employer.[54] As with public-sector employees, a private-sector employee must also first have a reasonable expectation of privacy relative to the intrusion.[55] In addition, the

53. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960). These four invasions were later more formally codified in the Restatement. The first being: "Intrusion upon Seclusion[:] One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." RESTATEMENT (SECOND) OF TORTS § 652B (1997). Second: "Appropriation of Name or Likeness[:] One who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy." *Id.* § 652C. The third being:

> Publicity Given to Private Life[:] One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.

Id. § 652D. And the fourth:

> Publicity Placing Person in False Light[:] One who gives publicity to a matter concerning another that places the other before the public in a false light is subject to liability to the other for invasion of his privacy, if (a) the false light in which the other was placed would be highly offensive to a reasonable person, and (b) the actor had knowledge of or acted in reckless disregard as to the falsity of the publicized matter and the false light in which the other would be placed.

Id. § 652E. Although New York was the first state to enact a specific right to privacy statute, it was limited solely to the commercial appropriation of a person's name or likeness without permission. N.Y. C.P.L.R. § 50 (McKinney 2008). This New York statute was held constitutional in *Rhodes v. Sperry & Hutchinson Co.*, 85 N.E. 1097 (N.Y. 1908), *aff'd*, 220 U.S. 502 (1911); *see also* Robert E. Mensel, *"Kodakers Lying in Wait": Amateur Photography and the Right of Privacy in New York, 1885–1915*, 43 AM. Q. 24, 25 (1991) (noting New York was the first state to enact a privacy statute). New York does not recognize a common law right to privacy. *See* Chimarev v. TD Waterhouse Investor Servs., Inc., 280 F. Supp. 2d 208, 216 (S.D.N.Y. 2003) (citing Howell v. N.Y. Post Co., 612 N.E.2d 699, 703 (N.Y. 1993)).

54. *See, e.g.*, Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999); K-Mart Corp. Store No. 7411 v. Trotti, 677 S.W.2d 632 (Tex. App. 1984).

55. *See, e.g.*, *Thygeson*, 2004 WL 2066746, at *18–21 (holding that the employee did not have a reasonable expectation of privacy in e-mail messages accessed from work although stored in a personal e-mail account, where the employer prohibited such conduct); *McLaren*, 1999 WL 339015, at *4 (concluding that the employee did not have a reasonable expectation of privacy in e-mail messages sent across and stored on the employer's computer system; distinguishing *K-Mart Corp.*); *K-Mart Corp.*, 677 S.W.2d at 640 (holding that the employer intruded upon an area where the employee had a "legitimate expectation of privacy" by searching the employee's locker which was secured by the employee's personal lock).

common law tort of intrusion upon seclusion requires that the intrusion be highly offensive to be actionable.[56]

Although public and private sector employees' work-related rights to privacy derive from different sources, all employees working in the United States face a common constraint on these rights: the employee must have a reasonable expectation of privacy, i.e., an actual expectation "that society is prepared to recognize as 'reasonable.' "[57] Employers can destroy actual expectations through the use of notices and consent forms. However, as the following review of cases and surveillance methods shows, the level of detail and specificity of such notices must increase when the intrusiveness of the surveillance program increases.[58] As a result, it is possible that courts may raise the bar for sufficient detail in notices so high that it cannot practically be met with respect to overly intrusive technologies. After all, employers are subject to operational limitations; updating monitoring notices to capture every new type of technology and monitoring measure provides a practical challenge. Additionally, employers compete for talent, and disclosing overly intrusive monitoring practices would deter candidates and drive away talent.[59] But, courts have stopped at raising the bar for notices and thus far have not clearly acknowledged an absolute core of privacy expectations that is protected against notices and consent altogether.[60] With no such common

56. *See* RESTATEMENT (SECOND) OF TORTS § 652B; *see also McLaren*, 1999 WL 339015, at *5 (holding that even if the employee could establish a reasonable expectation of privacy in e-mail messages sent across and stored on the employer's computer system, the employer's interception of those messages was not highly offensive).

57. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

58. *See* discussion *infra* Section II.C.

59. Barry A. Friedman & Lisa J. Reed, *Workplace Privacy: Employee Relations and Legal Implications of Monitoring Employee E-mail Use*, 19 EMP. RTS. & EMP. POL'Y J. 75, 81 (2007).

60. *See, e.g.*, Feminist Women's Health Ctr. v. Superior Court, 61 Cal. Rptr. 2d 187, 196 (Ct. App. 1997) (holding that a health center's requirement that female health workers perform vaginal and cervical self-examinations in front of co-workers and patients did not violate a health worker's right to privacy because the health workers were notified of the requirement in written policies). In *Feminist Women's Health Center*, the employee argued that the self-examination requirement, which mandated that the plaintiff "disrobe and insert a speculum in [her] vagina in front of a group of health workers," was an egregious breach of her right to privacy as protected by the California Constitution. 61 Cal. Rptr. 2d at 195. The court held that "[t]he Center was not obligated to hire plaintiff, and consent remains a viable defense even in cases of serious privacy invasions." *Id.* at 196 (citing Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 657 (Cal. 1994)); *see also* Cramer v. Consol. Freightways, Inc., 209 F.3d 1122, 1131 (9th Cir. 2000) ("[P]rivacy rights can be altered or waived under California law and must be considered in context . . . ."), *amended en banc*, 255 F.3d 683 (9th Cir. 2001); Sporer v. UAL Corp., C 08-02835 JSW, 2009 WL 2761329, at *5 (N.D. Cal. Aug. 27, 2009) ("[H]aving advance notice that a company monitors computer use for compliance with the company's policies . . . and having an opportunity to consent to such monitoring,

law source, absolute core protections of employee privacy currently only arise from statutes, some of which establish very narrowly drafted prohibitions against monitoring that cannot be destroyed through unilateral notices.

3. Statutory Rights to Privacy

The United States has an amalgam of privacy statutes, enacted at different times, targeted for different purposes, and applicable to different entities.[61] Due to concerns arising from the growth of computer databases in the 1960s and 1970s,[62] Congress passed the Privacy Act of 1974, which regulates the collection and use of records by federal agencies.[63] The Act applies only to federal agencies, not to state or local agencies, nor to the private sector;[64] as such, its potential work-related application is limited to federal employers.[65] Most of the remaining federal privacy-related laws apply

---

further diminishes any reasonable expectation of privacy.") (citing TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 163–64 (Ct. App. 2002)); Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1077 (Cal. 2009) ("[N]otice of and consent to an impending intrusion can 'inhibit reasonable expectations of privacy . . . .' ") (quoting *Hill*, 865 P.2d at 655); *Hill*, 865 P.2d at 655 ("[E]ven when a legally cognizable privacy interest is present, other factors may affect a person's reasonable expectation of privacy[,] . . . [f]or example, advance notice of an impending action may serve to 'limit [an] intrusion upon personal dignity and security' that would otherwise be regarded as serious . . . ."); *TBG*, 117 Cal. Rptr. 2d at 160 ("Assuming the existence of a legally cognizable privacy interest, the extent of that interest is not independent of the circumstances, and other factors (including advance notice) may affect a person's reasonable expectation of privacy.") (citing *Hill*, 865 P.2d at 655).

61. *See, e.g.*, PAUL M. SCHWARTZ & DANIEL J. SOLOVE, INFORMATION PRIVACY: STATUTES AND REGULATIONS (2010–2011) (reproducing thirty-eight state and federal statutes addressing some element of information privacy).

62. Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1164–65 (2002).

63. 5 U.S.C. § 552a (2006). Although the Privacy Act gives individuals the right to access and correct information about themselves held by federal agencies, *id.* § 552a(d), and restricts the use of information by federal agencies only for relevant and necessary purposes, *id.* § 552a(e), in reality, it provides only minimal privacy protection for individuals. For example, information held by federal agencies may be disclosed to law enforcement entities and consumer reporting agencies, *id.* § 552a(b)(7), (12), as well as for any routine use that is compatible with the purpose for which the agency collected the information, *id.* § 552a(b)(3). This "routine use exception" has been described as a significant loophole which has done little to prevent disclosure of personal information. Solove, *supra* note 62, at 1167–68.

64. SCHWARTZ & SOLOVE, *supra* note 61, at 133.

65. Application of the Privacy Act would be limited to employment-related records of federal employees and potentially employees of federal contractors. The Supreme Court has granted certiorari to address the issues of whether the government violates a federal contract employee's constitutional right to informational privacy when: (1) it asks in the course of a background investigation whether the employee has received counseling or treatment for illegal drug use that has occurred within the past year, and the employee's response is used only for employment purposes and is protected under the Privacy Act; or (2) it asks the employee's designated references for any adverse information that may have a bearing on the

only to specific entities and specific types of information collection.[66] The vast majority of federal privacy statutes apply to records, not necessarily to searches, surveillance, or intrusions;[67] as such, they do not apply to employment relationships.

At the state and federal levels, there are statutes that nominally address workplace communications privacy. For example, two states, Connecticut and Delaware, have statutes regulating employer monitoring of employee communications and actions, requiring the employers to first provide notice to employees of such monitoring.[68] In addition, nine states have statutes that prohibit recording communications without the consent of all parties to the conversation.[69] In practice, two-way consent requirements cannot have much impact on workplace-internal communications and activities. For instance, California's statute specifically exempts communications "in which the parties to the communication may reasonably expect that the communication

employee's suitability for employment at a federal facility, the reference's response is used only for employment purposes, and the information obtained is protected under the Privacy Act. NASA v. Nelson, 130 S. Ct. 1755, 1755 (2010).

66. For example: the Gramm-Leach-Bliley Act, 15 U.S.C. § 6802 (2006), limits information sharing by financial institutions with third parties without prior consent by customers; the Privacy Protection Act, 42 U.S.C. § 2000aa (2006), restricts the search or seizures of work product materials in the possession of third parties by government officers; the Cable Communications Policy Act, 47 U.S.C. § 551 (2006), requires notice to cable customers of any disclosure of personal information; the Video Privacy Protection Act, 18 U.S.C. § 2710 (2006), prohibits video rental stores from disclosing customer video rental and purchase information; and the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104-191, 110 Stat. 1936 (1996) (codified as amended in scattered sections of titles 18, 26, 29, and 42 of the U.S. Code), regulates the disclosure of health information.

67. As for protecting records, the protections of the federal statutes are generally limited to when the records are in the "hands of third parties." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1148 (2002). In other words, "the statutory regime does not protect records based on the type of information contained in the records, but protects them based on the particular types of third parties that possess them." *Id.*

68. CONN. GEN. STAT. § 31-48d (2011); DEL. CODE ANN. tit. 19, § 705 (2010). Three states have recently introduced similar legislation including: Massachusetts (H.R. 1862, 186th Sess. (Mass. 2009)), New York (A3871-A S4755 (N.Y. 2009), and Pennsylvania (S.B. 363 (Pa. 2009)).

69. *See* California: CAL. PENAL CODE § 632(a) (Deering 2010); Connecticut: CONN. GEN. STAT. § 52-570d(a) (2011); Florida: FLA. STAT. § 934.03(2)(d), (3)(d) (2010); Illinois: 720 ILL. COMP. STAT. 5/14-2(a)(1) (2006); Maryland: MD. CODE ANN., CTS. & JUD. PROC. § 10-402(c)(3) (2011); Massachusetts: MASS. ANN. LAWS ch. 272, § 99(b)(4), (c)(1) (LexisNexis 2010); New Hampshire: N.H. REV. STAT. ANN. § 570-A:2(1-a) (2010); Pennsylvania: 18 PA. CONS. STAT. § 5704(4) (2010); Washington: WASH. REV. CODE § 9.73.030(1)(a) (2011).

may be overheard or recorded."[70] The statute would therefore not apply if employees had been provided notice that their work-related communications are subject to recording. Furthermore, the employer can make an employee's consent to recording a condition of continued employment. The situation is different with respect to monitoring of communications between employees and external parties (such as customers, distributors, suppliers, and personal contacts of employees). Employers may find it more challenging to rule out limited, reasonable expectations of privacy for such external parties, or to obtain consent from the same.[71]

The Federal Electronic Communications Privacy Act (ECPA)[72] can also apply to work-related monitoring. However, as discussed in Section II.B.3.a, *infra*, most of the ECPA's requirements are satisfied with one party's consent (so employers can marginalize its impact by providing notice to their employees) and its application has been somewhat challenging for the courts.

a) The Electronic Communications Privacy Act

In 1968, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[73] which became generally known as the "Wiretap

70. CAL. PENAL CODE § 632(c).

71. Increasingly, enterprises include notices about e-mail filtering and communications monitoring in outbound e-mail footers that are automatically included in all communications through company networks; however, such notices may not reach outsiders in advance of initial contact or at all with respect to communications through channels outside the control of the employer, such as webmail, instant messenger, and text messaging. *See* Lothar Determann & Lars Brauer, *Employee Monitoring Technologies and Data Privacy—No One-Size-Fits-All Globally*, 9 IAPP PRIVACY ADVISOR 1, 4 (2009) ("But it is more difficult to inform third-party Web sites or e-mail and text message recipients of monitoring practices, let alone ask for upfront consent (as the first message presumably is subject to the monitoring)."); Lothar Determann, *When No Really Means No: Consent Requirements for Workplace Monitoring in the U.S.*, 3 WORLD DATA PROTECTION REP. 22, at 2 (2003) ("Some employers implement recordings informing callers that 'all calls can be monitored [] for quality assurance' and some ask employees to include monitoring notices in their e-mail signatures, but such notices cannot reach all third parties, especially not in the arena of first-time electronic communications.").

72. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. I, 100 Stat. 1848, 1848–59 (codified as amended at 18 U.S.C. §§ 2510–2522 (2006)); tit. II, 100 Stat. at 1860–68 (codified at 18 U.S.C. §§ 2701–2711 (2006)); tit. III, 100 Stat. at 1868–73 (codified at 18 U.S.C. §§ 3121–3127 (2006)).

73. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 197, 212 (codified as amended at 18 U.S.C. §§ 2510–2520 (2006)). Title III not only prohibited general wiretapping and electronic eavesdropping but also established requirements for state and federal officials to obtain wiretapping and eavesdropping warrants.

Act."[74] While the Wiretap Act was "the primary law protecting the security and privacy of business and personal communications in the United States," it soon became "hopelessly out of date."[75] The Wiretap Act only proscribed unauthorized aural interception of wire or oral communications—it only applied where the contents of a communication could be overheard and understood by the human ear.[76] In addition, it applied only to interceptions of communications sent via common carriers.[77] By the mid-1980s, e-mail, computer-to-computer data transmissions, cellular and cordless phones, and video conferencing were becoming commonplace; telephone calls were being transmitted by wire, microwave, and fiber optics, often in the form of digitized voice, data, and video. Additionally, many different companies, not just common carriers, were offering telephone and communications services.[78] Not only were the technological means of communication advancing, but so too were the surveillance devices and techniques to monitor such communications.[79] A 1985 Office of Technology Assessment report concluded that existing protections against telephone[80] and e-mail surveillance were "weak, ambiguous, or nonexistent."[81]

In 1986, recognizing that technology was surpassing the protections afforded by the Wiretap Act,[82] Congress recast the Wiretap Act as the Electronic Communications Privacy Act.[83] Title I of the ECPA addresses the interception of wire, oral, and electronic communications; Title II addresses

74. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 n.7 (3d Cir. 2003) ("The Wiretap Act was formally known as the 1968 Omnibus Crime Control and Safe Streets Act . . . . [I]t was superseded by the ECPA.").

75. S. REP. NO. 99-541, at 2 (1986) (internal quotations omitted).

76. *Id.* (citing United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)).

77. *Id.* (citing 18 U.S.C. § 2510(10) (1968)).

78. *Id.* at 2–3.

79. *Id.* at 3.

80. OFFICE OF TECH. ASSESSMENT, U.S. CONGRESS, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES 29, 30 (1985), *available at* http://www.fas.org/ota/reports/8509.pdf.

81. *Id.* at 45.

82. *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 1–2 (1986) (statement of Rep. Robert Kastenmeier).

83. *See* statutes cited *supra* note 72; *see also* GINA STEVENS & CHARLES DOYLE, CONGRESSIONAL RESEARCH SERV., PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 6–7 (2008), *available at* http://digital.library.unt.edu/ark:/67531/metacrs10538/m1/1/high_res_d/98-326_2008Sep02.pdf.

access to stored wire and electronic communications and transactional records; and Title III addresses pen registers and trap and trace devices.[84]

Title I of the ECPA, still generally referred to as the Wiretap Act, makes punishable the intentional: (1) interception, or attempted interception, of "any wire, oral, or electronic communication;"[85] (2) use, or attempted use, of "any electronic, mechanical, or other device to intercept any oral communication;"[86] (3) disclosure, or attempted disclosure, "to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the ECPA];"[87] or (4) the use, or attempted use, of "the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of [the ECPA]."[88] Violations of the

84. S. REP. NO. 99-541, at 2–3. Titles I and II of the ECPA are discussed in more detail *infra*. A pen register device records outgoing address or routing information regarding a communication, *see generally* 18 U.S.C. § 3127(3) (2006 & Supp. 2009), while a trap and trace device records incoming address or routing source-identifying information, *see generally* 18 U.S.C. § 3127(4) (2006).

85. *See* 18 U.S.C. § 2511(1)(a) (2006 & Supp. 2008).

86. *See id.* § 2511(1)(b).

87. *See id.* § 2511(1)(c).

88. *See id.* § 2511(1)(d). The ECPA also prohibits the intentional disclosure, or attempted disclosure, to any other person the contents of any wire, oral, or electronic communication, intercepted by authorized means, where (1) there is knowledge that the communication was intercepted in connection with a criminal investigation; (2) the information was obtained or received in connection with a criminal investigation; and (3) there is intent to improperly obstruct, impede, or interfere with a duly authorized criminal investigation. *See id.* § 2511(1)(e). The ECPA defines "wire communication" as:

> [A]ny aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce[.]

Id. § 2510(1). "Oral communication" is defined as "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication[.]" *Id.* § 2510(2). "Electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include . . . any wire or oral communication." *Id.* § 2510(12). As such, "a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and

ECPA carry criminal penalties.[89] In addition, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of [the ECPA]" may bring a civil action for relief, including equitable relief, money damages, and attorney's fees.[90]

Title II of the ECPA, the Stored Communications Act (SCA), makes it unlawful to access stored communications. The ECPA defines electronic storage as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and . . . any storage of such communication by an electronic communication service for purposes of backup protection of such communication."[91] The SCA prohibits, with the threat of fines and imprisonment: "(1) intentionally access[ing] without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceed[ing] an authorization to access that facility; and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ."[92] Similar to the Wiretap Act, the SCA provides civil remedies for anyone aggrieved by a violation of the Act.[93]

The purpose of the SCA is to address "the growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the public."[94] For example, while there is no violation of the SCA when a subscriber accesses her own stored e-mail messages, "[a]ccessing the storage of other subscribers without specific authorization to do so would be a violation . . . ."[95] "Similarly, a member of the general public authorized to access the public portion of a computer facility would violate . . . [the SCA] by intentionally exceeding that authorization and accessing the private portions of the facility."[96]

While the goals of the ECPA appear to be quite straightforward, applying the ECPA has been wrought with difficulty, particularly for alleged violations arising from the workplace. Almost from its inception, the language used within the ECPA has been subject to highly technical parsing to determine

cannot fairly be characterized as containing the human voice." S. REP. NO. 99-541, at 14. "This term also includes electronic mail . . . ." *Id.*

89. *See* 18 U.S.C. § 2511(4)(a).
90. *See id.* § 2520(a)–(b).
91. *Id.* § 2510(17).
92. *Id.* § 2701(a).
93. *Id.* § 2707.
94. S. REP. NO. 99-541, at 35 (1986).
95. *Id.* at 36.
96. *Id.*

the Act's application in the workplace. It has not been regarded as a model of statutory clarity.[97] Part of the difficulty with the ECPA has been the interplay between Title I (Wiretap Act), which prohibits the interception of wire, oral, and electronic communications, and Title II (SCA), which protects stored wire and electronic communications and transaction records.[98]

Ironically, although the principal motivation to update the 1968 Omnibus Crime Control and Safe Streets Act with the 1986 ECPA was because statutory protections against electronic eavesdropping had, as discussed *supra*, become out of date, the ECPA itself was quickly found to be behind the technological curve.[99] For example, in *Konop v. Hawaiian Airlines, Inc.*, when the Ninth Circuit Court of Appeals addressed whether an employer's executive had accessed an employee's (Konop's) private website without authorization in violation of the SCA, the court noted: "[T]he ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website."[100]

Konop had restricted access to his website to only pre-approved individuals, mostly pilots and other employees of Hawaiian Airlines.[101] A Hawaiian Airlines vice president asked for and received access information for Konop's website from two pilots Konop had pre-approved.[102] The vice president then used that information to access and read Konop's website.[103] "Section 2701(c)(2) of the SCA allows a person to authorize a third party's access to an electronic communication if the person is (1) a user of the

97. *See, e.g.*, Steve Jackson Games, Inc. v. United States, 36 F.3d 457, 462 (5th Cir. 1994) (referring to the Wiretap Act as "famous (if not infamous) for its lack of clarity"); Forsyth v. Barr, 19 F.3d 1527, 1542–43 (5th Cir. 1994) ("[C]onstruction of the Wiretap Act is fraught with trip wires.").

98. *See, e.g.*, United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998) ("[T]he intersection of the Wiretap Act and the Stored Communications Act is a complex, often convoluted, area of the law.") (citations omitted).

99. *See, e.g.*, Jeremy U. Blackowicz, Note, *E-mail Disclosure to Third Parties in the Private Sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80, 104 (2001) ("Commentators are practically unanimous in calling for statutory solutions in the form of both amendments and revisions to the ECPA or a new statutory scheme to give employees some form of protection.") (citation omitted); Lee Nolan Jacobs, *Is What's Yours Really Mine?:* Shmueli v. Corcoran Group *and Penumbral Property Rights*, 14 J.L. & POL'Y 837, 876 (2006) ("With the continued evolution of technology, any protections afforded by the ECPA have become practically irrelevant.") (citation omitted).

100. 302 F.3d 868, 874 (9th Cir. 2002).

101. *See id.* at 872.

102. *See id.* at 873.

103. *See id.*

service and (2) the communication is of or intended for that user."[104] The *Konop* court noted "some indication in the legislative history that Congress believed addressees or intended recipients of electronic communications would have the authority under the SCA to allow third parties access to those communications."[105] Therefore, the Hawaiian Airlines executive would not have violated the SCA if he gained access to Konop's website by using information obtained from authorized users. However, the individuals from whom the executive obtained the access information had never actually *used* Konop's website; therefore they were never "users" under the language of the SCA. The *Konop* court relied on this technicality and perhaps overly-literal interpretation of the statute to reverse the district court's grant of summary judgment dismissing Konop's SCA claim.[106]

Exceptions within the ECPA also render much of the Act inapplicable to ordinary uses of computer and communications systems within the workplace. Section 2511(2)(a)(i) exempts officers, employees, and agents of a wire or communications service provider from liability for intercepting, disclosing, or using communications transmitted over the service in the ordinary course of business.[107] Section 2511(2)(d) exempts from liability anyone who intercepts a communication who is a party to the communication, or where one of the parties has consented to interception.[108] Based on the language of these two sections, "employers who own and provide their own e-mail [and communications] systems are exempt from the ECPA's requirements."[109] Employers who outsource their e-mail and

104. *Id.* at 880 (quotations and citation omitted); *see also* 18 U.S.C. § 2701(c)(2) (2006).

105. *Konop*, 302 F.3d at 880 (citing H.R. REP. NO. 99-647, at 66–67 (1986)).

106. *See id.* The *Konop* court upheld the lower court's dismissal of Konop's Title I Wiretap Act claims, holding that in order to "intercept" the content of Konop's website, it would have to be acquired during transmission, not while in electronic storage, *id.* at 878, presumably in transmission from Konop's computer to the storage location of the website content versus in transmission from the storage location to someone else's computer. *See* Pietrylo v. Hillstone Rest. Group, No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009) (upholding a jury's verdict that an employer had violated the SCA by accessing without authorization an invitation-only private MySpace chat group maintained by an employee).

107. 18 U.S.C. § 2511(2)(a)(i) (2006).

108. *Id.* § 2511(2)(d). *See also* Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *5–6 (N.D. Cal. Aug. 27, 2009) (holding the employer's monitoring of employees' e-mail messages did not violate § 2511 because employees impliedly consented to monitoring by consenting to the employer's monitoring policy). *But see* Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("[K]nowledge of the *capability* of monitoring alone cannot be considered implied consent . . . .") (alteration in original) (citation omitted) (applying pre-ECPA § 2511).

109. Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 67 (2009).

communications systems to service providers can also rely on the exception when they work with their service provider to intercept employee communications.[110]

Although the SCA does not specifically reference e-mail,[111] as noted, *supra*, Congress clearly intended the SCA to protect against unauthorized access of e-mail messages. The SCA prohibits unauthorized access of communications while in electronic storage;[112] however, similar to § 2511(2)(a)(i) of the Wiretap Act, § 2701(c) of the SCA exempts from liability providers of the wire or electronic storage.[113] Courts have applied § 2701(c) to employers, holding they are exempt from liability under the SCA for accessing employee e-mail messages stored on their computer systems.[114] Because of the exemptions contained in both the Wiretap Act and the SCA, commentators are in general agreement that the ECPA is ineffective in providing employees with any privacy protections relative to work-related e-mail messages and other forms of wire and electronic communications.[115]

C. INTRUSIVE WORKPLACE MONITORING AND EMPLOYEE PRIVACY

Privacy rights afforded electronic communications have a complex history that provides little guidance as technologies evolve. The surreptitious "listening" to other people's conversations has evolved from literally standing outside a home to overhear conversations,[116] to tapping phone lines

110. Leonard Court & Courtney Warmington, *The Workplace Privacy Myth: Why Electronic Monitoring Is Here To Stay*, 29 OKLA. CITY U. L. REV. 15, 28–30 (2004).

111. *See id.* at 26.

112. 18 U.S.C. § 2701(a). *See also id.* § 2510(17) (defining "electronic storage" under the ECPA).

113. *Id.* § 2701(c).

114. *See* Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114–15 (3rd Cir. 2003).

115. *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, 299 (2002) ("[T]he ECPA is ineffective in regulating the employer/employee relationship.") (citation omitted); Porter II & Griffaton, *supra* note 9, at 66 (concluding the ECPA "provides employees little protection from the monitoring of their workplace electronic communications"); Lawrence E. Rothstein, *Privacy or Dignity?: Electronic Monitoring in the Workplace*, 19 N.Y.L. SCH. J. INT'L & COMP. L. 379, 401 (1999) (concluding the ECPA "has generally proven ineffective in protecting employees in the workplace from their employers' monitoring") (citation omitted). *See also* Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. REV. 331, 340 n.37 (2010) (summarizing commentators who have criticized application of the ECPA in the employment context).

116. "Eaves-droppers, or such as listen under walls or windows or the eaves of a house, to hearken after discourse, and thereupon to frame slanderous and mischievous tales, are a common nuisance and presentable at . . . [court]." 4 SIR W.M. BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 168–69 (Thomas B. Wait & Co. 1807).

to record conversations,[117] to today's incarnation of reviewing the keystrokes one types on a computer keyboard, revealing, along with passwords and the addresses of websites visited, the content of messages composed and sent to others.[118]

New instant photography and audio recording technologies prompted Warren and Brandeis in 1890 to call for a right "to be let alone."[119] In his later dissent in *Olmstead v. United States*, in which the Supreme Court ruled a warrantless wiretap of a telephone conversation did not violate the Fourth Amendment, Justice Brandeis warned that "in the application of a constitution, our contemplation cannot be only of what has been but of what may be."[120] The majority in *Katz v. United States* chose to re-evaluate the notion of eavesdropping in light of, at that time, "the vital role that the public telephone has come to play in private communication."[121]

In his dissent in *Katz*, Justice Black argued that changes in technology should not expand the reach of the Fourth Amendment.[122] This concern

---

117. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 456–57 (1928) (describing wire tapping as intercepting messages on telephones by inserting small wires along ordinary telephone wires); *see also* ROBERT ELLIS SMITH, BEN FRANKLIN'S WEB SITE: PRIVACY AND CURIOSITY FROM PLYMOUTH ROCK TO THE INTERNET 156 (2000) (describing one of the earliest known surreptitious recordings of a conversation, in 1895, in which a postal inspector hid a recording device in his top hat to successfully record the words of a lawyer suspected of the illegal use of the mail).

118. *See, e.g.*, Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *1 (E.D. Mich. Feb. 6, 2008) (describing a key logger as a program designed to record every keystroke made on the computer and store it in a text file on the computer's hard drive); United States v. Ropp, 347 F. Supp. 2d 831, 831 (C.D. Cal. 2004) (involving a key logger program that "recorded and stored the electronic impulses traveling down the cable between [the user's] keyboard and the computer to which it was attached").

119. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1880) ("The right to one's person may be said to be a right of complete immunity: to be let alone.")). "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' " *Id.*

120. 277 U.S. at 474 (Brandeis, J., dissenting) (internal quotation marks omitted). "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Id.*

121. 389 U.S. 347, 352 (1967).

122. Justice Black stated:

> Tapping telephone wires, of course, was an unknown possibility at the time the Fourth Amendment was adopted. But eavesdropping (and wiretapping is nothing more than eavesdropping by telephone) was . . . an ancient practice which at common law was condemned as a nuisance . . . . There can be no doubt that the Framers were aware of this

forms the crux of the uncertainty over the extent to which evolving technologies can invade one's privacy. In *Kyllo v. United States*, the Supreme Court addressed the extent to which new technologies should "shrink the realm of guaranteed privacy."[123] In *Kyllo*, the Supreme Court ruled that thermal imaging technology, used without a warrant to measure the heat emanating from a home and hence indicating whether marijuana was being grown inside, constituted a Fourth Amendment search requiring a warrant.[124] The Court reasoned that the warrant was required because information was gleaned through the use of technology that otherwise could not have been obtained without a physical "intrusion into a constitutionally protected area . . . ."[125]

But the Supreme Court has been quick to back away from an expansive application of *Kyllo*. In *Illinois v. Caballes*, the Supreme Court held contraband detected by a drug sniffing dog during a routine traffic stop did not fall within the realm of *Kyllo*.[126] The Court reasoned that the thermal imaging device at issue in *Kyllo* was able to detect lawful activity, particularly intimate details in a home, whereas "[a] dog sniff conducted during a concededly lawful traffic stop that reveals no information other than the location of a substance that no individual has any right to possess does not violate the Fourth Amendment."[127] And most recently in *Quon*, the Supreme Court expressed a cautious approach vis-à-vis technology: "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[128] In fact, the latter part of that statement reflects an important qualification in *Kyllo*'s holding: the Supreme Court held the use of thermal imaging technology constituted a Fourth Amendment search—"at least where . . . the technology in question is not in general public use."[129] As a result, as Justice Stevens noted in his *Kyllo*

---

practice, and if they had desired to outlaw or restrict the use of evidence obtained by eavesdropping, I believe that they would have used the appropriate language to do so in the Fourth Amendment.

Id. at 366 (Black, J., dissenting) (citations and internal quotation marks omitted).

123. 533 U.S. 27, 34 (2001).

124. *See id.*

125. *Id.* (citation and internal quotation marks omitted).

126. 543 U.S. 405 (2005).

127. *Id.* at 409–10.

128. 130 S. Ct. 2619, 2629 (2010). "A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted." *Id.* at 2630.

129. *Kyllo*, 533 U.S. at 34.

dissent, "the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[130]

The role of emerging technology is important because, ultimately, the right to privacy is dependent upon an individual's expectation of privacy. An individual's expectation of privacy must be both actual (subjective) and one that society is willing to accept as reasonable.[131] If and to the extent an individual employee can substantiate an actual expectation of privacy, the following question as to the reasonableness of such expectation—and hence the existence and scope of the employee's rights—depends upon societal norms.[132] The "reasonableness" assessment is contextual: it depends upon the circumstances of any particular event. It must therefore be determined on a case-by-case basis.[133] There is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."[134] As such, guidance on when actionable workplace privacy exists, or does not exist, can only arise from an examination of decisions exploring the various circumstances in which an employee claims an invasion of privacy by an employer. Before turning to the parameters of such examination, it is important to remember that such examination becomes relevant only where the employee can substantiate an *actual* expectation of privacy. In practice, it is largely up to the employer whether employees are allowed to nurture such an actual expectation of privacy. Employers can—and often do—destroy any actual expectation of privacy by notifying employees in painstaking detail about the existence and intrusiveness of monitoring and surveillance

130. *Id.* at 47 (Stevens, J., dissenting). In his majority opinion, Justice Scalia differentiated *Kyllo* from *California v. Ciraolo*, 476 U.S. 207 (1986), on the basis that discovering marijuana plants from an airplane flyover was not a Fourth Amendment search because such flights were routine, whereas use of thermal imaging technology was not routine. *Kyllo*, 533 U.S. at 39 n.6.

131. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* TBG Ins. Servs. Corp. v. Superior Court, 117 Cal. Rptr. 2d 155, 160 (Ct. App. 2002) ("When affirmative relief is sought to prevent a constitutionally prohibited invasion of privacy, the plaintiff must establish (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy.") (citation and internal quotation marks omitted) (applying CAL. CONST. art. I, § 1).

132. *See* Oliver v. United States, 466 U.S. 170, 178 n.8 (1984), *cited with approval in* O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

133. This is a clearly enunciated approach for public-sector employees. *See, e.g.*, *O'Connor*, 480 U.S. at 718 ("[T]he question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis."). While not stated so directly, courts do perform a case-by-case analysis to determine whether a private-sector employee has a reasonable expectation of privacy. *See, e.g.*, Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 WL 2066746, at *17–22 (D. Or. Sept. 15, 2004).

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

technologies deployed. Yet, occasionally employers find it difficult to keep up with technological progress, and notices become outdated. This allows for the growth of limited expectations of privacy in communication methods not covered by outdated employer notices. Also, during periods of economic growth or in industries with limited access to talent, employees gain market power, forcing employers to try harder to remain attractive to employees. In such circumstances, employers tend to keep notices and policies friendlier to employees. Thus, when notices become outdated or employees gain market power, actual expectations of privacy may develop and raise the question of whether they are "reasonable" in the face of deployments of intrusive monitoring technologies.

As a general matter, courts believe that in most circumstances, employees do not have a reasonable expectation of privacy in e-mail messages sent or received over their employer's computer systems.[135] Courts have also been reluctant to find a reasonable expectation of privacy for personal use of an employer-provided computer.[136] In particular, courts have taken the

135. *See, e.g.*, Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *6–7 (N.D. Cal. Aug. 27, 2009) (holding an employee had no expectation of privacy in e-mail messages transmitted on work computer because he was aware the employer would monitor such messages; noting the employee was fired after receiving an e-mail message containing a pornographic video from a non-employee friend and then forwarding the message to his personal e-mail account); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding an employee could not have "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") (applying Pennsylvania law); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4–5 (Tex. App. May 28, 1999) (holding an employee had no reasonable expectation of privacy in e-mail messages stored in a password-protected personal folder located on the employee's work computer). Indeed, some courts believe there is no appropriate expectation of privacy in e-mail messages once they have been sent to and received by a third party. *See, e.g.*, Rehberg v. Paulk, 598 F.3d 1268, 1281–82 (11th Cir. 2010); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001). *But see* United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (stating the contents of an e-mail message, like that of a letter, may deserve Fourth Amendment protection because it is expected to be read only by the intended recipient).

136. *See, e.g.*, United States v. Barrows, 481 F.3d 1246, 1249 (10th Cir. 2007) (holding 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); *TBG Ins. Servs. Corp.*, 117 Cal. Rptr. 2d at 163 (holding the employee had no reasonable expectation of privacy in personal files stored on an employer-provided computer because he was aware of the employer's computer use policy which stated the computer was not to be used for personal purposes and its content could be monitored at any time). *But see* Curto v. Med. World Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2006 WL 1318387, at *5–6 (E.D.N.Y. May 15, 2006) (holding an employee had a reasonable expectation of privacy in personal e-mail messages and files stored on and

approach that since employers routinely monitor employee work-related communications and computer use,[137] "the use of computers in the employment context carries with it social norms that effectively diminish the employee's reasonable expectation of privacy with regard to his use of his employer's computers."[138]

Similar to the determination of a reasonable expectation of privacy, there is no bright-line test for what constitutes a highly offensive intrusion upon seclusion.[139] One conclusion the Supreme Court clearly reached in *Quon* is that public employers do not have to use the least intrusive means possible in order to conduct a permissible warrantless search under the Fourth Amendment.[140] While courts will generally not tolerate surveillance for "repugnant" or "socially unprotected" reasons,[141] they have used a case-by-case approach to determine what is a highly intrusive invasion of privacy.[142]

---

then deleted by the employee from an employer-provided laptop computer used by the employee solely at her home and which was never connected or used through the employer's computer system).

137. *See, e.g.*, discussion *supra* note 7.

138. *TBG Ins. Servs. Corp.*, 117 Cal. Rptr. 2d at 162.

139. *See, e.g.*, Turnbull v. Am. Broad. Cos., No. CV 03-3554 SJO (FMOX), 2004 WL 2924590, at *13 (C.D. Cal. Aug. 19, 2004) ("[A] court determining the existence of 'offensiveness' would consider the degree of intrusion, the context, conduct and circumstances surrounding the intrusion, the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded.") (citation omitted); Hernandez v. Hillsides, Inc., 211 P.3d 1063, 1073 (Cal. 2009) (noting California tort law contains no bright line on determining the offensiveness of an intrusion).

140. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2632 (2010) ("This Court has repeatedly refused to declare that only the least intrusive search practicable can be reasonable under the Fourth Amendment.") (citation and internal quotation marks omitted).

141. *See Hernandez*, 211 P.3d at 1080 (identifying blackmail, harassment, and prurient curiosity as repugnant and socially unprotected reasons for surveillance) (citing Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 493 (Cal. 1998)).

142. *Compare id.* at 1073 *with* Nelson v. Salem State Coll., 845 N.E.2d 338 (Mass. 2006). In *Hernandez*, the employer secretly installed a hidden camera in a shared office space in an attempt to ascertain who was entering the office after hours to use a computer to access pornography. 211 P.3d at 1066. Although the California Supreme Court believed the employees had a reasonable expectation of privacy in their shared office space, *id.* at 1076, it ruled the employer's video monitoring was not overly intrusive because it was limited in scope and directly related to protecting the goals of the workplace (protecting abused children). *Id.* at 1082. In *Nelson*, the employer secretly installed a hidden camera in a shared office space based on concerns of after-hours unauthorized access to the work area. 845 N.E.2d at 343. The plaintiff sued her employer for invasion of privacy after she discovered she had been recorded by the video surveillance changing clothes in the office space. *Id.* at 341. Despite the fact that the camera was set to record twenty-four hours per day for the purpose of monitoring after-hours access, the plaintiff had locked the door to the office, and her activities were recorded just before and after regular business hours, the court ruled she

There is a close relationship between a reasonable expectation of privacy and the degree of permissible intrusiveness. As courts have shown, particularly in relation to workplace monitoring, where employees are aware the employer may intrude upon their privacy for legitimate business purposes, there can be no expectation of privacy.[143] Where the employer's monitoring goes beyond legitimate business purposes, however, and intrudes on what society may consider highly personal areas beyond the scope of work, then an actionable invasion of privacy may be found.[144] There are currently three areas where monitoring by employers may, according to social norms, be considered so personal as to constitute an inappropriate intrusion: access to personal web-based applications; use of webcams; and use of location-tracking technologies.

1. Employer Access to Personal Web-Based Applications

According to a recent survey on information technology policies in the workplace, over fifty percent of responding employees accessed personal web-based e-mail accounts from work using employer-provided computers, although only seventeen percent of the respondents said their companies permitted such conduct.[145] Courts have found that employees can have an expectation of privacy in e-mail messages stored on personal web-based e-mail services, even when they have accessed those services at work through

did not have a reasonable expectation of privacy within the office because other people had keys to the office and could have walked in on her at any time. *Id.* at 349.

143. *See, e.g.*, cases cited *supra* note 142.

144. *Compare* Phillips v. Smalley Maint. Servs., 711 F.2d 1524 (11th Cir. 1983) (finding an invasion of an employee's privacy based on the employer's repeated inquiries into the employee's sex life), Johnson v. K Mart Corp., 723 N.E.2d 1192, 1196–97 (Ill. App. Ct. 2000) (reversing summary judgment granted in favor of the defendant-employer as to plaintiffs' intrusion upon seclusion claims; holding the employer's investigation concerning workplace thefts, vandalism, and drug use went too deeply into personal lives of employees, beyond any business purpose), *and* Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 79, 86 (Ct. App. 1991) (holding 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), *with* Morenz v. Progressive Cas. Ins. Co., No. 79979, 2002 WL 1041760, at *2, *4 (Ohio Ct. App. May 23, 2002) (finding no invasion of privacy where the employer asked the employee if he was gay; concluding the purpose of the question, asked in private, was merely to ascertain the employee's job satisfaction and comfort living in the south). *See generally* 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, 632–34 (2004) (discussing when employers' monitoring stays within or goes beyond the scope of legitimate business purpose).

145. PONEMON INSTITUTE, TRENDS IN INSIDER COMPLIANCE WITH DATA SECURITY POLICIES 7 (2009), http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/Trends%20in%20Insider%20Compliance%20with%20Policies%20Final%203.pdf.

employer-provided computer systems. For example, in *Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC*, the court made three specific conclusions in finding an employee had a reasonable expectation of privacy in personal e-mail messages stored on a third party's service, although the employee had accessed that outside service while at work, using employer-provided equipment.[146] The *Pure Power Boot Camp* court found that: (1) an employer's access of personal e-mail messages from an employee's web-based e-mail service without authorization violates the SCA;[147] (2) an employer's computer use and e-mail policy which explicitly prohibited personal use of the Internet at work and provided notice that all e-mail messages could be monitored did not create an implied consent on the part of the employee that his personal e-mail messages stored with an outside service provider could be monitored, even though the employee had accessed the outside service provider at work using employer-provided equipment;[148] and (3) the fact that the employee's username and password to a personal web-based e-mail account were later automatically filled in on the employee's work computer because of the employee's earlier access to the account did not imply authorization for others to access the employee's account.[149]

Stengart v. Loving Care Agency, Inc. also involved an employee's correspondence with her attorney through personal e-mail messages stored on a third-party web-based system.[150] Rather than access the messages directly through the service, Stengart's employer accessed copies of her messages that had been automatically stored on her company-provided laptop computer.[151] Although the employer's computer use policy warned that e-mail messages "are not to be considered private or personal," the court noted the policy did not provide any express notice that messages sent or received on a personal, web-based e-mail account would be subject to monitoring if company equipment was used to access the account.[152] The court concluded that Stengart had a reasonable expectation of privacy in her personal e-mail correspondence with her attorney because of the steps she

146. 587 F. Supp. 2d 548 (S.D.N.Y. 2008).

147. *Id.* at 556.

148. *Id.* at 559. The e-mail messages were "personal" in that they were in no way related to the employer's business. *See id.* at 560.

149. *Id.* at 561 (providing the analogy that had the employee left a key to his house on his desk, that would not imply authorization for anyone else to use the key to "rummage" through his house).

150. 990 A.2d 650 (N.J. 2010).

151. *Id.* at 655–56.

152. *Id.* at 659.

took to protect the privacy of those messages. In particular, she used "a personal, password-protected e-mail account instead of her company e-mail address and did not save the account's password on her computer."[153]

Pietrylo v. Hillstone Restaurant Group, though not involving e-mail messages, is similar in facts to *Konop*.[154] In *Pietrylo*, a supervisor "coerced" an employee to provide access to information in a restricted communications area within a MySpace account in which employees were making comments critical of their employer and management.[155] The court ruled such access was unauthorized and in violation of the SCA.[156] These cases indicate a clear willingness on the part of the courts to consider e-mail and other types of electronic messages stored on personal web-based accounts to be within a zone in which employees have a reasonable expectation of privacy. Furthermore, an employer's invasion of this zone constitutes an actionable invasion of privacy.

2. Webcams

Webcams and cameras built into laptop computers are becoming ubiquitous in the workplace. Worldwide sales of webcams are predicted to increase from $1.2 billion in 2006 to $6.2 billion by 2013.[157] Employers are no longer only using webcams for video conferencing or virtual training; they are also beginning to use webcams for employee monitoring.[158] Webcams built into laptop computers raise the potential of intrusive employer monitoring beyond the physical bounds of "traditional" workplace video monitoring.

A recent survey of workplace monitoring reveals that nearly fifty percent of employers use video monitoring to counter theft, violence, and sabotage.[159] As a general matter, courts find no objection to video monitoring

153. *Id.* at 663. *See also In re* Asia Global Crossing, Ltd., 322 B.R. 247, 259–61 (Bankr. S.D.N.Y. 2005) (holding certain executives had an expectation of privacy in personal e-mail messages sent through the company's e-mail system because the company's computer use policy was equivocal regarding certain uses and monitoring); Nat'l Econ. Research Assocs., Inc. v. Evans, No. 04-2618 BLS2, 2006 WL 2440008, at *3–5 (Mass. Super. Ct. Aug. 3, 2006) (holding same on similar facts).

154. Pietrylo v. Hillstone Restaurant Grp., No. 06-5754 (FSH), 2009 WL 3128420 (D.N.J. Sept. 25, 2009); *see* discussion *supra* Section II.B.3.a. regarding Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002).

155. *Pietrylo*, 2009 WL 3128420, at *3.

156. *Id.*

157. Michelle V. Rafter, *Smile, You're on the Company Webcam*, INC. TECH. (Mar. 1, 2008), http://technology.inc.com/hardware/Articles/200803/webcams.html.

158. *Id.*

159. AMA & EPOLICY INST., *supra* note 7, at 3 (reporting also that only seven percent of employers use video surveillance to track employees' on-the-job performance).

in open workplaces.[160] Where courts require more detailed and specific notices to negate a reasonable expectation of privacy on the employee's side is surveillance of areas in which employees tend to have a greater actual expectation of privacy: restrooms and dressing rooms.[161] But, even with respect to highly sensitive circumstances, courts have not acknowledged a core expectation of privacy that is protected against waivers, consents, and notices as a matter of public policy.[162] In some cases, state legislatures have stepped in and prohibited certain forms of surveillance outright. For example, section 435 of the California Labor Code prohibits "audio or video

160. For example, in *Vega-Rodriguez v. Puerto Rico Telephone Co.*, the court explained:

> [N]o legitimate expectation of privacy exists in objects exposed to plain view as long as the viewer's presence at the vantage point is lawful. And the mere fact that the observation is accomplished by a video camera rather than the naked eye, and recorded on film rather than in a supervisor's memory, does not transmogrify a constitutionally innocent act into a constitutionally forbidden one.

110 F.3d 174, 181 (1st Cir. 1997) (citation and footnote omitted); *see also* Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 651 (N.D. Ill. 2005) (holding the use of hidden cameras in an open office setting does not automatically transform a non-private area into a private one).

161. *See, e.g.*, Williams v. City of Tulsa, Okla., 393 F. Supp. 2d 1124, 1137–38 (N.D. Okla. 2005), *aff'd*, 204 F. App'x 762 (10th Cir. 2006) (holding city could potentially be liable for violations of the Fourth Amendment and the ECPA as well as for intentional infliction of emotional distress for alleged surreptitious video monitoring of the restroom, but the plaintiffs did not present sufficient evidence it had occurred). The court had no issue with video cameras hidden in clocks which recorded activities in general work areas, *id.* at 1134, nor with audio recording equipment discovered in the air conditioner vent above one supervisor's office, *id.* at 1134–36. *See also* Rosario v. United States, 538 F. Supp. 2d 480 (D.P.R. 2008) (denying employer Department of Veterans Affairs' motion to dismiss employee's Fourth Amendment violation of privacy claims based on video surveillance of locker room); Trujillo v. City of Ontario, 428 F. Supp. 2d 1094 (C.D. Cal. 2006), *aff'd sub nom.* Bernhard v. City of Ontario, 270 F. App'x 518 (9th Cir. 2008) (holding male police officers had a reasonable expectation of privacy against video surveillance in their locker room where employer did not provide notice of surveillance). *But see* Thompson v. Johnson Cnty. Cmty. Coll., No. 96-3223, 1997 WL 139760, at *2 (10th Cir. Mar. 25, 1997) (unpublished opinion) (holding employees had no expectation of privacy in locker area which was located in a room that housed heating and air conditioning equipment and a storage area and for which access was not restricted). An interesting variation on dressing room surveillance, but which highlights the contextual nature of the expectation of privacy, is found in *Bevan v. Smartt*, 316 F. Supp. 2d 1153, 1160–61 (D. Utah 2004) (holding night club dancers had no expectation of privacy vis-à-vis video surveillance of their dressing room by club security personnel, but the dancers did have an expectation of privacy when government agents viewed the same surveillance without a warrant). *See also* Colorado v. Galvadon, 103 P.3d 923 (Colo. 2005) (holding same as to store manager and video surveillance of back room in store with no public access).

162. Feminist Women's Health Ctr. v. Superior Court, 61 Cal. Rptr. 2d 187, 196 (Ct. App. 1997).

recording to be made of an employee in a restroom, locker room, or room designated by an employer for changing clothes, unless authorized by court order."[163] But, the existence of such narrowly-drafted statutes only confirms the general rule that—in the absence of such statutes—employers can destroy the expectation of privacy with detailed notices.

One key concern with webcams is their portability when installed in a laptop computer. They can record an employee's conduct in front of the computer while the employee is at work, at home, or even in a hotel room while traveling on business. The employee may not know if the webcam is activated, or even if it is installed on the laptop being used. While there have not been any reported claims of violations of privacy by employers activating laptop webcams, there has been at least one highly-publicized case involving laptop webcams.

In November 2009, a Pennsylvania high school student and his family learned the school district had obtained video images of the student allegedly engaging in improper behavior in his home from the student's district-issued laptop computer webcam.[164] The webcam on this particular student's laptop computer, like the ones on all the district-issued laptops, could be activated and monitored remotely without the student's or his family's knowledge.[165] The plaintiff alleged the school district had thousands of photos of students in their homes, including some showing students or the family sleeping or in various states of undress.[166] Although the FBI opened an investigation into the incident,[167] authorities decided not to prosecute because they concluded

163. CAL. LAB. CODE § 435(a) (Deering 2010). In addition, this prohibition cannot be waived or derogated from by notice: "No recording made in violation of this section may be used by an employer for any purpose. This section applies to a private or public employer, except the federal government." *Id.* § 435(b). This provision "represent[s] society's understanding that a locker room is a private place requiring special protection." *Trujillo*, 428 F. Supp. 2d at 1106.

164. Complaint at 6, Robbins v. Lower Merion Sch. Dist., No. 10-CV-00665-JD (E.D. Pa. Feb. 16, 2010). The student's allegedly improper behavior was ingesting drugs while using the laptop; in fact, the student was eating candy at the time. John P. Martin, *1,000s of Web Cam Images, Suit Says*, PHILA. ENQUIRER, Apr. 16, 2010, at A1.

165. Complaint, *supra* note 164, at 7.

166. Motion for Sanctions ¶¶ 2, 4, *Robbins*, No. 10-CV-00665-JD (Apr. 15, 2010), ECF No. 44.

167. *See* Order, *Robbins*, No. 10-CV-00665-JD (May 10, 2010), ECF No. 61 (allowing the Government access to the school district's computers and servers); Press Release, Dep't. of Justice, Inquiry into Lower Merion School District Activating Web Cams on Student Issued Computers (Feb. 22, 2010), http://philadelphia.fbi.gov/dojpressrel/pressrel10/ph022210a.htm.

there was no criminal intent on the part of the school district's employees.[168] The school district subsequently settled all cases brought against it by students.[169]

An employer's use of webcams to monitor employee behavior at home can be particularly troublesome for employers. The Supreme Court clearly identifies the home as a bastion of intimacy and privacy.[170] While most courts have ruled against an invasion of privacy based on video recording in the workplace, courts often draw the line in areas society perceives to be intimate.[171] It is within these areas of intimacy that individuals have a reasonable expectation of privacy, an invasion of which could easily be perceived as highly offensive.

3. GPS

Location-tracking technologies allow employers to monitor the exact location of employees, both at the workplace and off-site. One of the principal means of location-tracking, Global Positioning System (GPS) devices, and its employee privacy implications, are discussed in this Section.

GPS uses a satellite positioning system to record both the precise location of a GPS device—as well as the person carrying or using such a device—and the time of positioning.[172] GPS devices are typically installed in vehicles as well as cell phones and can provide tracking information such as the route travelled, the address of all stops, the duration of stops, the amount of time spent traveling between stops, the maximum speed between stops, and whether the device (or person) has entered or exited a pre-determined boundary.[173] Employers primarily use GPS devices to track employee use of vehicles, often to ensure employees are going where they are supposed to be

168. *See* Press Release, Dep't. of Justice, No Criminal Charges Filed Following Lower Marion School District Student Computer Monitoring Investigation (Aug. 17, 2010), http://philadelphia.fbi.gov/dojpressrel/pressrel10/ph081710.htm.

169. Chloe Albanesius, *Pa. School District Settles Webcam Spying Case for $610K*, PCMAG.COM (Oct. 12, 2010), http://www.pcmag.com/Article2/0,2817,2370622,00.asp.

170. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

171. *See supra* notes 160–61.

172. *See* Mason Weisz, *Monitoring Employee Location with GPS and RFID in 2005: Workplace Privacy Issues*, *in* WORKPLACE PRIVACY: PROCEEDINGS OF THE NEW YORK UNIVERSITY 58TH ANNUAL CONFERENCE ON LABOR 69, 78–79 (Jonathan Remy Nash & Samuel Estreicher eds., 2010); *see also* Jill Yung, *Big Brother IS Watching: How Employee Monitoring in 2004 Brought Orwell's* 1984 *to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 170–72 (2005) (providing a description of GPS technology).

173. *See* Weisz, *supra* note 172, at 80.

going and not wasting time during or in between trips.[174] Though recent surveys indicate employers have been slow to adopt GPS technology,[175] the National Workrights Institute predicts work-related GPS tracking will increase because the technology is quickly becoming an affordable option for small businesses.[176]

As with other forms of work-related monitoring, the privacy implications of GPS tracking are unsettled. California is the only state with a statute directly addressing GPS tracking, prohibiting any person or entity within the state from using "an electronic tracking device to determine the location or movement of a person."[177] However, the statute still permits employers to use GPS devices to track the location of their vehicles.[178] Some commentators have concluded that GPS tracking does not fit within any of the types of communications covered under the ECPA.[179]

---

174. *See, e.g.*, *id.* at 81 (recounting a trash hauling business that reduced weekly overtime claims from 300 to 70 hours after installing GPS devices in the company's trucks; also noting transit systems combine GPS with weather and traffic monitoring systems to predict arrival times); Johnathon Williams, *Get a Handle on Your Overhead: Technology Is Making It Easier for You To Keep Tabs on Your Business's Resources*, ENTREPRENEUR, Apr. 21, 2009, http://www.entrepreneur.com/article/201342 (describing one employer who gave employees a per diem for hotels on business trips of over 150 miles only to learn through GPS tracking that some employees were instead driving to and from the work site each day, pocketing the per diem and increasing the mileage and gasoline costs for the company vehicles).

175. *See, e.g.*, AMA & EPOLICY INST., *supra* note 7, at 3 (reporting that only eight percent of employers used GPS to track company vehicles and only three percent used GPS to track company-provided cell phones).

176. NAT'L WORKRIGHTS INST., ON YOUR TRACKS: GPS TRACKING IN THE WORKPLACE 5–6, http://workrights.us/wp-content/uploads/2011/02/NWI_GPS_Report.pdf (last visited Mar. 29, 2011); *see also* Williams, *supra* note 174 (noting that the CEO of a company providing GPS tracking services claims sales have recently grown in "astronomical proportions").

177. CAL. PENAL CODE § 637.7(a) (Deering 2010).

178. *Id.* § 637.7(b) ("This section shall not apply when the registered owner, lessor, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle."). Though Connecticut has a statute requiring employers to give employees notice of any electronic monitoring, it is limited to the collection of information at an employer's premises. CONN. GEN. STAT. § 31-48d(3) (2011) (" 'Electronic monitoring' means the collection of information *on an employer's premises* concerning employees' activities or communications by any means other than direct observation . . . .") (emphasis added). Delaware's statute requiring employers to provide employees notice of electronic monitoring only applies to the monitoring or interception of any "telephone conversation or transmission, electronic mail or transmission, or Internet access or usage." DEL. CODE ANN. tit. 19, § 705(b) (2010). *See generally supra* Section II.B.3 (discussing Connecticut's and Delaware's statutory requirements that employers provide notice to employees of workplace electronic monitoring).

179. *See, e.g.*, Weisz, *supra* note 172, at 86.

As discussed *infra*, the contours of permissible GPS tracking are currently being established in federal criminal cases, addressing the constitutionality of warrantless GPS tracking. Though they are not directly applicable to employment scenarios, particularly in the private employment sector, as with *Katz v. United States*, these cases may lay the doctrinal foundation for determining the degree of privacy that may be afforded employees vis-à-vis employer use of GPS tracking.[180]

Most courts have held that the use of GPS devices to track the movements of criminal suspects does not require a warrant based on the U.S. Supreme Court's holding in *United States v. Knotts*.[181] In *Knotts*, a beeper device was attached to a drum of chemicals and then used by law enforcement agents to track the transport of the drum from its point of purchase to the suspect's secluded cabin.[182] The Supreme Court ruled the use of the device did not require a warrant because a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[183] The rationale used by the Court is that:

> One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view.[184]

However, in *United States v. Maynard*, the D.C. Circuit Court of Appeals held a suspect's reasonable expectation of privacy was violated by the FBI's warrantless continuous surveillance of the defendant for approximately one month through the installation of a GPS tracking device on the defendant's automobile.[185] The *Maynard* court considered *Knotts* inapplicable because *Knotts* concerned a discreet journey of approximately 100 miles, whereas the

180. 389 U.S. 347 (1967); *see* discussion *supra* Section II.B.2.

181. 460 U.S. 276 (1983); *see, e.g.*, United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007); United States v. Jesus-Nunez, No. 1:10-CR-00017-01, 2010 WL 2991229 (M.D. Pa. July 27, 2010). *But see* People v. Weaver, 909 N.E.2d 1195, 1201 (N.Y. 2009) ("The massive invasion of privacy entailed by the prolonged use of the GPS device was inconsistent with even the slightest reasonable expectation of privacy.").

182. *Knotts*, 460 U.S. at 277.

183. *Id.* at 281.

184. *Id.* (citation and internal quotation marks omitted).

185. 615 F.3d 544 (D.C. Cir.), *reh'g en banc denied*, 625 F.3d 766 (D.C. Cir. 2010), *cert. granted sub nom.* United States v. Jones, No. 10-1259, 2011 U.S. LEXIS 4956 (U.S. June 27, 2011).

surveillance in *Maynard* was continuous, twenty-four hours per day, lasting twenty-eight days.[186] As such, the *Maynard* court concluded the prolonged surveillance of the defendant's movements revealed an "intimate picture" of his life that he would expect no one else to have—i.e., he had a reasonable expectation of privacy in his movements over the course of the twenty-eight days.[187]

In contrast, the Ninth Circuit Court of Appeals has held that repeatedly monitoring a suspect's vehicle over a four-month period using various types of mobile tracking devices did not require a warrant.[188] The Ninth Circuit concluded the police obtained no more information than they could have by physically following the suspect and that the use of the tracking devices merely made their work more efficient, which is not unconstitutional.[189] When the Ninth Circuit denied a rehearing en banc, Judge Kozinski wrote in his dissent, "1984 may have come a bit later than predicted, but it's here at last."[190] Judge Kozinski differentiated the beeper technology at use in *Knotts* (which "could help police keep vehicles in view when following them, or find them when they lost sight of them," but "still required at least one officer[,] and usually many more[,] to follow the suspect[]") from current GPS technology (which "can record the car's movements without human intervention[,] quietly, invisibly, with uncanny precision").[191] Judge Kozinski's primary concern is that "[b]y tracking and recording the movements of millions of individuals the government can use computers to detect patterns and develop suspicions. It can also learn a great deal about us because where we go says much about who we are."[192]

Courts are beginning to re-examine the fundamental basis for *Knotts*—that location tracking outside the home is analogous to physical surveillance and therefore does not require a warrant—in light of evolving technology.[193] As expressed by the District Court for the Eastern District of New York:

---

186. *Id.* at 556, 558.

187. *Id.* at 563 (referencing Katz v. United States, 389 U.S. 347 (1967)).

188. United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010), *reh'g denied*, 617 F.3d 1120.

189. *Id.* at 1216.

190. United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010) (Kozinski, J., dissenting).

191. *Id.* at 1124.

192. *Id.*

193. *See, e.g.*, *In re* An Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 596 (E.D.N.Y. 2010) (concluding the Fourth Amendment prohibits as an unreasonable search and seizure an order for cell phone-based locational data in the absence of a showing of probable cause); *see also In re* An Application of

> [T]echnology has progressed to the point where a person who wishes to partake in the social, cultural, and political affairs of our society has no realistic choice but to expose to others, if not to the public as a whole, a broad range of conduct and communications that would previously have been deemed unquestionably private.[194]

Arguably, employers and employees may find themselves in an ever-changing landscape of privacy protection vis-à-vis the use of GPS tracking devices. Initially, most courts do not consider the use of such devices as an invasion of privacy. However, as their use becomes more sophisticated and continuous, revealing a portrait of personal activities versus merely a recording of location after location, courts begin to recognize an invasion of a reasonable expectation of privacy. This privacy protection may be lost, however, as reflected in the reasoning of *Kyllo v. United States*, once continuous GPS tracking becomes common.[195] U.S. laws condition privacy protections on "actual" expectations of privacy and recognize the validity of implied consent by employees who continue to show up for their "at will" employment. As long as these legal conditions remain, it is up to employers to specifically notify employees of all monitoring and surveillance practices, however intrusive the practices may be, and thus destroy any "actual" expectation of privacy.

D. WORKPLACE PRIVACY TRENDS IN THE UNITED STATES

Absent specific state laws limiting intrusive employee monitoring—which tend to be few and narrowly drafted—employers are free to destroy U.S. employees' expectations of privacy via detailed notices, and without an actual expectation of privacy, employee privacy is not protected against monitoring under federal law and general state privacy laws. The U.S. Supreme Court could have changed this situation in *Quon* by developing core privacy rights that cannot be destroyed or limited through notices, but the Court chose not to. Instead, the Court found it prudent to not "establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices."[196] The Court was not concerned with whether Quon had a reasonable expectation of privacy in his text communications; as long as it had a legitimate business purpose, the City of Ontario could review his text

---

the U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 10-MC-897 (NGG), 2011 U.S. Dist. LEXIS 93494 (E.D.N.Y. Aug. 22, 2011) (holding same).

194. *In re An Application*, 736 F. Supp. 2d at 582 (citations omitted).

195. *Kyllo*'s reasoning suggests that increased "general public use" might diminish an expectation of privacy. *See supra* Section II.C.

196. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010).

messages.[197] And when subsequently confronted with the question of whether employees had a reasonable expectation of work-related privacy, the Supreme Court again refused to discuss its contours. Instead, it merely assumed the existence of a right to informational privacy before deciding that legitimate employer needs justified investigatory background checks regarding employees' personal lives.[198]

Even without acknowledging a fundamental or core privacy right that is beyond destruction via employer notices, U.S. courts can protect employee privacy by holding the level of detail provided in employer notices to high and increasing standards. For example, if an employer notifies employees about e-mail monitoring in general terms, courts may find that such notice is not sufficient to destroy an expectation of privacy in private e-mail (even if accessed at work), text messaging, or instant messaging. But, the jurisprudence on this point is mixed and U.S. courts tend to interpret monitoring notices broadly in favor of employer monitoring, so long as the monitoring serves legitimate business purposes. For example, in *Stengart v. Loving Care Agency, Inc.*, the Superior Court of New Jersey ruled that an employee had a reasonable expectation of privacy in e-mail messages she sent to her personal attorney using an employer-provided computer.[199] However, the *Stengart* court declined to "attempt to define the extent to which an employer may reach into an employee's private life or confidential records through an employment rule or regulation."[200] And a California Court of Appeal, in a situation very similar to *Stengart*, held that an employee did not have a reasonable expectation of privacy in e-mail messages she sent to her personal attorney using an employer-provided computer because the employer had "unequivocally" informed its employees that those who used the company's computers to send personal e-mail would have "no right of privacy" in the information sent.[201]

In summary, we see two trends emerging from cases addressing employees' reasonable expectations of privacy in work-related

197. *Id.* at 2631.

198. NASA v. Nelson, 131 S. Ct. 746 (2011).

199. 973 A.2d 390, 401 (N.J. Super. Ct. App. Div. 2009) ("A policy imposed by an employer, purporting to transform all private communications into company property—merely because the company owned the computer used to make private communications or used to access such private information during work hours—furthers no legitimate business interest.") (citation omitted).

200. *Id.*

201. Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 896–97 (Ct. App. 2011) (internal quotation marks omitted). The *Holmes* court described the plaintiff's sending personal e-mails through the company's computer system as "akin to consulting her lawyer in her employer's conference room, in a loud voice, with the door open." *Id.* at 883.

communications. First, courts, particularly the U.S. Supreme Court, have shied away from acknowledging a core privacy right that employers cannot destroy by way of notice. Thus, employers in the United States are free to completely or partially destroy employee privacy expectations—and with the expectations, also destroy most forms of legal protections for data privacy under U.S. law, because privacy protections are conditioned on privacy expectations. Second, any limited expectation of privacy that may exist due to too narrowly or poorly drafted employer notices can be negated based on a broad interpretation of the applicable notice if the actual monitoring at hand is supported by an employer's legitimate business interest in monitoring employee communications. While the courts appear willing to address the legitimacy of business interests, the issue will most likely be decided on a case-by-case basis. And in evaluating the legitimacy of a business interest, the guidance is not necessarily clear. In *Stengart*, the court concluded the employer's policies were ambiguous as to employees' personal use of computer systems,[202] while the *Holmes* court concluded the employer's policies were unambiguous.[203] Finally, in *Quon*, the Supreme Court acknowledged that the employer's policies did not explicitly address text messages but concluded that verbal notice that text messages were considered the same as e-mail messages was sufficient to incorporate text messages into the formal city policies.[204]

Thus, employees should anticipate very minimal expectations of privacy in workplaces within the United States.

III. EMPLOYER MONITORING AND EMPLOYEE PRIVACY—EUROPEAN PERSPECTIVE

Employers in Europe have access to the same monitoring technologies that are available to employers in the United States. Furthermore, multinational groups operating in Europe and the United States tend to face technical pressures to implement technologies uniformly across the global enterprise. Thus it is not surprising that in a few cases, employers have become entangled in some of the same monitoring-related disputes in European courts as discussed in Part II, *supra*, with respect to the United States.[205] But, the following review of European cases will show that: first, the monitoring activities challenged in European courts tend to be far less

202. *Stengart*, 973 A.2d at 396.
203. *Holmes*, 119 Cal. Rptr. 3d at 896–97.
204. City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2625 (2010).
205. For discussion of U.S. law, see *supra* Part II.

intrusive as in some U.S. cases; second, European employees tend to win privacy-based lawsuits; third, European employers are not required or expected to engage in intrusive employee monitoring; and fourth, European employers are typically unable to defend their practices based on notices.

A. LAWS IN EUROPE—OVERVIEW

First, in Europe, there is technically no uniform body of "European law" that directly applies between employers and employees. In most if not all European countries, however, some laws agreed to or enacted on a supranational level apply in one form or another, as implemented into national law or with immediate legal effect at the national law level. To understand current employee privacy law in Europe, one must note the different legal regimes, legislatures, and courts in Europe that have been making and interpreting law in this area, including: national legislatures, international treaties, and the European Union (and its predecessor organizations). Second, the concept of data protection in Europe does not completely mirror the concept of privacy in the United States.

B. CIVIL RIGHTS PROTECTIONS FOR PRIVACY AT THE EUROPEAN LEVEL

The European Convention on Human Rights was signed in 1950 by ten founding member states.[206] Today, a larger group of European countries has signed and implemented the European Convention on Human Rights, adjudicated by the European Court of Human Rights in Strasbourg. The Convention expressly protects individual privacy against government interference:

> Article 8—Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[207]

206. Belgium, Denmark, France, Ireland, Italy, Luxembourg, the Netherlands, Norway, Sweden, and the United Kingdom. Convention for the Protection of Human Rights and Fundamental Freedoms, June 1, 2010, C.E.T.S. No. 194, *available at* http://conventions.coe.int/treaty/en/Treaties/Html/005.htm [hereinafter Human Rights Convention].

207. Human Rights Convention, *supra* note 206, § 1.

Article 8 has been refined in a number of cases by national courts and the European Court of Human Rights, which have applied the right to various forms of intrusion into data privacy. However, the courts have usually only applied the Article 8 right to privacy in situations where a state actor (i.e., a government entity), and not a private sector employer, has interfered. For example, in *Halford v. United Kingdom*[208] and *Kopp v. Switzerland*,[209] the European Court of Human Rights acknowledged that state employees have a right to privacy with respect to phone calls made from their government-operated work locations.

In *Copland v. United Kingdom*,[210] the European Court of Human Rights expanded Article 8 protection to e-mails and ruled that phone connection data (e.g., time of connection and numbers called) as well as e-mail and internet usage information (e.g., websites visited and numbers of e-mails sent and received) were also protected. In *Copland*, a state-owned college had monitored the e-mail and internet usage of its employees for purposes of determining abuse. Details of the monitoring program were disputed by the parties to the underlying litigation, but the court decided that even the undisputed minimal amounts of the college's monitoring (e.g., recording and analysis of connection information) were incompatible with the protections in Article 8 of the Convention without a specific statutory basis.[211] The general statutory authorization of the college to do " 'anything necessary or expedient' for the purposes of providing higher and further education" was insufficient as a basis for the monitoring; hence, the monitoring violated the plaintiff's rights.[212]

Given this finding, the court in *Copland* was neither required nor given the opportunity to decide what the college—or another government institution—could monitor, given more specific statutory authorizations; but based on other cases, the court would likely have applied a balancing test of the individual's right to privacy and any legitimate purposes of government that are necessary in a democratic society.[213] The European Court of Human Rights weighed heavily the fact that the plaintiff had a "reasonable expectation" of privacy which was not met due to the lack of notices and

208. Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).
209. Kopp v. Switzerland, App. No. 23224/94, 27 Eur. H.R. Rep. 91 (1998).
210. 45 Eur. Ct. H.R. 253 (2007).
211. *Id.*
212. *Id.* ¶ 47.
213. *See* Gerrit Hornung, *EGMR: Überwachung Privater E-Mail und Internetnutzung am Arbeitsplatz [Monitoring of Private E-mail and Internet Use at the Workplace]*, 12 MULTIMEDIA UND RECHT [MMR] 431, 432 (2007).

specific legislation or other publicized rules.[214] Therefore, it appears that the court might have accepted a statutory basis for monitoring that both requires the employer to give employees reasonable prior notice and applies some restraint on the methods used with respect to their intrusiveness.[215] But how strict a degree of scrutiny the court would apply to such legislation remains unclear.

The European Convention and Court of Human Rights exist independently of the European Union (EU), which is not a member of the convention and which has grown out of efforts to achieve economic integration rather than civil rights protections.[216] In 1957, France, Germany, Italy, and the Benelux countries—a different group of founders than for the European Convention of Human Rights—signed the Treaty of Rome to establish the European Economic Community (EEC), whose primary goal was to achieve integration via trade with a view to economic expansion.[217] In 1992, a larger group of countries signed the Maastricht Treaty and eliminated "Economic" from the name of the new European Community (EC), reflecting a collective determination to expand the Community's powers to non-economic domains.[218]

The Maastricht Treaty also created the European Union to document ambitions for non-economic integration.[219] But while the European Union was to serve largely symbolic functions, the European Community remained the law-making body, and economic integration remained the main driver of EC activities for the remainder of the last century.[220] Therefore, much of the supranational European legislation remained focused on removing barriers to trade and protecting the economic freedoms of businesses in Europe.[221]

---

214. *Copland*, 45 Eur. Ct. H.R. 253, ¶ 42.

215. *See* Hornung, *supra* note 213, at 432.

216. According to Article 6 of the Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, the Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. 2007 O.J. (C 306) 1, 135 (Dec. 17, 2007), *available at* http://www.ecb.int/ecb/legal/pdf/en_lisbon_treaty.pdf [hereinafter Treaty of Lisbon].

217. *See* Treaty of Rome, Mar. 25, 1957, *available at* http://ec.europa.eu/economy_finance/emu_history/documents/treaties/rometreaty2.pdf.

218. *See* The Maastricht Treaty: Provisions Amending the Treaty Establishing the European Economic Community with a View to Establishing the European Community, Feb. 7, 1992, 31 I.L.M. 247 (1992), *available at* http://www.eurotreaties.com/maastrichtec.pdf [hereinafter Maastricht Treaty].

219. *See id.* tits. IX–XI.

220. *See id.*

221. *See, e.g.*, Peter Tettinger, *Die Charta der Grundrechte der Europäischen Union* [*The Charter of Fundamental Rights of the European Union*], 54 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 1010 (1014), 2001 (Ger.).

Consequently at the European level, there was relatively little mandate or perceived need to protect privacy. Whenever national authorities and legislatures restricted individual freedoms or civil rights, EC law offered protective rights to individuals to challenge restrictions in the economic sector, and national constitutional laws offered additional protection for individual rights in the economic and private spheres.[222] But, in its effort to harmonize economic conditions, the EEC (and later the EC and EU) not only struck down trade-restricting national legislation and regulations but also increasingly imposed harmonized legislation, primarily through Directives that the member states were required to implement into national law.[223] EEC legislation covered any topic considered economically relevant (e.g., environmental and product safety standards, consumer contracts, advertising) and sought to create a level playing field for businesses in Europe.[224] As such, the legislation had the potential to restrict individual freedoms as much as previously-national legislation did.

Given the supremacy of EC law (and later EU law) over national law, national constitutions could no longer fully protect individual rights without endangering European harmonization and integration. To reduce the risk of challenges to European laws under national constitutional laws as well as the risk of diverging national standards on this topic, the European Court of Justice (the European Community's Court and now the European Union's Court) tried to fill the "civil rights vacuum" by inventing a suite of European constitutional principles that could be used to challenge EC/EU legislation, and of which the European Court of Justice remained the ultimate guardian.[225] The European Court of Justice developed these European civil rights in reference to principles in the European Convention of Human Rights and national constitutional laws, as assessed and defined by the European Court of Justice from time to time.[226] EU member states perceived this "ad hoc" development of human rights protections as unsatisfactory. After long negotiations, the EU member states agreed on a Charter of Fundamental Rights of the European Union in 2000.[227] This Charter expressly protects privacy and personal data:

---

222. THOMAS DIETERICH ET AL., ERFURTER KOMMENTAR ZUM ARBEITSRECHT [COMMENT ON LABOR] ¶¶ 114–117, at 23–24 (10th ed. 2010).

223. *See* Tettinger, *supra* note 221.

224. *See id.*

225. *See, e.g.*, *id.* at 1014.

226. *See id.*

227. Charter of Fundamental Rights of the European Union, 2000 O.J. (C 364) 1 (Dec. 18, 2000), *available at* http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

> Article 7—Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8—Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her.
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
>
> 3. Compliance with these rules shall be subject to control by an independent authority.[228]

Under the Treaty of Lisbon, the Charter is legally binding.[229] However, due to the jurisdictional limitations of EU law, the EU Charter of Fundamental Rights applies only if and to the extent that EU member states implement or enforce EU law over their respective national laws. Courts and scholars increasingly reference EU law, usually without clarifying whether the existence of a particular civil right protection in the EU Charter actually changed the legal situation as a matter of law, rather than as a matter of public policy.[230]

C. THE EC'S DATA PROTECTION DIRECTIVE

In 1995, because diverging national standards and cross-border data transfer restrictions had become an obstacle to trade in the Common Market,[231] the European Community attempted to harmonize data protection laws across the EC member states through the EC Data Protection Directive.[232] In order to secure approval from EC member states with

---

228. *Id.* arts. 7–8.

229. Article 6 of the Treaty on the European Union, as amended by the Lisbon Treaty, is binding on all EU member states, except for member states with an opt-out for this provision. *See* Treaty of Lisbon, *supra* note 216, at 156.

230. *See, e.g.*, Tettinger, *supra* note 221, at 1014.

231. The German State of Hessen passed the world's first data protection law in 1970. *See Privacy in Hessen*, LANDESPORTAL HESSEN, *available at* http://www.hessen.de/irj/hessen_Internet?cid=098693b3bbacadc19b81045a1c2300f2 (last visited Jan. 26, 2011). Other German states and European countries quickly followed suit. *See Law Texts and Comments*, VIRTUAL PRIVACY OFFICE, *available at* http://www.datenschutz.de/recht/gesetze/ (last visited Mar. 6, 2011).

232. Directive 95/46/EC, 1995 O.J. (L 281) 31 (Nov. 23, 1995), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML [hereinafter EC Data Protection Directive].

historically high data protection standards, the EC adopted a general prohibition on the processing of any personal data and a particular ban on transfers outside the European Economic Area (EEA), subject to a number of narrow, enumerated exceptions.[233] All EEA member states[234] had to implement these substantive requirements into national legislation,[235] but they retained jurisdiction to legislate administrative details such as notification and approval requirements, penalties, and enforcement procedures. Given the jurisdictional limitations of the European Community to regulate economic activity via Directives, the EC Data Protection Directive covers data processing activities by private sector employers and possibly government-owned businesses, but not by government entities in their capacity as state actors.[236]

A primary objective of the national legislation that prompted the EU harmonization initiative was to regulate and limit automated processing of personal data because of perceived danger from government—Big Brother

---

233. The European Economic Area (EEA) is comprised of the twenty-seven EU member states, plus three more—Iceland, Liechtenstein, and Norway—which agreed under a separate treaty to adopt certain EU laws. *See* Agreement on the European Economic Area (EEA), 1994 O.J. (L 1) 3 (May 2, 1992), *available at* http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=1.

234. The EEA was established in 1994, following an agreement between the member states of the European Free Trade Association (EFTA) and the EC, later the EU. The treaty allows Iceland, Liechtenstein, and Norway to participate in the EU's single market without a conventional EU membership. In exchange, they are obliged to adopt all EU legislation related to the single market, except laws regarding agriculture and fisheries. One EFTA member, Switzerland, has not joined the EEA.

235. The EC Commission collects unofficial English translations of national legislation. *See Policy Papers from National Data Protection Authorities*, EUR. COMM'N, *available at* http://ec.europa.eu/justice/policies/privacy/policy_papers/policy_papers_en.htm (last updated Aug. 6, 2010).

236. Article 3.2 of the EC Data Protection Directive provides:

> This Directive shall not apply to the processing of personal data . . . in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law.

EC Data Protection Directive, *supra* note 232. This limitation is a function of the principles of limited competences and subsidiary, which are codified in Articles 4 and 5 of the EU Treaty, as amended by the Lisbon Treaty, whereby the EU has limited competences and the EU shall only exercise its competences to the extent the Member States cannot effectively legislate a particular topic. *See* Consolidated Version of the Treaty on European Union, 2010 O.J. (C 83) 13 (Mar. 3, 2010), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0013:0046:EN:PDF.

watching the "transparent citizen"[237]—and the private sector—businesses creating large databases that could be accessed and abused by government.[238] Consequently, EC data protection laws, on a national level as well in the Directive, prohibit the processing of personal data unless a specific statutory exemption applies.[239]

In contrast to U.S. data *privacy* laws, European data *protection* laws do not condition protection on an expectation of privacy. The data protection laws protect the right to privacy and regulate the processing of personal data within the European Union. These laws define "personal data" and "processing" very broadly and cover even publicly available data. Any information relating to an identifiable individual is "personal data"[240] and any

---

237. The term "transparent citizen" originates from the German term "gläserner Bürger" (literally translated: glass citizen) used by scholars and politicians to illustrate the dangers of government and private surveillance. *See, e.g.*, Hans U. Buhl & Günter Müller, *The "Transparent Citizen" in Web 2.0: Challenges of the "Virtual Striptease,"* 4 BUS. & INFO. SYS. ENGINEERING 203 (2010), *available at* http://www.bise-journal.org/pdf/1_60896.pdf.

238. *See* Stefan Krempel, *Vom gläsernen Bürger zum gläsernen Staat* [*From the Glass Citizen to the Glass State*], TELEPOLIS, June 18, 2000, *available at* http://www.heise.de/tp/artikel/8/8262/1.html; *see also* ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVerfGE] [Federal Constitutional Court] 37 NJW 419 (422), 1984 (Ger.) (holding in the census decision that there are no insignificant dates given the technical development, and deriving the right to informational self-determination from the general personality right interpreting Article 2, ¶ 1 in conjunction with Article 1, ¶ 1 of the German Constitution). The decision had a profound impact both in Germany and Europe—the principles laid down in it appear in the state data protection acts the following years, as well as in the General Amendment to the German Federal Data Protection Act of 1990.

239. Article 7 of the EC Data Protection Directive:

> [P]ersonal data may be processed only if: (a) the data subject has unambiguously given his consent; or (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or (d) processing is necessary in order to protect the vital interests of the data subject; or (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

EC Data Protection Directive, *supra* note 232, art. 7.

240. Article 2(a) of the EC Data Protection Directive:

> "[P]ersonal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to

collection, use, and transfer—even the redaction and deletion thereof—constitutes "processing."[241]

Employers in the European Economic Area routinely rely on three exemptions for their processing of personal data: (1) a necessity to perform contractual obligations with the data subject, (2) individual consent from the data subject, and (3) a legal requirement to process personal data based on statutory obligations or orders from the government of the country whose data protection laws apply.[242] In extraordinary situations they may be able to rely on a balancing-of-interests test,[243] but in practice, employers typically

---

an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Id. art. 2(a). Switzerland and some EEA Member States, including Austria, expand the definition of personal data to information relating to a specific legal entity. *See* BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DPA] [FEDERAL ACT ON DATA PROTECTION], SR 235.1 (1992), art. 3(a), (b) (Switz.), *available at* http://www.admin.ch/ch/e/rs/2/235.1.en.pdf ("data subjects: natural or legal persons whose data is processed"); BUNDESGESETZ ÜBER DEN SCHUTZ PERSONENBEZOGENER DATEN [DSG] [FEDERAL ACT CONCERNING THE PROTECTION OF PERSONAL DATA] BUNDESGESETZBLATT I [BGBL I], No. 165/1999, art. 2, pt. 1, § 4, ¶ 3 (Austria), *available at* http://www.dsk.gv.at/DocView.axd?CobId=41935 (last visited Apr. 26, 2011) (" 'Data Subject' . . . : any natural or legal person or group of natural persons not identical with the controller, whose data are processed . . . .").

241. Art. 2(b) of the EC Data Protection Directive:

> "[P]rocessing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

EC Data Protection Directive, *supra* note 232, art. 2(b).

242. There are a variety of situations exemplifying this point. Employers are typically required to report certain information to local tax authorities, and local law enforcement agencies can demand the disclosure of certain personal data so long as procedural and formal safeguards are observed. However, multinational companies cannot always rely on these exceptions where data collection or disclosure obligations follow from statutes or government agencies in another country, in particular from countries outside the EEA. For instance, airlines were for a while caught in a crossfire of conflicting data protection/disclosure obligations. *See* Lothar Determann, *Conflicting Data Laws: Airlines Are Damned If They Do, Don't*, S.F. DAILY J., Sept. 23, 2003, at 5. More recently, the Society for Worldwide Interbank Financial Telecommunication (SWIFT) was caught between European data protection requirements and subpoenas from U.S. tax authorities. *See* Press Release, European Commission, The SWIFT Case and the American Terrorist Finance Tracking Program (June 28, 2007), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/07/266&format=HTML&aged=0&language=EN&guiLanguage=en.

243. Article 7 of the EC Data Protection Directive also allows processing if necessary for (c) "compliance with a legal obligation to which the controller is subject" (but legal obligation means typically "legal obligation under local law" or "under laws that conform to EC law"); (d) "in order to protect the vital interests of the data subject" (interests are

find it difficult to meet the high standards applied by courts and data protection authorities.[244] Principal exceptions to processing personal information are discussed *infra*.

1. Necessity Under Contract

Contractual duties serve as justification only if the processing is truly necessary for the performance of a contract between the data subject and the data controller.[245] Necessity can be assumed where the employer processes personal data to enable employees to do their job (e.g., by offering e-mail, internet connectivity, data storage, etc.). However, with respect to monitoring, employers will typically not be able to show a necessity under employment contracts, because European employers do not include express duties to monitor in their agreements and they are not obligated to monitor employees under applicable statutes.[246]

2. Consent

Unlike in the United States, it is not possible within the European Union to unilaterally destroy an expectation of privacy—the employer must affirmatively seek employee consent in order to rely on it as an exception from the general prohibition of monitoring activities involving data processing.[247] Further, consent is valid only if the data subject grants it in an informed, voluntary, express, specific, and written manner.[248] The

considered vital in cases of medical emergencies, but probably not in most cases of commercial convenience or in most other situations in which companies would like to refer to this exception); (e) "for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed;" or (f) "for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)" (again, national data protection authorities apply high standards). EC Data Protection Directive, *supra* note 232, art. 7.

244. *See Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries*, EUROPEAN COMM'N, 49, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf (last updated Aug. 6, 2010) [hereinafter FAQ].

245. *See* EC Data Protection Directive, *supra* note 232, arts. 2(h), 7, 26.

246. Achim Lindemann, *Betriebsvereinbarungen zur E-Mail-, Internet- und Intranet-Nutzung [Operating Agreements for E-Mail, Internet and Intranet Use]*, DER BETRIEBSBERATER 1950, 1951 (2001).

247. *See* Lindemann, *supra* note 246.

248. *See* EC Data Protection Directive, *supra* note 232, arts. 2(h), 7(a). Recent Mexican data privacy legislation follows the EU model in many respects, but it accepts implied consent upon receipt of a sufficiently detailed notice, which is similar to the U.S. approach in this respect. *See* Lothar Determann & Sergio Legorreta, *New Data Privacy Law in Mexico*, 10

"voluntariness" requirement raises significant difficulties in the employment context. The national data protection authorities in most EEA member states[249] presume that employee consent is coerced, and hence involuntary, given the typical balance of power in the employment relationship.[250] In order to overcome this presumption, the employer must give conspicuous notice that each employee is entitled to withhold consent without any unduly adverse consequences, so that employees are truly in a position where they can voluntarily grant or deny consent. As a practical matter, however, employers can then expect that some employees will deny or later revoke their consent. This alone tends to render any systematic deployment of monitoring technologies based on employee consent impractical.

3. Statutory Obligations

Employers are not legally required to monitor employees in most EU member states, nor do they face the same kinds of liabilities as U.S. employers that provide indirect motivation for monitoring programs.[251] But automated monitoring programs such as e-mail filtering and blocking of potentially harmful websites may best address the obligations imposed by data protection laws and laws requiring enterprises to maintain controls and transparency.[252] For example, Germany enacted a statute in 1998 regarding controls and transparency in enterprises, which requires companies to establish risk management, protection, and control systems, as well as monitoring programs to enforce such controls.[253] Also, data protection laws

IAPP PRIVACY ADVISOR 1 (Nov. 2010), *available at* https://www.privacyassociation.org/publications/2010_10_26_new_data_privacy_law_in_mexico/.

249. Article 29 Working Party Working Document on Surveillance and Monitoring of Electronic Communications in the Workplace (Article 29 Data Prot. Working Party, Working Paper No. 55, Reference 5401/01, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf. The "national data protection authorities" are in reference to independent government agencies and not a body of law. For a list, see *Privacy and Data Protection Authorities*, COUNCIL OF EUR., http://www.coe.int/t/dghl/standardsetting/dataprotection/Supervisory%20_Authorities_en.asp (last visited May 22, 2011).

250. FAQ, *supra* note 244, at 50; *see also* Determann & Brauer, *supra* note 71; Determann, *supra* note 71.

251. *See supra* Section II.A.

252. *See* Michael Schmidl, *E-Mail-Filterung am Arbeitsplatz* [*E-mail Filtering in the Workplace*], 13 MMR 343, 345–46 (2005); Michael Schmidl, *Aspekte des Rechts der IT-Sicherheit* [*Aspects of the Law of IT-Security*] [Feb. 18, 2010], 63 NJW 476 (478), 2010 (Ger.).

253. *See* GESETZ ZUR KONTROLLE UND TRANSPARENZ IM UNTERNEHMENSBEREICH [KONTRAG] [CORPORATE SECTOR SUPERVISION AND TRANSPARENCY ACT], Mar. 5, 1998, DEUTSCHER BUNDESTAG: DRUCKSACHE [BT] 13/10038 art. 1, § 9(c) (Ger.), *available at* http://www.sicherheitsforum-bw.de/x_loads/KonTraG.pdf (last visited May 22, 2011) (adding a section 91, paragraph 2 of the German Share Corporation Act (Aktiengesetz)

require technical and administrative security measures to protect the integrity and confidentiality of personal data.[254]

4. Balancing Test

Pursuant to Article 7(f) of the EC Data Protection Directive, EU member states have enacted exceptions from the general prohibition to process personal information if and to the extent that "data processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection . . . ."[255] In one example, based on the German version of this "balancing test exception," the German Federal State-owned railway company, Deutsche Bahn AG, engaged in data mining, comparing names in its human resources database with names in its accounts-payable database to identify matches that might warrant further investigations into self-dealing, bribery, nepotism, and favoritism regarding suppliers with family connections to employees.[256] The company apologized publicly and acknowledged that it had conducted automated comparisons of the addresses and bank account information of 175,000 employees with those of Deutsche Bahn suppliers.[257] Prosecutors announced investigations of the management of Deutsche Bahn.[258] Public outcry with respect to this monitoring program, as well as allegations regarding individual follow-up investigations, caused the CEO of Deutsche Bahn to resign and the German government to amend the Federal Data Protection Act. A new Section 32 clarified that employers may generally

according to which share companies have to establish risk management controls and monitoring programs, arguably also including information technology control mechanisms).

254. For example, section 9 of the German Federal Data Protection Act requires technical protection measures. For additional examples and references, see Lothar Determann & Jesse D. Hwang, *Data Security Requirements Evolve: From Reasonableness to Specifics*, 26 COMPUTER & INTERNET LAW., Sept. 2009, at 6, 10.

255. EC Data Protection Directive, *supra* note 232, art. 7(f).

256. Nicolas Mähner, *Neuregelung des § 32 BDSG zur Nutzung Personenbezogener Mitarbeiterdaten am Beispiel der Deutschen Bahn AG* [*Revision of § 32 BDSG [German Federal Data Protection Act] on the Use of Personal Employee Data Using the Example of the Deutsche Bahn AG*], 13 MMR 379 (2010).

257. Von M. Bauchmüller & Klaus Ott, *Mehdorn Verschweigt Weiteren Daten-Skandal* [*Mehdorn Conceals New Data Scandal*], SUEDDEUTSCHE.DE, Feb. 3, 2009, *available at* http://www.sueddeutsche.de/wirtschaft/386/457048/text/; Brett Neely, *Deutsche Bahn Chief Mehdorn Apologizes to Workers on Data Probe*, BLOOMBERG (Feb. 6, 2009), http://www.bloomberg.com/apps/news?pid=20601100&sid=aMDxC5iRb7nM.

258. Sabine Siebold, *Staatsanwaltschaft prüft Ermittlungen gegen Bahn-Chef* [*Public Prosecutors Consider Investigations of Deutsche Bahn Chief*], REUTERS (Feb. 12, 2009), http://de.reuters.com/article/deEuroRpt/idDELC60224520090212.

process personal data of employees only for purposes of concluding, maintaining, and terminating employment relationships. Personal data of employees may be collected and otherwise processed for purposes of uncovering criminal actions only if and to the extent that (1) actual documented facts create a suspicion of criminal activities, (2) the processing is necessary, and (3) the interests of the individual employee do not outweigh the interests of the employer.[259] These specific rules do not contemplate routine monitoring or processing of personal data for purposes of investigating infractions that do not amount to criminal acts (such as potential violations of a company-wide code of conduct or similar rules).[260] Employee consent is not mentioned as a possible means of legitimizing monitoring programs.

D. NATIONAL WIRETAP LAWS IN EUROPE (CASE STUDY: GERMANY)

In addition to data privacy laws, employers must observe restrictions under anti-wiretap laws, which have not (yet) been harmonized throughout Europe. Under German federal telecommunications law, for example, employers who expressly allow or tolerate some private use of the Internet, e-mail, or other electronic communications systems are treated like telecommunications service providers and are fully subject to telecommunications secrecy provisions.[261] As such, employers cannot even implement anti-spam filtering or anti-virus filtering technologies without

259. Mähner, *supra* note 256.

260. On August 25, 2010, the German government presented a bill amending the Federal Data Protection Act. The bill, *inter alia*, deals with the automated matching of employee data for internal compliance investigations. The bill provides for a two stage escalation model. In the first stage, only anonymous or aliased data may be matched for the purpose of disclosing severe breaches of duty, especially crimes committed during the employment (e.g., corruption). Marie-Theres Tinnefeld, Thomas Petri & Stefan BrinkTinnefeld, *Aktuelle Fragen um ein Beschäftigtendatenschutzgesetz—Eine erste Analyse und Bewertung* [*Current Topics Around Employees' Data Protection*], 13 MMR 727, 732 (2010); Norton Rose LLP, *Neuer Gesetzesentwurf zum Beschäftigtendatenschutz* [*New German Draft Bill Regarding Employee Data Protection*], *available at* http://www.nortonrose.com/knowledge/publications/2010/pub30760.aspx?lang=de-de&page=all (last visited Apr. 29, 2011). According to the draft bill, employers may initiate the first stage without cause for suspicion of breach. Routine spot tests are permissible. *See* Michael Schmidl & Benjamin Baeuerle, *German Employee Data Protection Law Proposed by Government*, 10 WORLD DATA PROTECTION REP., no. 9, 2010, at 28, 28–29.

261. *See, e.g.*, Thorsten B. Behlinger, *Compliance Versus Fernmeldegeheimnis* [*Compliance Versus Privacy of Telecommunications*], 19 BETRIEBS BERATER 892, 892 (2010); René Hoppe & Frank Braun, *Arbeitnehmer-E-Mails: Vertrauen ist Gut—Kontrolle ist Schlecht—Auswirkung der neusten Rechtsprechung des Bundesverfassungsgerichts auf das Arbeitsverhältnis* [*Employees' E-mails: Faith Is Good, Checks Are Bad—Consequences for the Employer-Employee Relationship Arising Out of the Latest Decisions by the Federal Constitutional Court*], 13 MMR 80, 81 (2010).

valid, individual consent, which is extremely difficult, if not impractical, to obtain from individuals. Without such consent, filtering technologies can only be deployed as necessary to protect the network, without an option for the employer to access individual filter reports or quarantined e-mails for productivity or compliance monitoring.[262] Theoretically, German employers can avoid this consequence by strictly prohibiting personal use of communications systems, because the German telecommunications laws only apply to public systems, not to closed systems. But, in practice, employees expect, and employers allow, limited personal use of company communications systems.

E. WORK-RELATED ELECTRONIC MONITORING

French courts have been even stricter by protecting employees from e-mail searches whether or not the employer allows private use. In one case, an employer was sanctioned for terminating the employment contract of an employee who had been running a competing consulting business from his workplace, using the employer's e-mail system to accept orders and process engagements for services that were similar to those that the employer offered to customers.[263] The court reprimanded the employer for the fact that it had not notified the employee of the possibility of searches into e-mail folders that were labeled "personal," as well as for the fact that the employer had not submitted required notifications to the French data protection authorities.[264] Consequently, the court invalidated the termination, ordering reinstatement and damages for the employee.

A number of EC member states, including Germany, Italy, the Netherlands, Spain, and the United Kingdom, strictly prohibit ongoing monitoring of employee communications and permit electronic monitoring

---

262. Michael Schmidl, *Decision 2 BvR 902/06 of the German Constitutional Court: The End of E-Mail Screening in the Workplace*, 9 WORLD DATA PROTECTION REP., no. 8, 2009, at 15, 15; Schmidl, *E-Mail-Filterung*, *supra* note 252, at 345.

263. Cour d'Appel [CA] [regional court of appeal] Versailles, Apr. 2, 2003, Aff. No. 02/00293 (Fr.); *see also* Kunz Kömpf, *Kontrolle der Nutzung von Internet und E-Mail am Arbeitsplatz in Frankreich und Deutschland* [*Controlling the Use of Internet and E-mail in the Workplace in France and Germany*], 26 NEUE ZEITSCHRIFT FÜR ARBEITSRECHT [NZA] 1341, 1343 (2007) (Ger.); Christiane Féral-Schuhl, *Cyber Surveillance at Work*, UNI GLOBAL UNION, 22, *available at* http://www.uniglobalunion.org/Apps/UNIPub.nsf/vwLkpById/F6403CF3DFEEBF01C125757C00367650/$FILE/feral-schuhl_cybersurveillance-en.pdf (last visited Apr. 29, 2011).

264. *See* Cour d'Appel [CA] [regional court of appeal] Versailles, Apr. 2, 2003, Aff. No. 02/00293 (Fr.). *Contra* McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. May 28, 1999) (holding no right to privacy in e-mail messages stored in a password-protected "personal" folder).

only in very limited circumstances (e.g., where an employer already has concrete suspicions of wrong-doing against particular employees),[265] subject to significant restrictions with respect to the duration, mode, and subjects of the monitoring activities.[266] Several jurisdictions worldwide, including France, the Netherlands, and Israel, require filings with data protection or labor authorities, while others, including France, Germany, Italy, the Netherlands, and China, require employers to consult or at least notify trade unions or other employee representative bodies before subjecting their employees to surveillance measures.[267]

Complaints by an employee in a country with a high level of data protection can trigger investigations and lawsuits by data protection authorities, trade unions, consumer watchdogs, and similar organizations, and can also lead to criminal complaints.[268] Employers found in non-compliance may face steep penalties, damages awards, and possibly even prison time, along with plenty of bad press, as some recent examples demonstrate.

In September 2008, German authorities ordered discount retailer Lidl to pay fines totaling around 1.5 million euros for a variety of alleged data protection violations, including monitoring employees and customers through the use of in-store hidden cameras to counter a wave of theft.[269] In

265. Astrid Wellhörner & Phillip Byers, *Datenschutz im Betrieb—Alltägliche Herausforderung für den Arbeitgeber* [*Data Protection at Work—Everyday Challenges for Employers*], 18 BETRIEBS BERATER 2310, 2311 (2009).

266. For instance, in the context of internal audits in Germany it is often necessary to inform employees in detail about the reasons for the internal audit, the controller's identity, the categories of data collected, etc. *See* Michael Schmidl, *Germany: Internal Audits and Protection of Employee Data*, 7 WORLD DATA PROTECTION REP., no. 6, 2007, at 10, 10–11 (2007).

267. *See, e.g.*, German Works Constitution Act § 87(1)(6), Sept. 25, 2001, BGBL. I at 2518, repromulgated Dec. 23, 2003, BGBL. I at 2848, art. 81 (Ger.), *available at* http://www.bmwi.de/English/Redaktion/Pdf/__Archiv/labour-law/works-constitution-act1,property=pdf,bereich=bmwi,sprache=de,rwb=true.pdf.

268. *See, e.g.*, STRAFGESETZBUCH [STGB] [PENAL CODE] § 202a (Ger.) (illegally spying on data—with a maximum penalty of three years' imprisonment); *id.* § 206 (telecommunication secrecy—with a maximum penalty of five years' imprisonment); *id.* § 303a (deleting or changing data—with a maximum penalty of two years' imprisonment); BUNDESDATENSCHUTZGETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Jan. 14, 2003, § 44 (Ger.) (with a maximum penalty of two years' imprisonment).

269. *Millionen-Strafe für die Schnüffler* [*A Penalty of Millions for Snoops*], SUEDDEUTSCHE, Sept. 11, 2008, *available at* http://www.sueddeutsche.de/wirtschaft/860/309795/text/. As a result of this and similar incidents, the degree of possible fines and penalties based on the German Federal Data Protection Act increased on November 1, 2009. *See* DEUTSCHER BUNDESTAG: BESCHLUSSEMPFEHLUNG UND BERICHT [DECISION AND RECOMMENDATION

2009, Deutsche Telekom came under scrutiny when the company admitted to having collected and reviewed telephone call data of its directors and executives in order to investigate management irregularities.[270] Deutsche Telekom reacted by creating a management board position dedicated to data privacy and security matters.[271] Despite a historic emphasis on data protection, even companies based in Europe struggle with privacy compliance. This suggests that it is imperative for U.S. companies with operations abroad to obtain legal advice on the implications of their contemplated monitoring activities under the laws of all jurisdictions in which affected employees are located.

In Europe, public companies are not required or encouraged to establish whistleblower hotlines, monitor employees, or conduct investigations. In fact, employers must obtain various authorizations from national authorities, which tend to require that electronic monitoring programs protect employee data privacy.[272] Employment contracts in Europe are also not "at will" agreements, and employees are protected against termination more generally. Consequently, employers are less exposed to vicarious liability claims based on employee wrong-doings, perhaps because European laws seem to acknowledge employers' lesser degree of control over their employees' communications and other activities.[273]

TO MODIFY THE FEDERAL DATA PROTECTION ACT] [BT] 16/13657 (Ger.), *available at* http://dip21.bundestag.de/dip21/btd/16/136/1613657.pdf.

270. *Telekom Bespitzelte Aufsichtsräte, Manager und Journalisten* [*Telecom Spied on Board of Directors, Managers, and Journalists*], SPIEGEL ONLINE (May 24, 2008) (Ger.), http://www.spiegel.de/wirtschaft/0,1518,555148,00.html.

271. *See Manfred Balz*, DEUTSCHE TELEKOM [T-MOBILE], http://www.telekom.com/dtag/cms/content/dt/en/579544 (last visited July 12, 2011).

272. Melissa Klein Aguilar, *Finally: German Whistleblower Guidelines Released*, COMPLIANCE WK., May 1, 2007, *available at* http://www.eapdlaw.com/files/News/684ef9c3-942d-4a1a-a43e-5e91edd73573/Presentation/NewsAttachment/3b385aac-c8cf-4165-9f64-67ee78bc64a4/Finally_German%20Whistleblowers%20GuidlinesReleased_pdf.pdf; Cynthia Jackson, *A Global Whistle-Stop Tour*, DAILY J., Feb. 19, 2009, *available at* http://www.bakermckenzie.com/files/Publication/b3442009-d314-4585-a396-f1ec419acc6e/Presentation/PublicationAttachment/4840fa55-490c-448a-983f-fbdb28b9f7f5/ar_sfpa_DJ8GlobalWhistleStopTour_feb09.pdf.

273. It is difficult to prove a negative, but the authors note a dearth of reported cases on employer liability for harassment or unlawful contact of employees from European jurisdictions.

IV. DIFFERENCES IN POLICY, LAW, AND PRACTICE—AND THE IMPACT ON GLOBAL EMPLOYERS AND EMPLOYEES

True to their respective, fundamentally different approaches to data privacy and employment relations in principle, the United States and the European Union offer entirely different parameters for workplace privacy and employer monitoring—in law and practice. In the United States, some state statutes increasingly seek to protect employees' privacy rights from overly intrusive monitoring; however, for the most part key differences between the U.S. and European privacy regimes still exist. As such, global employers must be cognizant of the two contrasting privacy regimes.

In the United States, privacy is legally protected only where an actual and reasonable expectation of privacy exists. Employers are free to eliminate actual employee privacy expectations through detailed, specific notices and deploy even highly intrusive monitoring technologies, except where prohibited by a few, narrowly worded statutory prohibitions of extremely intrusive employer monitoring in some states (such as video surveillance in locker rooms and restrooms).[274] Courts could apply increasingly higher requirements for the level of detail required to allow employer notices and find limited expectations of privacy where employer notices are outdated or incomplete. But, many U.S. courts have interpreted notices broadly in the employer's favor and found either no actual or no reasonable privacy expectations where employers pursued legitimate interests with their monitoring efforts.

In Europe, companies are generally prohibited from collecting and processing personal data under data protection laws that are intended to

274. Some state laws and state courts have begun to consider privacy claims in working environments and employee privacy has gained ground in the United States. N.Y. GEN. BUS. LAW § 395-b (2010) bans the use of surveillance devices—whether they're video or conventional "peep-hole" types—by business owners, and covers areas such as changing rooms or areas, bathrooms, and any other place where a reasonable expectation of personal privacy exists. Employers who violate this law are subject to fines up to $300, fifteen days in jail, or a combination of fines and time served. New York State has passed an "eavesdropping" statute similar to the Federal Wiretapping Statutes as well. *See* N.Y. PENAL LAW §§ 250.00, 250.05 (2010). A person is guilty of the felony of eavesdropping when he or she unlawfully engages in, *inter alia*, "wiretapping" or "intercepting or accessing of an electronic communication." In California it is a crime to intercept or eavesdrop upon any confidential communication, including a telephone call or wire communication, without the consent of all parties. CAL. PENAL CODE §§ 631–632 (2010). The appellate court has ruled that using a hidden video camera in a private place violates the statute. California v. Gibbons, 263 Cal. Rptr. 905 (Ct. App. 1989).

minimize the existence of personal data.[275] Employers are not required or encouraged to deploy intrusive monitoring technologies. Employees can freely deny or revoke consent to monitoring programs and their consent is presumed to be invalid as coerced, unless employers can prove that employees consented voluntarily (i.e., are given the option to say "no" without adverse consequences), which in practice limits or precludes the implementation of monitoring technologies altogether.

Global employers therefore have to navigate the contrasting legal environments carefully. There are ample opportunities for pitfalls and difficulties, for example, in connection with the global deployment of e-mail and web servers as well as anti-spam and virus protection filters, investigations into potential wrong-doings involving employees in multiple jurisdictions, management of multi-country teams and reporting lines, or short- and long-term secondments of employees.

Practical options for global employers include the following three approaches:

(1) Country-specific monitoring protocols tailored to local requirements and permissions. A multinational enterprise could determine, on a country-by-country basis, how much monitoring is necessary and permissible, and then develop information security and monitoring policies that are optimal for the particular jurisdiction. But this approach severely limits the ability to maintain global systems and policies, involves significant costs (for legal research, system design, and compliance maintenance), and does not even guarantee full compliance or optimal compromises for situations that involve several jurisdictions (e.g., investigations into alleged illegal practices that involve employees of several different subsidiaries, or concerns regarding harassment across borders where employees in one country e-mail offensive materials to employees in another).

(2) Reducing global surveillance to the standards permissible in the most restrictive jurisdiction. For example, a company with presences in the United States, the United Kingdom, and Germany could deploy only monitoring technologies and processes that comply with German data protection laws.

275. The collection, processing, and use of data is governed by the principles of data avoidance and data economy. In the interest of collecting as little data as possible, personal data shall only be collected to the extent required for the purposes of processing the relationship between the parties. For instance, the Federal Data Protection Act states the "data omission and data parsimony" principle, ensuring that no or as little as possible person-related data is collected, processed, and used. BUNDESDATENSCHUTZGETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Jan. 14, 2003, as amended, § 3a (Ger.). Consequently the technical infrastructure shall already minimize the amount of collected, processed, and used data. This data shall be kept in anonymous or pseudonymous form if possible.

This approach enables globally uniform systems and should help minimize potential exposure to employee privacy claims. However, this approach may leave the multinational enterprise unreasonably exposed to liability arising from employee misconduct in jurisdictions where monitoring is permissible and expected by governments and in courts applying due diligence standards, such as the United States.

(3) Regional combination approaches whereby intrusive technologies are deployed in the United States and jurisdictions with similarly lenient privacy laws, whereby restrictive jurisdictions are excluded. This approach tries to mitigate the disadvantages of the first option (high costs, fragmented systems and processes) and second option (undue exposure in jurisdictions where monitoring is permissible and expected) by differentiating on a regional basis or "country category basis." The global enterprise could develop policies that implement two or more levels of employee monitoring for certain jurisdictions or regions. This approach offers the comfort of remaining relatively close to local practices and requirements without investing extensively in legal research and country-specific systems and processes. But, as with any compromise, this approach tends to involve some trade-offs; for instance, without closely analyzing local requirements, companies cannot be sure that their practices fully comply with applicable law.

Global employees also have choices. In the United States, they can look for employers with less intrusive monitoring policies and quit when they receive notice that the policies have changed. If enough employees are sufficiently concerned, employer policies can be expected to change according to the dynamics of the labor marketplace. In the meantime, the employees may depart in favor of a different working situation. If the employees move to Europe, they will find a different legal environment. European employers cannot rely on notices that destroy the employees' privacy expectations and employees can freely deny or revoke consent to monitoring and surveillance at any time.

Thus, in Europe, employees have (but do not need, as a condition for legal protection) reasonable privacy expectations, whereas in the United States, employees currently do not have (but need, as a condition for legal protection) reasonable privacy expectations.