
Robert Sprague

Follow this and additional works at: https://repository.jmls.edu/lawreview

Part of the Business Organizations Law Commons, Computer Law Commons, Internet Law Commons, Labor and Employment Law Commons, and the Privacy Law Commons

Recommended Citation

https://repository.jmls.edu/lawreview/vol42/iss1/4

This Article is brought to you for free and open access by The John Marshall Institutional Repository. It has been accepted for inclusion in The John Marshall Law Review by an authorized administrator of The John Marshall Institutional Repository.
ORWELL WAS AN OPTIMIST:
THE EVOLUTION OF PRIVACY IN THE
UNITED STATES AND ITS DE-EVOLUTION
FOR AMERICAN EMPLOYEES

ROBERT SPRAGUE*

"Privacy is not merely a personal predilection; it is an important functional requirement for the effective operation of social structure."1

"You already have zero privacy—get over it."2

ABSTRACT

This Article argues that the difficulties associated with understanding and applying rights to privacy in modern America, and its near extinction, particularly for employees, are a direct result of the conceptual approach used to determine whether a legal right to privacy exists. This approach was formally adopted in the latter part of the twentieth century and it makes privacy protection dependent upon any given situation, determined by whether there is a reasonable expectation of privacy for that given situation. This makes the current right to privacy in the United States contextual, fluid, and easily subject to elimination. One of the greatest impacts on one's expectation of privacy—and, hence, one's right to privacy—is technology. In most cases, technology has eroded expectations of privacy—and, consequently, one's right to privacy. As employees spend more time at the workplace, and spend more time working at home, using increasingly advanced technology with greater frequency, the dichotomy of privacy

* J.D., M.B.A., Assistant Professor, Department of Management & Marketing, University of Wyoming College of Business. The author thanks Aaron J. Lyttle, J.D. 2010, University of Wyoming College of Law, for his excellent research assistance for this article.

1. ROBERT MERTON, SOCIAL THEORY AND SOCIAL STRUCTURE 429 (Free Press 1968) (1957) (internal quotation marks omitted).

protection between the highly protected home and the less-protected workplace begins to break down. Employees, for the most part, are unable to bring the stronger home-based privacy protections into work while, at the same time, employer interests begin to intrude upon the sanctity of the home. This Article argues that as more workers bring their work into their home and private lives, "workplace" restrictions on privacy will erode the one last bastion of privacy—one's home. Thus the concern is no longer limited to "workplace privacy" but employee privacy. This Article concludes that what few remaining privacy rights United States employees enjoy are in serious jeopardy, and recommendations are presented to re-establish employee privacy, particularly in the home.

I. INTRODUCTION

Employees have virtually no privacy. Job applicants are screened through personality tests, investigated by databases that uncover extensive financial and transactional histories, and scrutinized by what they publish or what is published about them on the Internet. Onsite, workers are subject to continuous video and electronic surveillance; even the amount of time they spend in the bathroom can be recorded. Every Internet address visited, every computer keystroke made, every phone number dialed can be recorded—and not just at the office but also in employees’ homes if the employer provides cell phones, BlackBerrys, and computers. Offsite, employees’ whereabouts can be tracked twenty-four hours per day, seven days a week. The employer has the potential to be a Big Brother, always watching, listening, and recording.3

While this description of an omniscient employer is a reality in the twenty-first century, employee monitoring is not a new concept. In the early twentieth century, Frederick Taylor introduced "scientific management" techniques to improve workplace efficiency.4 With Taylor’s scientific management approach, workers were under the constant surveillance of a manager with a stopwatch.5 Through the twentieth century, the

3. See generally GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949) (introducing into American culture the phrase “Big Brother Is Watching You” to describe an omnipresent government that monitored every aspect of the populace).


5. See ROBERT KANIGEL, THE ONE BEST WAY 466 (1997) (providing that to workers, the stopwatch “was a hideous invasion of privacy, an oppressive all-seeing eye that peered into their work lives, ripping at their dignity”); see also Terry Morehead Dworkin, It’s My Life—Leave Me Alone: Off The-Job Employee
office replaced the factory floor, with telephones, computers, e-mail, and the Internet becoming the tools of the modern workplace.  

In 1990, Gary Marx envisioned a company attempting to improve productivity by using technology to select and monitor its employees. Marx's hypothetical and omniscient corporation believed the ends justified the means—improving productivity and profitability by breaking down the barrier between work and home, selecting only healthy job applicants to reduce absenteeism, evaluating performance through impersonal, objective, and less-expensive computer programs, and strengthening loyalty through visibility by monitoring every aspect of work. Most prescient, Marx's hypothetical corporation recognized that instant communication is vital in a global economy: "The global market does not function only from 9 to 5. Modern technology can greatly increase productivity by ensuring instant access and communication. Periodic disruptions to vacations or sleep are a small price to pay for the tremendous gains to be won in worldwide competition."  

Marx's hypothetical corporation is becoming more of a reality. American employers routinely monitor employees. And the 24/7/365 always-connected employee is becoming the norm.

---

*Associational Privacy Rights*, 35 AM. BUS. L.J. 47, 47 (1997) (discussing Ford Motor Company's early twentieth century investigators "who monitored employees—often in their homes—to make sure they did not drink too much, they led 'unblemished' sex lives, their houses were clean, and their leisure time properly spent") (footnote omitted).


8. Id. at 12-13.

9. Id. at 14-15.

10. Press Release, American Management Association, 2007 Electronic Monitoring & Surveillance Survey (Feb 28, 2008), available at [http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey](http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey). Nearly two-thirds of employers surveyed monitored Internet connections; nearly half track the content, keystrokes, and time spent at the computer keyboard; 43% monitor e-mail; as for telephone and voice mail, 45% monitor time spent and numbers called, another 16% record phone conversations, and an additional 9% monitor employees' voicemail messages; nearly half use video monitoring (though primarily to counter theft, violence and sabotage—only 7% use video surveillance to track employees' on-the-job performance); and 8% use Global Positioning Systems ("GPS") to track company vehicles, 3% use GPS to monitor cell phones, and fewer than 1% use GPS to monitor employee identification cards. *Id.*

Employee monitoring technologies have reached to point that four states—California, Missouri, North Dakota, and Wisconsin—have taken the preemptive step of enacting legislation prohibiting employers from embedding radio frequency identification ("RFID") chips in their employees.

This penchant for monitoring is somewhat understandable in context of the degree of surveillance Americans undergo. A number of federal intelligence and law enforcement agencies routinely sift, store and analyze the communications, spending habits and travel patterns of United States citizens, searching for suspicious activity. Meanwhile, according to witnesses testifying

lawsuits by employees who find themselves constantly working due to their continuous electronic connections to work). A BlackBerry is a hand-held device that connects wirelessly to the Internet, providing e-mail, phone, and other communications capabilities. See Blackberry, Blackberry Enterprise Solution Overview, http://na.blackberry.com/eng/ataglance/solutions/ (last visited Dec. 23, 2008).

12. CAL. CIV. CODE § 52.7 (West 2008) (prohibiting any person from requiring, coercing, or compelling any other individual to undergo the subcutaneous implanting of an identification device).


14. N.D. CENT. CODE § 12.1-15-06 (2008) (prohibiting a person from requiring that an individual have inserted into that individual's body a microchip containing a radio frequency identification device).

15. Wis. STAT. § 146.25 (2008) (prohibiting a person from requiring an individual to undergo the implanting of a microchip).

16. See CAL. CIV. CODE § 52.7(h)(1) (defining "identification device" as any item capable of transmitting personal information, including but not limited to, devices using radio frequency technology).

17. See Bradley Olson, Domestic Spying Quietly Goes On, BALTIMORE SUN, July 7, 2008, at 1A ("There's virtually no branch of the U.S. government that isn't in some way involved in monitoring or surveillance"); see also id. (quoting Matthew Aid, an intelligence historian and fellow at the National Security Archives at The George Washington University).

before the Senate Subcommittee on the Constitution, United States border agents are copying and seizing the contents of laptops, cell phones and digital cameras from United States and foreign travelers entering the United States.\textsuperscript{18} The National Security Agency ("NSA") reportedly has the ability to eavesdrop on all communications in the United States—landlines, cell phones, e-mails, BlackBerry messages, and Internet searches.\textsuperscript{19}

But the United States government is not the only entity collecting information about United States citizens. The amount of personal information collected by private businesses is vast. One company reportedly maintains databases of credit and demographic information for over 200 million Americans, while another company reportedly has over 14 billion records on individuals and businesses for uses such as pre-employment screening of job candidates.\textsuperscript{20} Corporations routinely record consumer transactions, selling dossiers of personally identifiable information to direct marketers and data collectors.\textsuperscript{21} Consumers are often unaware of the increasingly sophisticated methods devised to collect information about them.\textsuperscript{22} Websites engage in "behavior advertising"—tracking consumers’ activities online in an


\textsuperscript{19} Bamford, supra note 17. “NSA personnel . . . have the ultimate goal of intercepting and reviewing every syllable and murmur zapping into, out of, or through the United States . . . with . . . massive dishes vacuuming the airwaves, and electronic ‘packet sniffers,’ software that monitors network traffic, diverting e-mail and other data from fiber-optic cables . . . .” Id. at 70.


\textsuperscript{21} Stan Karas, Privacy, Identity, Databases, 52 AM. U. L. REV. 393, 394 (2002).

\textsuperscript{22} Paul M. Schwartz, Property, Privacy, and Personal Data, 117 HARV. L. REV. 2055, 2056 (2004); see also Brett Winterford, Logged In or Out, Facebook Is Watching You, ZDNET AUSTRALIA, Dec. 4, 2007, available at http://www.zdnet.com.au/news/security/soaLogged-in-or-out-Facebook-is-watching-you/0,130061744,339284281,00.htm (reporting that the popular social networking site Facebook is able to track the buying habits of its users on affiliated third-party websites even when the users are logged out of their Facebook account or have opted out of Facebook’s tracking service); see also Jeffrey Rosen, The Eroded Self, N.Y. TIMES MAG., Apr. 30, 2000, at 46-49 (describing consumer electronics that can communicate with one another, as well as websites, through networks; warning that the incessant information exchanged by these appliances can generate detailed records of the most intimate details of an individual’s daily life; foreseeing a situation in which one’s liquor cabinet automatically orders replenishments from the local liquor store while also prompting the television to display ads for alcoholics anonymous).
attempt to increase the effectiveness of their advertising by targeting advertisements more closely to the interests of their audience.\textsuperscript{23}

Corey Ciocchetti has documented the extent to which personal information can be quickly and easily obtained. The University of Denver professor provided his name, address, and $29.95 to an online investigations company—fifteen minutes later he received via e-mail a fairly comprehensive dossier on himself, including an extensive address history (reaching back to his days as a second-grader), past and present property ownership records, political party affiliation, various information concerning his current neighbors and past relatives (including his father-in-law’s ex-wife); and, if it had applied, the dossier would have also included known aliases, results of a nationwide criminal search, sexual offense conviction records, bankruptcies, tax liens and judgments, UCC filings, airplane and boat registrations, and hunting, fishing, and concealed weapons permits.\textsuperscript{24} “Individually, each of these pieces of personal information represents a mere pixel of my life, but when pieced together, they present a rather detailed picture of my identity.”\textsuperscript{25}

Is there no privacy in modern America?\textsuperscript{26} Solove asserts that privacy is a concept in disarray, with philosophers, legal theorist, and jurists frequently lamenting the great difficulty in reaching a

\begin{itemize}
\item \textsuperscript{24} Corey A. Ciocchetti, E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors, 44 AM. BUS. L.J. 55, 55 (2007).
\item \textsuperscript{25} Id. at 56; see also Helen Nissenbaum, Privacy in an Information Age: The Problem of Privacy in Public, 17 LAW & PHIL. 559, 561 (1998) (“people have become targets of surveillance at just about every turn of their lives.”) “In transactions with retailers, mail order companies, medical care givers, daycare providers, and even beauty parlors, information about them is collected, stored, analyzed and sometimes shared.” Id.
\item \textsuperscript{26} Not according to Google, Inc. In May 2007, Google introduced its “Street View” feature that links with Google’s Maps feature, providing panoramic street-level views of various streets and roads in major cities in the United States. Defendant Google Inc.’s Memorandum of Law in Support of Its Motion to Dismiss Complaint at 5, Boring v. Google, Inc. No. 08-cv-694 (W.D. Pa. filed May 28, 2008). To create the Street View feature, drivers with panoramic cameras attached to the roofs of cars drive around various cities filming continuous footage of the view from the streets of these cities. See id. Residents in Pittsburgh, Pennsylvania, whose homes were captured by Street View cameras, sued Google for, \textit{inter alia}, invasion of privacy. See id. at 3, 5. Countering the \textsc{RESTATEMENT (SECOND) OF TORTS'} comment that “[c]omplete privacy does not exist... except in a desert,” Google asserts, “[t]oday's satellite-image technology means that even in today's desert, complete privacy does not exist.” Id. at 1-2, (quoting \textsc{RESTATEMENT (SECOND) OF TORTS,} § 652D cmt. c (1977)). The court denied the Boring’s claim of invasion of privacy, granting Google’s Motion to Dismiss the Boring’s complaint. Memorandum Opinion, Boring v. Google, Inc. No. 08-cv-694 (W.D. Pa. filed Feb. 17, 2009).
\end{itemize}
satisfying conception of privacy.\textsuperscript{27} This article argues that the difficulties associated with understanding and applying rights to privacy in modern America, and its near extinction for employees, are a direct result of the conceptual approach used to determine whether a legal right to privacy exists. This approach was formally adopted in the latter part of the twentieth century and it makes privacy protection dependent upon any given situation, determined by whether there is a reasonable expectation of privacy for that given situation. This makes the current right to privacy in the United States contextual, fluid,\textsuperscript{28} and easily subject to elimination.

One of the greatest impacts on one’s expectation of privacy—and, hence, one’s right to privacy—is technology. In some cases, technology has created an expectation of privacy where one did not previously exist.\textsuperscript{29} But in most cases, technology has eroded expectations of privacy—and, consequently, one’s right to privacy.\textsuperscript{30} To paraphrase James Bamford, this article addresses

\begin{itemize}
  \item \textsuperscript{27} See Daniel J. Solove, Understanding Privacy 1 (2008).
  \item \textsuperscript{28} “[P]rivacy . . . is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy . . ..” Sanders v. Am. Broad. Cos., 978 P.2d 67, 72 (Cal. 1999); see also Bevan v. Smartt, 316 F. Supp. 2d 1153, 1160-61 (D. Utah 2004) (holding night club dancers had no expectation of privacy regarding video surveillance of their dressing room, of which they were aware, by club security personnel, but did have an expectation of privacy as to government agents viewing the same surveillance without a warrant; loss of privacy in one context, such as undressing in one’s home before an open window, does not lead to loss of privacy in other aspects, such as an unwarranted search by police of that same home for illegal drugs); see generally Brief and Argument for Appellant, State v. Jahnke, No. 06-CF-169 (Wis. Ct. App. filed Nov. 26, 2007) (raising issue of whether a woman has an expectation of privacy as to unpublished pictures taken of her in the nude without her knowledge and consent by her boyfriend, before whom she has knowingly and voluntarily appeared nude).
  \item \textsuperscript{29} See, e.g., Susan W. Brenner, The Fourth Amendment in an Era of Ubiquitous Technology, 75 MISS. L.J. 1, 8-12 (2005) (describing how in the mid-1800’s the self-sealing adhesive envelope was introduced, meaning letters could be truly sealed, arguably leading to the U.S. Supreme Court’s later ruling that sealed letters in the mail are subject to Fourth Amendment search and seizure requirements); see also infra note 117 and accompanying text (discussing constitutional guarantee of the right of individuals to be secure in their papers). A similar transformation took place with the telephone. In the early days of telephone service, phones had no dial tone, and, with party lines, the only way to determine whether a line was available was to listen to whether a conversation was taking place. Robert Ellis Smith, Ben Franklin’s Web Site: Privacy and Curiosity from Plymouth Rock to the Internet 155 (2000). Then, all calls were placed through human operators, who could also listen to conversations. See id. at 155-56. Expectations of telephone privacy drastically increased in 1899 when automated switching technology was introduced, allowing individuals to directly dial other parties on a private line. See id. at 156.
  \item \textsuperscript{30} Professor Austin noted that: technology is not simply eroding our privacy—it may also be forcing us
the issue of what happens when technology outstrips the law’s ability to protect employees from it.\textsuperscript{31}  

Understanding the state of the modern right to privacy in the United States, particularly for employees, requires an understanding of the development of privacy, both as a human concept and as a legally protectable right. Part I of this Article provides a brief history of the evolution of the concept of privacy up to the late nineteenth century, at which point privacy was beginning to be recognized as a legal right in the United States. Part II of this Article reviews the development of the right to privacy within the United States, focusing on three sources: common law; the Constitution; and specific federal statutes.  

Part III of this Article focuses on privacy in the workplace. Americans spend a good deal of their waking hours at work, so the degree of privacy enjoyed in the workplace is not a trivial matter.\textsuperscript{32}  

The focus of Part III is on the degree to which employees have a reasonable expectation of privacy with regard to their employers. One theme reflected throughout this Article is privacy in one’s home (“a man’s house is his castle”). But as employees spend more time at the workplace, and spend more time working at home, the dichotomy of privacy protection between the highly protected home\textsuperscript{33} and the less-protected workplace\textsuperscript{34} begins to break down. Employees, for the most part, are unable to bring the stronger

\begin{itemize}
\item to rethink what we mean by privacy. Increasingly, what we are worried about are practices that involve collecting, using and disclosing information that is not sensitive or intimate and that is increasingly collected in public—concerns that do not easily fall within the domain of traditional privacy theory.
\end{itemize}


31. See Bamford, supra note 17 (writing specifically about NSA surveillance capabilities: “What happens when the technology of espionage outstrips the law’s ability to protect ordinary citizens from it?”).

32. It is, unfortunately, all too true that the workplace has become another home for most working Americans. Many employees spend the better part of their days and much of their evenings at work... Consequently, an employee’s private life must intersect with the workplace... As a result, the tidy distinctions... between the workplace and professional affairs, on the one hand, and personal possessions and private activities, on the other, do not exist in reality.


home-based privacy protections into work while, at the same time, employer interests begin to intrude upon the sanctity of the home. And even in cases where employees have a reasonable expectation of privacy, there is no guarantee the employer is legally prohibited from intruding into its employees' personal affairs.

Part IV of this article turns its attention to technological developments—particularly how such developments blur the distinction between work and home—and how technology can blur the distinction between rights to privacy at work and at home. This article argues that as more workers bring their work into their home and private lives, "workplace" restrictions on privacy will erode the one last bastion of privacy—one's home. Thus the concern is no longer limited to "workplace privacy" but employee privacy. Part IV concludes that what few remaining privacy rights United States employees enjoy are in serious jeopardy, and recommendations are presented to re-establish employee privacy, particularly in the home.

II. A BRIEF HISTORY OF PRIVACY

Privacy has been described as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." Privacy has also been described as "a zone of immunity to which we may fall back or retreat, a place where we may set aside arms and armor needed in the public place, relax, take our ease, and lie about unshielded by the ostentatious carapace worn for protection in the outside world." Four basic "states" of privacy have been identified: (1) solitude, where an individual is separated from the group and freed from the observation of others; (2) intimacy, where an individual exercises seclusion to achieve a closer relationship with others; (3) anonymity, the freedom from identification and surveillance in public places or while performing public acts; and (4) reserve, the creation of a psychological barrier against unwanted intrusions.

Privacy is not necessarily a distinctly human trait. Studies reveal that virtually all animals seek periods of individual

35. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); see also Margaret Mead, Margaret Mead Re-examines Our Right to Privacy, REDBOOK, Apr. 1965, at 15 (describing privacy as "the right to live part of one's life out of the public eye, according to one's own choice, and free from interference by others . . . ").


37. WESTIN, supra note 35, at 31-32; see also SOLOVE, supra note 27, at 13 (identifying six types of privacy: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control over personal information; (5) personhood; and (6) intimacy).

38. WESTIN, supra note 35, at 8.
seclusion or small-group intimacy, as well as elaborate distance-setting mechanisms to define territorial spacing of individuals in the group—i.e., establishing "personal distance." Nor is privacy a construct just of modern, complex societies. "Anthropological studies have shown that the individual in virtually every society engages in a continuing personal process by which he seeks privacy at some times and disclosure or companionship at other times."

Historians suggest it was not until the second century A.D. (at least in Western civilization) that recognition of the self entered society. It was at this point that "[w]hat was most private in the individual, his or her most hidden feelings and motivations..." were beginning to be acknowledged. In the feudal age (approximately 1000 A.D.), privacy evolved to the concept "that there are acts, individuals, and objects by law not subject to public authority; for that reason they are situated in a precisely delineated sphere designed to thwart any attempt at intrusion." By the end of the first millennium, the typical home had become an "intimate haven".

Private life took on greater importance in the Middle Ages as the "[t]he cult of urbanity collapsed, and private life took its place." By the fourteenth century, the family was the heart of private life. The emphasis on the family and the individual continued from 1500 to 1800 as the notion of private life, derived from "a change in the forms of sociability: from the anonymous social life of the street, castle courts, square, or village to a more restricted sociability centered on the family or even the individual." The declaration that "a man's home is his castle" aptly summarizes not just the security, but also the solitude, afforded by the family dwelling. While this maxim dates to

39. Id. at 8-9 (footnote omitted).
40. Id. at 13.
41. Peter Brown, Late Antiquity, in I A HISTORY OF PRIVATE LIFE, supra note 36, at 229-32.
42. Id. at 254. Previously, there was some hostility to the notion of privacy. Id. Plato considered the guardians of the city to be subject to complete publicity. STANLEY ROSEN, PLATO'S REPUBLIC 129 (2005).
44. Evelyne Patlagean, Byzantium in the Tenth and Eleventh Centuries, in I A HISTORY OF PRIVATE LIFE, supra note 36, at 571.
48. "[T]he house of every one is to him as his castle and fortress, as well for his defense against injury and violence as for his repose." Pavesich v. New
Roman law, where "to enter a man's house against his will, even to serve a summons, was regarded as an invasion of his privacy[.]"\textsuperscript{49} it was quickly adopted in the emerging United States:

An Englishman's dwelling House is his Castle. The Law has erected a Fortification around it—and as every Man is Party to the Law, i.e. the Law is a Covenant of every Member of society with every other Member, therefore every member of Society has entered into a solemn Covenant with every other that he shall enjoy in his own dwelling House as compleat a security, safety and Peace and Tranquility as if it was surrounded with Walls of Brass, with Ramparts and Palisadoes and defended with a Garrison and Artillery.\textsuperscript{50}

Along with the notion of the private home, there were also signs of growing personal autonomy, beginning in the twelfth century.\textsuperscript{51} Social taboos against a desire for solitude began to fade by the end of the seventeenth century,\textsuperscript{52} and "[t]he sense of individual identity became more distinct and spread more widely throughout the nineteenth century."\textsuperscript{53} It is also at the beginning of the nineteenth century that formal legal rights to privacy began to be recognized in England and the United States.

III. THE RIGHT TO PRIVACY IN THE UNITED STATES

There are three primary sources of a legal right to privacy in the United States: common law, constitutional law, and federal statutes. Despite their various sources and differing priorities, there are two common themes to United States rights to privacy: (1) the home is given the greatest protection; and (2) all require an underlying expectation of privacy which can only be invaded by an unreasonable intrusion.

\textsuperscript{49} Id. (quoting Hunter's Roman Law (3d ed.) 149 (alteration in original)).

\textsuperscript{50} 1 LEGAL PAPERS OF JOHN ADAMS 137 (L. Kinvin Wroth & Hiller B. Zobel eds., 1965), quoting Adams' notes of his argument in the 1774 case King v. Stewart, in which a mob had broken into the home of a District of Maine merchant, destroying windows and furniture and burning papers; see also Phile v. The Ship Anna, 1 U.S. 197, 206 (1787) (balancing the interests of the public associated with seizing contraband versus personal privileges, as in "a man's house is considered as his castle"). This maxim also serves as the fundamental motivation for the Fourth Amendment to the U.S. Constitution. See Weeks v. United States, 232 U.S. 383, 390 (1914) (recognizing the maxim that "every man's house is his castle" is made a part of constitutional law in the clause prohibiting unreasonable searches and seizures) (internal quotation marks and citation omitted).


\textsuperscript{52} See Ariès, supra note 47, at 5.

A. The Development of the Common Law Right to Privacy in the United States

Physical life in colonial America dictated part of the evolution of privacy in the United States. In some aspects there was almost no privacy. It was expected that travelers would share a bed, either in a tavern or the home of an acquaintance—hence the term "bedfellow." The manner in which homes were constructed permitted "eaves-droppers" to literally stand under the eaves of houses and listen to the conversations inside. Due to the abundance of open space in early America, it has been argued that a formal privacy legal regime was stymied by the "vast opportunities for solitude or for a fresh start far away." In addition, early Americans’ penchant for settling perceived invasions of personal privacy with duels, horsewhippings, or shootings often negated the need for formal legal proceedings. From very early on, though, citizens of the emerging United States did fashion formal legal protections against unwanted intrusions, either from overly curious individuals or the government.

54. See SMITH, supra note 29, at 19-20 (discussing the practice of bed-sharing primarily due to the lack of beds and for warmth). This also explains how it was that Ishmael first met his companion Queequeg when they shared a bed in the Spouter-Inn: "Upon waking the next morning about daylight, I found Queequeg's arm thrown over me in the most loving and affectionate manner. You had almost thought I had been his wife." HERMAN MELVILLE, MOBY DICK 28 (Northwestern University Press) (1988).

55. See DAVID J. SEIPP, THE RIGHT TO PRIVACY IN AMERICAN HISTORY 2 (1978) (discussing how home construction made listening to private conversations possible).

56. SMITH, supra note 29, at 76; see also Thomas H. O'Connor, The Right to Privacy in Historical Perspective, 53 MASS. L. Q. 101, 104-5 (1968) (asserting that, particularly as a result of the Louisiana Purchase, "the solitary isolation of the explorers, the pioneers, and the settlers of the West was so absolute that privacy was assured by the very physical dimensions which circumscribed the frontier") (citation omitted).

57. See id. at 103 (asserting also that an invasion of privacy was usually viewed as a matter of personal honor).

58. "As soon in the progress of civilization as men ... retreated into private houses, a desire on the part of their neighbors to know what was going on in the private houses sprang up rapidly, and has flourished ever since the world over." E. L. Godkin, The Rights of the Citizen. IV.—To His Own Reputation, SCRIBNER'S MAG., July-Dec. 1890, at 58, 66 (relating also the story of a traveler visiting a western mining town who pinned a shirt across his open window for privacy, only to see a hand draw it aside and a voice ask, "[w]e want to know what there is so darned private going on in there?"). "[T]he courts in colonial New England protected privacy in indirect or derivative fashion, by prosecuting trespassers, limiting search and seizure, entertaining defamation cases, and protecting the privileged communications of husbands and wives in the courtrooms." DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 248 (1972); see also infra notes 111-48 and accompanying text (discussing how the Fourth Amendment to the United States Constitution is recognized as the one provision within the Constitution that provides some
Eavesdropping was considered an actionable public nuisance in England by the beginning of the nineteenth century, and adopted by American courts early in the nineteenth century: "No man has a right to pry into your secrecy in your own house." At least two courts early on recognized a right of privacy beyond eavesdropping. In Dennis v. LeClerc, a Louisiana court prohibited a newspaper editor from publishing the contents of a letter without permission from the sender. And in De May v. Roberts, in which a doctor allowed an unmarried man with no medical training to be present while a woman gave birth, the court acknowledged the woman’s right to privacy during “a most sacred” occasion, stating “[i]t would be shocking to our sense of right, justice and propriety to doubt even but that for such an act the law would afford an ample remedy.”

During the latter part of the nineteenth century, two developments occurred which had direct bearing on the evolution of common law rights to privacy in the United States. One development was the emergence of the press. Although

---

59. See Sir William Blackstone, Commentaries on the Laws of England 168-69 (Thomas B. Wait, & Co. 1807) (classifying eavesdropping as one of seven wrongs whose punishment is short of death). "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]." Id. 60. Commw. v. Lovett, 4 Pa. L.J. Rpts. (Clark) 226, 226 (Pa. 1831) (recognizing “eaves-dropping” as an actionable offense in Pennsylvania, though declining to find the defendant guilty because he was hired by a husband to spy on the husband’s wife); see also SEIPP, supra note 55, at 4-5 (upholding an eavesdropping indictment as “consistent with the situation of any society whatever”) (internal quotation marks omitted). Additional privacy-related wrongs were recognized in early nineteenth-century law, including those related to gossips, common scolds, and peeping toms. See Blackstone, supra note 59, at 168 (describing the common scold as a public nuisance); SEIPP, supra note 55, at 6 (noting victims of the “incorrigible gossipmonger” could have recourse to the law of defamation); Lance E. Rothenberg, Re-Thinking Privacy: Peeping Toms, Video Voyeurs, and Failure of the Criminal Law to Recognize a Reasonable Expectation of Privacy in the Public Space, 49 Am. U. L. Rev. 1127, 1140-42 (2000) (describing the origin of the term “peeping tom” as well as early prosecutions as a breach of the peace). 61. 1 Mart. (o.s.) 297 (Orleans 1811); see Neil M. Richards & Daniel J. Solove, Privacy’s Other Path: Recovering the Law of Confidentiality, 96 Geo. L.J. 123, 143 (2007). But see Westin, supra note 35, at 337, n.25 (listing similar cases with different results). There was initially no institutionalized postal service in colonial America. See SEIPP, supra note 55, at 7; see also infra note 117 and accompanying text (discussing how official postal services were established and much of the concern regarding privacy in letters was directed to government prying, and therefore generally fell under Fourth Amendment search and seizure restrictions). 62. 9 N.W. 146, 148-49 (Mich. 1881).
newspapers had long contained salacious material, the number and aggressiveness of newspapers increased during the latter part of the nineteenth century. "Keyhole journalism" drove circulations, to the extent that "prying sensationalism robbed American life of much of its privacy, to the gain chiefly of morbid curiosity." Critics worried that the growth of journalism had developed an "inordinate hunger and thirst for gossip," to the degree that the maxim "a man's home is his castle" was becoming simply a relic.

The second development impacting the evolution of common law rights to privacy was a spate of technological advancements. The period from 1844 to 1888 gave rise to, among a variety of new technologies, the telegraph, the typewriter, the telephone, the dictating machine, and the instant camera. All of these

63. See, e.g., WALTER ISAACSON, BENJAMIN FRANKLIN: AN AMERICAN LIFE 64-69 (2003) (discussing how Franklin's Pennsylvania Gazette contained some salacious information, including stories involving sex, outlandish crimes, as well as gossip).

64. See SEIPP, supra note 55, at 67 (noting that the number of newspapers doubled each decade from 1870 to 1899).

65. FRANK LUTHER MOTT, AMERICAN JOURNALISM: A HISTORY OF NEWSPAPERS IN THE UNITED STATES THROUGH 250 YEARS 1690 TO 1940 444 (1941) (describing keyhole journalism as "closely connected with sensationalism ... was the invasion of privacy by prying reporters. The prevalence of gossip and scandal stories, in which innocent persons were frequently dragged into the columns of newspapers, produced a kind of 'keyhole journalism'..."); see also Augustus A. Levey, The Newspaper Habit and Its Effects, 143 N. AM. REV. 309 (1886) (describing the "Newspaper Habit" as satisfying the thirst for scandal).

66. ARTHUR MEIER SCHLESINGER, THE RISE OF THE CITY 1878-1898 194 (1933); see also Joseph B. Bishop, Newspaper Espionage, 1 FORUM 533, 534 (1886) (describing the conduct of the press during President Grover Cleveland's honeymoon, standing in the bushes outside the bridal cottage and examining the dishes when meals were sent from the hotel to the cottage); MOTT, supra note 65, at 510-11 (noting also that when Cleveland was married in a "private" ceremony at the White House, reporters surrounded the White House, vowing not to let the newlyweds escape them). But see ISAACSON, supra note 63, at 70 (describing a letter Benjamin Franklin wrote and published anonymously in his own newspaper defending gossip as keeping some people from becoming too popular while maintaining the virtue of others who fear being exposed in the press).

67. George T. Rider, The Pretensions of Journalism, 135 N. AM. REV. 471, 478 (1882) ("[I]ndeed, we are in danger of becoming a nation of gossips").

68. M. J. Savage, A Profane View of the Sanctum, 141 N. AM. REV. 137, 146 (1885) ("And the sturdy old British saying that 'An Englishman's house is his castle' seems to be regarded as a relic of the ... old world that has no place in a free and glorious republic like ours").

69. See SMITH, supra note 29, at 123 (listing technological developments in the latter half of the nineteenth century); see also Robert E. Mensel, "Kodakers Lying in Wait": Amateur Photography and the Right to Privacy in New York, 1885-1915, 43 AM. Q. 24, 25 (1991) (discussing the impact of unprecedented technological change upon the public's psyche as well).
technologies combined to drive the growth and breadth of
technologies. Instant photography had a particularly significant
impact. It has been argued "that amateur photography played an
important role in provoking outrage among editorial
commentators, judges, and legislators which eventually helped
lead to the recognition of the right to privacy...." It was not
just "Kodakers" lying in wait to photograph unsuspecting
prominent members of society that led to privacy concerns. As
noted above, the development of the self was one of the
foundations of the notion of privacy, and "[t]he most important
factor in the development of individual self-awareness was the
spread of the [photographic] portrait...." However, "[a]fter
1880 amateur photographers were able to cut out the professional
middleman. Thereafter poses became less elaborate, and all of
private life was laid open to the lens, whose appetite for intimate
scenes was unlimited."

Meanwhile, libel laws became less onerous through court
decisions and legislation, affirming that truth was a complete
defense to libel. In practice, libel law did little to protect the
individual, often inviting further publicity to compound the
damage. Godkin noted also that at that time there was
confusion and uncertainty in the public mind as to what was
libelous and what was not. Short of shooting the "newspaper

70. See SEIPP, supra note 55, at 67 (discussing the growth of newspapers).
71. Mensel, supra note 69, at 25 (referring specifically to the recognition of
a right to privacy in the state of New York, it being the first state to enact
privacy-related legislation).
72. See J. Flynn, Letter to the Editor, The Right of Privacy, N.Y. TIMES,
Aug. 23, 1902, at 8.
73. See supra notes 41-42 and accompanying text.
74. Corbin, supra note 53, at 460.
75. Id. at 466; see also The Legal Relations of Photographs, 17 AM. L. REG.
1, 8 (1869) (predicting that an embarrassing clandestine photograph could
serve as the basis of a libel suit).
76. See MOTT, supra note 65, at 508-09.
77. See SEIPP, supra note 55, at 73 (noting that formerly, the legal maxim
had been "the greater the truth, the greater the libel"); The Legal Relations of
Photographs supra note 75, at 8 (discussing truth as a defense to libel).
78. See John Bascom, Public Press and Personal Rights, 4 EDUC. 604, 605
(1884) (discussing the initial effect of libel laws); see also SEIPP, supra note 55,
at 72 (reviewing the application of libel laws). For a modern application of this
phenomenon, see John F. Burns, A British Trial About Privacy in Which Not a
Shred Remains, N.Y. TIMES, July 9, 2008, at A1 (describing the breach of
privacy action brought by Max Mosley, president of the International
Automobile Federation, against the News of the World, a London, England,
tabloid, which ran a story, accompanied by a video, of a supposed "Nazi-
themed sex orgy" Mr. Mosely arranged and participated in; resulting in Mr.
Mosely detailing in court testimony his 45-year passion for sadomasochism).
79. See Godkin, supra note 58, at 63 (detailing the public misunderstanding
of libel laws).
editor who was considered to have overstepped the boundaries of
good taste or discretion[,]"80 there were few effective legal remedies
to thwart the "hungry eyes" of the press peering "into private houses[]."81

Returning to the maxim, "a man's house is his castle," in mid-
1890 Godkin claimed a "natural right" to decide how much the
public may know of an individual's personal thought and feeling,
tastes, habits, and private doings and affairs, including those of
the family living under one's roof.82 Shortly thereafter, Samuel
Warren and Louis Brandeis published The Right to Privacy in the
Harvard Law Review.83 Their principal objection was the
overzealous press and new technologies: "Instantaneous
photographs and newspaper enterprises 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.'"84
Warren and Brandeis called for a right "to be let alone,"85 and

80. O'Connor, supra note 56, at 103.
81. Rider, supra note 67, at 479. See also Godkin, supra note 58, at 66
("The chief enemy of privacy in modern life is that interest in other people and
their affairs known as curiosity, which in the days before newspapers created
personal gossip.").
82. Godkin, supra note 58, at 65.
83. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 HARV.
L. REV. 193 (1890).
84. Id. at 195. "The press is overstepping in every direction the obvious
bounds of propriety and of decency. Gossip is no longer the resource of the idle
and the vicious, but has become a trade, which is pursued with industry as
well as effrontery." Id. at 196. (reporting that the authors' impetus for The
Right to Privacy was newspaper articles regarding Warren's family). Warren's
father-in-law, a U.S. Senator, presidential candidate, and Secretary of State,
was reportedly the frequent target of negative news coverage. SMITH, supra
note 29, at 121. Prosser reports Warren became annoyed "when the
newspapers had a field day on the occasion of the wedding of a daughter."
Warren's oldest daughter could not have been more than seven years old in
1890, it is suggested it was the reporting of the wedding of a cousin which
gave rise to The Right to Privacy. See James H. Barron, Warren and Brandeis,
The Right to Privacy, 4 Harv. L. Rev. 193 (1890): Demystifying a Landmark
Citation, 13 SUFFOLK U. L. REV. 875, 894 (1979) (noting that it "[i]s the public
disclosure that there were 'no bridesmaids' the embarrassing incident that
'launched a thousand lawsuits?'").
85. Warren & Brandeis, supra note 83, at 195 (footnote omitted). Warren
and Brandeis borrowed this term from the law relating to personal
immunity—i.e., assault. THOMAS M. COOLEY, TREATISE ON THE LAW OF TORTS
OR THE WrONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1880) (finding
that "[t]he right to one's person may be said to be a right of complete
immunity: to be let alone"); see also Union Pac. Ry. Co. v. Botsford, 141 U.S.
250 (1891) (affirming the lower court's denial of Union Pacific's motion to
surgically examine Botsford, who had brought a personal injury action against
Union Pacific). "No right is held more sacred, or is more carefully guarded, by
the common law, than the right of every individual to the possession and
echoing Godkin, they asserted that the "common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."  

Godkin apparently did not believe The Right to Privacy would have much influence. He argued that too many people demanded scandal and gossip. In contrast, an 1891 commentary in Scribner's Magazine was a bit more optimistic, supporting the right to privacy put forth in The Right to Privacy: "it is high time this thing were understood." At the close of the nineteenth century, Warren and Brandeis had laid the groundwork for a formalized development of a common law right to privacy in the United States.  

As Prosser notes, the development of a common law right to privacy was fairly slow initially after the publication of The Right to Privacy. Although a few courts appeared ready to recognize a legal right to privacy, in Roberson v. Rochester Folding Box Company, the New York Court of Appeals declared in a four-to-three decision there could be no common law right of privacy. Evidently, public disapproval of Roberson was so strong, one of the concurring judges was compelled to author a law review article justifying the decision. Roberson involved the commercial use by control of his own person, free from all restraint or interference of others, unless by clear and unquestionable authority of law." Id. at 251.

86. Warren & Brandeis, supra note 83, at 198 (footnote omitted). Though Warren and Brandeis made two references to Godkin's The Rights of the Citizen, supra note 58, in The Right to Privacy, it was Warren's "deepseated abhorrence of the invasions of social privacy" that was the genesis of the article. Barron, supra note 84, at 888 (quoting letters between Warren and Brandeis).

87. E. L. Godkin, The Right to Privacy, THE NATION, Dec. 25, 1890, at 496, 497 (noting that "[w]e fear there is no lymph in either common or statute law for this most deplorable form of moral tuberculosis").

88. The Point of View, SCRIBNER'S MAG., Jan.-Jun. 1891, at 261.

89. See Barron, supra note 84, at 877 (noting near unanimity among courts and commentators that The Right to Privacy created the structural and jurisprudential foundation of the tort of invasion of privacy).

90. See Prosser, supra note 84, at 384 (noting "[t]he article had little immediate effect upon the law.").

91. See id. at 384-85 (discussing an unreported decision of a New York trial judge enjoining the unauthorized photograph of a stage actress taken by an audience member, followed by three additional New York cases and a Massachusetts federal court coming close to recognizing a right to privacy).

92. 64 N.E. 442, 447 (N.Y. 1902).

An examination of the authorities leads us to the conclusion that the so-called 'right of privacy' has not as yet found an abiding place in our jurisprudence, and, as we view it, the doctrine cannot now be incorporated without doing violence to settled principles of law by which the profession and the public have long been guided.

Id.

93. See Prosser, supra note 84, at 385 (stating that a concurring judge took
the defendants of a photograph of the plaintiff without her consent. The circulation of photographs was one area, though not the only one, which Warren and Brandies considered an area deserving privacy protection. And it was for this one aspect of privacy that the first privacy-related state statute was passed. In 1903, the New York Legislature enacted legislation prohibiting the commercial use of a person's name or picture without that person's permission.

By the mid-twentieth century, though, a majority of states had recognized a common law right to privacy. In 1960, Prosser identified four distinct types of invasion of privacy recognized by the courts: (1) intrusion upon seclusion; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false light in the public eye; and (4) commercial appropriation of a person's name or likeness. In formulating this evolving common

“the unprecedented step” of authorizing an article defending Robertson); The Right of Privacy, supra note 72 (criticizing the Roberson decision). As stated by one of the Roberson justices:

The right of privacy, so called, represents an attractive idea to the moralist and social reformer, but to the lawmaker, who seeks to embody the right in a statute, the subject is surrounded with some serious difficulties. It is quite impossible to define with anything like precision what the right of privacy is or what its limitations are, if any; how or when the right is invaded or infringed, or what remedy can be applied if any.


94. See Warren & Brandeis, supra note 83, at 195-96 (discussing how photographs “have invaded the sacred precincts of private and domestic life”).

95. N.Y. CIV. RIGHTS LAW § 50 (McKinney 2008) (“A person, firm or corporation that uses for advertising purposes, or for the purposes of trade, the name, portrait or picture of any living person without having first obtained the written consent of such person...is guilty of a misdemeanor.”) (held constitutional, Rhodes v. Sperry & Hutchinson Co., 85 N.E. 1097 (N.Y. 1908), aff'd, Sperry & Hutchinson Co. v. Rhodes, 220 U.S. 502 (1911)).

96. See Prosser, supra note 84, at 386-89 (listing the states that had begun to recognize the right of privacy).

97. See id. at 389 (describing the four categories of invasion). These four invasions were later more formally restated:

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.

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.

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
law right to privacy, the courts evidently incorporated the social sentiments which gave rise to the call for recognition of privacy rights, particularly to protect the public from the overzealous press—the outrage,\textsuperscript{98} the scandal,\textsuperscript{99} the "deepseated abhorrence of the invasions of social privacy,"\textsuperscript{100} the need to cure this "moral tuberculosis."\textsuperscript{101} A significant limitation was placed on the first three of these newly recognized invasions of privacy: the intrusion, public disclosure, or false light publicity is actionable only if it would be highly offensive to a reasonable person.\textsuperscript{102}

In addition, the right to privacy only protects that which is private. "It is clear . . . that the thing into which there is prying or intrusion must be, and be entitled to be, private."\textsuperscript{103} "On the

---

\textit{Id.} § 652D.

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.

\textit{Id.} § 652E.

98. \textit{See, e.g., supra} note 71 and accompanying text (describing the outrage provoked by amateur photography); \textit{see also} De May v. Roberts, 9 N.W. 146, 148-49 (Mich. 1881) ("It would be shocking to our sense of right, justice and propriety to doubt even but that for such an act [allowing an unmarried man with no medical training to be present while a woman gave birth] the law would afford an ample remedy."); Melvin v. Reid, 297 P. 91, 93 (Cal. 1931) (describing a former prostitute and murder defendant who had abandoned her "life of shame," married, and led a life "as a respected and honored member of society" which was unaware of her past and was facing the publication of these facts; the publication "... of the unsavory incidents in the past life of [the woman] after she had reformed, coupled with her true name, was not justified by any standard of morals or ethics known to . . . " the court).

99. \textit{See, e.g., MOTT supra} note 65 (detailing the role that "gossip and scandal stories" played in the invasion of privacy).

100. \textit{See supra} note 86 (noting Warren's disgust of intrusions upon privacy).

101. \textit{See supra} note 87 (explaining the need for a remedy to respond to the proliferation of scandal and gossip).

102. \textit{See RESTATEMENT (SECOND) OF TORTS, §§ 652B, 652D, and 652E} (imposing liability for those types of privacy invasions only if a reasonable person would find the action highly offensive). In reviewing the cases under which intrusion of seclusion developed, Prosser stated "[i]t is . . . clear that the intrusion must be something which would be offensive or objectionable to a reasonable . . . " person. Prosser, \textit{supra} note 84, at 390-91. The prohibition of public disclosure of private facts "is not intended for the protection of any shrinking soul who is abnormally sensitive about such publicity." \textit{Id.} at 397. "It is quite a different matter when the details of sexual relations are spread before the public gaze, or there is highly personal portrayal of [one's] intimate private characteristics or conduct." \textit{Id.} (footnotes omitted). Similarly, false light publicity does not protect "the hypersensitive individual . . . ." \textit{Id.} at 400.

103. \textit{Id.} at 391. The same is true for the public disclosure of private facts—
public street, or in any other public place, the plaintiff has no right to be alone . . . .”104 Similarly, “no one can complain when publicity is given to information about him which he himself leaves open to the public eye . . . .”105

As noted previously, early privacy protections were associated with physical trespass—such as standing under the eaves of a house to listen to conversations therein106 or peering into windows.107 Recall though that it was the ability to invade privacy by intangible means, such as through instant photographs and recording machines, that drove the early efforts to recognize invasion of privacy as a legally recognized tort.108 Early on, the common law right to privacy adopted to technological innovations which could intrude not just a plaintiff’s physical space:

The invasion may be by physical intrusion into a place in which the plaintiff has secluded himself . . . . It may also be by the use of the defendant’s senses, with or without mechanical aids, to oversee or overhear the plaintiff’s private affairs, as by looking into his upstairs windows with binoculars or tapping his telephone wires.109

By the close of the twentieth century, therefore, common law recognized an individual right to privacy where individuals were protected from highly offensive invasions of privacy—as long as the invasion pertained to truly private matters. But common law is not the only source of privacy protection in the United States. Contemporaneous with the development of common law rights to privacy, the United States Supreme Court was also grappling with the notion of a constitutional right to privacy.

B. The Development of the Constitutional Right to Privacy in the United States

Although the United States Constitution does not contain the word privacy, it is reflected in concepts of individualism (through private religious judgment, private economic motives, and legal rights for individuals), limited government, and private property
The Fourth Amendment is considered a key element in American guarantees of privacy. The Supreme Court has recognized that the rights afforded under the Fourth Amendment are declared to be indispensable to the "full enjoyment of personal security, personal liberty and private property"; that they are to be regarded as of the very essence of constitutional liberty; and that the guaranty of them is as important and as imperative as are the guaranties of the other fundamental rights of the individual citizen.

"The well-known historical purpose of the Fourth Amendment, directed against general warrants and writs of assistance, was to prevent the use of governmental force to search a man's house, his person, his papers, and his effects, and to prevent their seizure against his will." With few exceptions, the Supreme Court's early Fourth Amendment decisions focused on

---

110. See Westin, supra note 35, at 330 (referring to the First, Third, Fourth, and Fifth Amendments); see also Alton I. Taylor & Catherine B. Tackney, Historical Trends of Privacy Rights, 14 NEW DIRECTIONS INSTITUTIONAL RES. 5, 5 (1977) (describing historical Americans' unique personality in religion, politics, and law as a driving force for privacy in the U.S.).

111. 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.

112. See Westin, supra note 35, at 332 (describing privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others").

Near in importance to exemption from any arbitrary control of the person is that maxim of the common law which secures to the citizen immunity in his home against the prying eyes of the government. The maxim that "every man's house is his castle", is made a part of our constitutional law in the clauses prohibiting unreasonable searches and seizures, and has always been looked upon as of high value to the citizen.


113. Gouled v. United States, 255 U.S. 298, 304 (1921) (referring to both the Fourth and Fifth Amendments). The Supreme Court has noted the close relationship between the Fourth and Fifth Amendments:

We have already noticed the intimate relation between the two amendments. They throw great light on each other. For the "unreasonable searches and seizures" condemned in the Fourth Amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the Fifth Amendment.


the requirements of particularity in warrants supporting searches, or the interrelationship between the Fourth and Fifth Amendments. By the end of the nineteenth century, the Supreme Court had decided only two cases which dealt with the scope of Fourth Amendment searches and seizures. In 1877, in *Ex parte Jackson*, the Supreme Court held that sealed letters in the mail could not be intercepted, opened, and read without a warrant. Nearly a decade later, the Supreme Court ruled that an individual's private papers are subject to the Fourth Amendment's warrant requirements.

Until the mid-twentieth century, the Supreme Court's application of the Fourth Amendment was based on a "trespass doctrine." Application of the Fourth Amendment focused on physical entries of the home, or the seizure of physical papers and books. But as communications evolved into intangible media, the Supreme Court was slow to adapt. For example, in *Olmstead v. United States*, the Court considered whether evidence obtained through surreptitious telephone wiretaps violated the Fourth Amendment. The *Olmstead* Court made a point of noting that the information used against the defendants was

115. The earliest published opinion by the Supreme Court involving the Fourth Amendment was a *habeas corpus* case in which the Court held the evidence supporting a Fourth Amendment search and seizure did not constitute probable cause. *See Ex parte Bollman*, 8 U.S. 75, 110 (1807) ("It is not necessary indeed that there should be positive proof of every fact constituting the offence; but nothing can be taken into the estimate, when forming an opinion of the probability that the fact was committed by the person charged, but facts supported by oath or affirmation.").

116. *See, e.g.*, *Boyd*, 116 U.S. at 634-35 (holding that compelling a person to be a witness against himself, within the meaning of the Fifth Amendment, is the equivalent of an unreasonable search and seizure within the Fourth Amendment), *overruled by* Interstate Commerce Comm'n v. Baird, 194 U.S. 25, 45-46 (1904).

117. 96 U.S. 727, 733 (1877) ("The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant.").

118. *Boyd*, 116 U.S. at 622 ("a compulsory production of a man's private papers to establish a criminal charge against him, or to forfeit his property, is within the scope of the Fourth Amendment to the Constitution").


120. *See, e.g.*, *Weeks* 232 U.S. at 390 (stating that a fundamental principal underlying the Fourth Amendment is "that a man's house [is] his castle and not to be invaded by any general authority to search and seize his goods and papers.").

121. *See, e.g.*, *Ex parte Jackson*, 96 U.S. 727, 733 (1877) (holding sealed papers in the mail cannot be examined without a warrant); *Boyd*, 116 U.S. at 622 (holding same as to private papers in a person's home).

122. 277 U.S. 438.
obtained through "[s]mall wires ... inserted along the ordinary telephone wires from the residences ..." and chief office of the defendants—"without trespass upon any property of the defendants."

The Olmstead Court noted the Fourth Amendment requires that "the search is to be of material things—the person, the house, his papers or his effects[,]" and it did not believe that "testimony only of voluntary conversations secretly overheard" fit within the Amendment.

In his dissent, Brandeis echoed a theme from his earlier article, *The Right to Privacy*, that legal protections should adopt to a changing world. Brandeis was concerned that wiretapping was merely the first step in the "progress of science in furnishing the Government with means of espionage . . . ." Perhaps foreseeing our modern, interconnected society of computers and the Internet, Brandeis warned: "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."

Despite Justice Brandeis' concerns, the Supreme Court maintained the trespass doctrine through the mid-twentieth century, incorporating the notion that voluntary conversations could be surreptitiously recorded as long as there was no physical trespass. But in 1967, the Supreme Court reversed itself,
expanding not only Fourth Amendment protection, but also fundamentally changing the scope of privacy protection in the United States.

In *Katz v. United States*, the Supreme Court not only abandoned the trespass doctrine, holding that "the Fourth Amendment protects people, not places[,]" but also reformulated the extent of privacy protection in the United States. In *Katz*, the Supreme Court adopted the position, at least as far as Fourth Amendment searches were concerned, that it is what a person seeks to keep private that may be constitutionally protected. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."

Justice Harlan restated this approach to privacy: first, a person must have an actual, subjective expectation of privacy; and second, that expectation must be one that society is prepared to accept as reasonable. Justice Harlan provided a few examples of how this "expectation of privacy" could be applied:

Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.

---

130. 389 U.S. 347, 359 (1967) (holding that conversations recorded, without a warrant, from a phone booth constituted an unreasonable search and seizure in violation of the Fourth Amendment).
131. *Id.* at 351.
132. *Id.* at 351-52 (citations omitted).
133. See *Id.* at 361 (Harlan, J., concurring).
134. *Id.* (citation omitted).
Justices Stewart (in the majority opinion) and Harlan were merely expressing what had previously been implied: only that which is private is entitled to protection. The expectation of privacy is based on what society considers reasonable. In theory, the rationale for this limitation is to address the problem of idiosyncratic individual preferences leading to an unusually strong desire for privacy, resulting in impossible demands for privacy. In practice, however, as discussed more fully below, a reasonable expectation of privacy can be difficult to establish, particularly in the modern workplace.

Prior to Katz, courts and commentators rarely used the phrase "expectation of privacy." Since Katz was decided, essentially every common law and constitutional right to privacy evaluation has centered on the expectation of privacy. The advantage of this approach is its flexibility; but that is also its major downfall, as there can never be a definitive test to determine what is and is not private. "We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable." Justice Scalia has referred

135. See supra notes 103-105 and accompanying text.
137. SOLOVE, supra note 27, at 71.
138. See Hammonds v. Aetna Cas. & Sur. Co., 243 F. Supp. 793, 795 n.1 (N.D. Ohio 1965) (referencing English common law that a medical patient has no expectation of privacy); United States v. Blank, 251 F. Supp. 166, 173 (N.D. Ohio 1966) (rejecting the government's claim that a tenant has no expectation of privacy in the hallways and stairways of the apartment building in which the tenant lives); Recent Cases, 104 U. Pa. L. Rev. 703, 718 (1956) (contrasting privacy rights between telephone users and radio operators; "the telephone user can ordinarily speak freely in reliance on the privacy of his medium, while a radio operator has no reasonable expectation of privacy . . . ." because any other operator attuned to the same frequency can receive a radio message); James A. Gardner, A Re-Evaluation of the Attorney-Client Privilege (Part II), 8 Vill. L. Rev. 447, 508 (1963) (discussing the expectation of privacy arising from the attorney-client privilege); California Damages Reform, Part III: Enforcement Techniques, 13 UCLA L. Rev. 686, 710-11, 713 (1966) (discussing expectations of privacy in public restrooms).
139. See, e.g., Couch v. United States, 409 U.S. 322, 336 (1973) (holding that "no Fourth Amendment claim can prevail where there exists no legitimate expectation of privacy."); Samson v. Calif., 547 U.S. 843, 850 (2006) (holding parolees have fewer expectations of privacy than probationers; exemplifying how the concept "expectation of privacy" has become an assumed element of Fourth Amendment analysis); Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 648 (Cal. 1994) ("the plaintiff in an invasion of privacy case must have conducted himself or herself in a manner consistent with an actual expectation of privacy"); Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 877 (8th Cir. 2000) ("A legitimate expectation of privacy is the touchstone of the tort of intrusion upon seclusion.").
140. See SOLOVE, supra note 27, at 72 (discussing the expectation approach).
141. O'Connor v. Ortega, 480 U.S. 709, 715 (1987). "[T]here is no natural line of separation between the realm of the private and personal matters of
to it as a “self-indulgent test” in which subjective expectations of privacy that society is prepared to recognize as reasonable “bear an uncanny resemblance to those expectations of privacy that [the Supreme] Court considers reasonable.”

Courts have carved out two delineations. First, there is a greater expectation of privacy in the home. Second, there the sender of messages has a greater expectation of privacy in the contents of the messages than the recipient. While sealed letters and packages in the mail are protected against warrantless searches, there is no protection for what is written on the outside of an envelope—e.g., an address. Similarly, while the contents of a telephone conversation may be constitutionally protected, phone numbers dialed are not. And in United States v. Forrester, the Ninth Circuit Court of Appeals held that “e-mail... users have no expectation of privacy in the to/from addresses of their messages . . . .” The reason phone numbers dialed and addresses, e-mail or postal, are not protected is because they are knowingly exposed to the public.

Congress has also enacted legislation to protect privacy.

legitimate interest to others.” James B. Rule, PRIVACY IN PERIL 2 (2007) (emphasis in original removed).

143. See, e.g., Weeks, 232 U.S. at 390 (recognizing the maxim that “every man’s house is his castle” is made a part of constitutional law in the clause prohibiting unreasonable searches and seizures) (internal quotation marks and citation omitted).
144. See Ex parte Jackson, 96 U.S. at 733 (discussing the privacy protection given to sealed letters and packages).
145. See United States v. Hernandez, 313 F.3d 1206, 1209-10 (9th Cir. 2002) (explaining that the outside of a letter, including the address, is not entitled to privacy protection).
146. See Smith v. Md., 442 U.S. 175, 174 (1979) (distinguishing the telephone number dialed from the contents of the call in relation to privacy).
147. 512 F.3d 500, 510 (9th Cir. 2008).
148. See Smith, 442 U.S. at 743 (holding phone customers have no legitimate expectation of privacy in the phone numbers they dial because that information is transmitted to the phone company, which uses and records that information for a number of legitimate business purposes); Forrester, 512 F.3d at 510 (holding e-mail and Internet users “have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information”).
The majority of the federal privacy-related laws focus on consumer protection and protection from government intrusion. Only a few have direct application to the workplace. And federal legislation specifically aimed at monitoring electronic communications may provide little, if any, employee privacy protection.

C. Protecting Privacy Through the Electronic Communications Privacy Act

Almost as soon as recording devices were introduced they were used to surreptitiously record conversations. Within twenty years after the first sound recording devices were introduced, one was used by a postal inspector to surreptitiously record a conversation with a person suspected of illegal use of the mail. In 1907, the Dictograph Co. marketed a device expressly for

---


152. Smith, supra note 29, at 156.
monitoring conversations. In 1912, *Scientific American* reported how the "famous Detective Burns and his associates" used an inconspicuously placed transmitter to record conversations of a "dynamiter" plot. Although the common law quickly viewed electronic eavesdropping as a potential invasion of privacy, its intangible nature kept it outside the scope of the Supreme Court's Fourth Amendment's trespass doctrine.

Congress attempted to regulate wiretapping through the Federal Communications Act of 1934. But this only applied to wire (or radio) communications and therefore did not prevent all electronic eavesdropping. For example, in *Goldman v. United States*, two federal agents placed a "detectaphone" against a partition wall, allowing the agents to hear the defendant's portion of a telephone conversation in the adjoining room. The Supreme Court concluded that "[w]ords spoken in a room in the presence of another into a telephone receiver do not constitute a communication by wire within the meaning of . . . § 605." Until 1968, there was no federal legislation prohibiting oral eavesdropping, and, until *Katz* in late 1967, as long as the eavesdropping was not accompanied by a trespass, or if the communication was recorded with the consent of one of the parties, there was no invasion of privacy.

Congress revisited wiretapping with Title III of the 1968 Omnibus Crime Control and Safe Streets Act (the "Wiretap Act"). In particular, the Act prohibits the interception and

---

153. *Id.*

154. *How Detective Burns Listened to Dynamiter Plots*, 106 SCI. AM. 284 (1912) (the subtitle of the article is, "Instruments That Can be Used for Eavesdropping or for Business Purposes").

155. *See supra* note 109 and accompanying text. *See also* Rhodes v. Graham, 37 S.W.2d 46, 47 (Ky. Ct. App. 1931) (holding "[w]ire tapping is akin to eavesdropping, which was an indictable offense at common law . . ." and stating "[w]henever a telephone line is tapped the privacy of those talking over the line is invaded and conversations, wholly proper and confidential, may be overheard"); McDaniel v. Atlanta Coca-Cola Bottling Co., 2 S.E.2d 810, 816 (Ga. Ct. App. 1939) (holding electronic eavesdropping of plaintiff's hospital room was an invasion of privacy).

156. *See supra* notes 123 & 129 and accompanying text. In *Olmstead*, the Supreme Court ruled that the evidence obtained via the wiretap was still admissible even though the act of wiretapping violated Washington state's wiretapping law. 277 U.S. at 469.


158. 316 U.S. at 131.

159. *Id.* at 133.

160. *See* Berger v. New York, 388 U.S. 41, 127 (1967) (White, J., dissenting) (finding that evidence obtained by eavesdropping is admissible if unaccompanied by trespass or recorded with consent).

The De-Evolution of Privacy for American Employees

disclosure of wire, oral, or electronic communications. The Electronic Communications Privacy Act ("ECPA") of 1986 amended the Wiretap Act, with some direct bearing on workplace monitoring, by protecting "against unwarranted interception or retrieval of electronic communications." Title I of the ECPA restricts the use of wiretaps. On its face Title I would have an impact on an employer's ability to monitor employee telephone calls. But as discussed below, particularly because of a "business use" exception in Title I, the statute provides minimal employee privacy protection. Title II of the ECPA, the Stored Communications Act ("SCA"), makes it illegal to access stored electronic communications without authorization. As discussed below, the SCA potentially affects the ability of employers to monitor employee computer-related communications.

IV. THE LACK OF PRIVACY IN THE MODERN WORKPLACE

Employers do have legitimate reasons to monitor employees and the workplace. "[E]mployers regard control of the workplace as their prerogative, including the right to protect and control their property, and the right to supervise and manage employee performance in terms of productivity, quality, training, and the recording of customer interactions." One significant motivation for monitoring is performance-based, ensuring that employees are performing their work effectively and efficiently, or at all.

166. Because Title I of the ECPA prohibits the interception of electronic communications, it has been interpreted as not applying when an employer accesses stored e-mail messages. See Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 113-14 (3rd Cir. 2004) (providing an analysis of cases which have interpreted same).
167. See infra note 202.
169. See David, supra note 164, at 328 (analyzing the Stored Communications Act).
170. See infra notes 208-209.
Employers also have a legitimate concern that confidential information, such as trade secrets, is not intentionally or inadvertently disclosed through communications systems.\footnote{173}

An additional concern for employers is that employees will create a hostile work environment by openly browsing pornographic Web sites or sending sexually explicit or racially insensitive e-mail messages. In \textit{Faragher v. City of Boca Raton},\footnote{174} and a companion case, \textit{Burlington Industries, Inc. v. Ellerth},\footnote{175} the Supreme Court held that an employer is subject to vicarious liability to a victimized employee for an actionable hostile environment created by a supervisor with immediate (or successively higher) authority over the employee, though when no tangible employment action is taken, a defending employer may raise an affirmative defense (a) that the employer exercised reasonable care to prevent and correct promptly any sexually harassing behavior, and (b) that the plaintiff employee unreasonably failed to take advantage of any preventive or corrective opportunities provided by the employer or to avoid harm otherwise.\footnote{176}

In both \textit{Faragher} and \textit{Burlington Industries}, Justice Thomas argued that absent an adverse employment consequence, an employer should not be held vicariously liable if a supervisor creates a hostile work environment.\footnote{177} Justice Thomas expressed his concern that "[s]exual harassment is simply not something that employers can wholly prevent without taking extraordinary measures—constant video and audio surveillance, for example—that would revolutionize the workplace in a manner incompatible with a free society."\footnote{178} Judge Posner expressed a similar concern

\footnote{173. See Ciocchetti, supra note 172, at 4 (listing preventing disclosure of trade secrets as reason to monitor employees' email); Kesan, supra note 172, at 310 (explaining that employee crimes include disclosure of trade secrets); Anne L. Lehman, \textit{E-Mail in the Workplace: Question of Privacy, Property or Principle?}, 5 COMMLAW CONSPECTUS 99, 110 (1997) (indicating that email creates risk to employers seeking to protect trade secrets).}

\footnote{174. 524 U.S. 775 (1998).}

\footnote{175. 524 U.S. 742 (1998).}

\footnote{176. \textit{Faragher}, 524 U.S. at 777-78; \textit{Burlington}, 524 U.S. at 745.}

\footnote{177. \textit{Faragher}, 524 U.S. at 810 (Thomas, J., dissenting); \textit{Burlington}, 524 U.S. at 767 (Thomas, J., dissenting).}

\footnote{178. \textit{Id.} at 770 (Thomas, J., dissenting) (citation omitted).}
in his dissent to the case's appellate court decision (which was upheld by Burlington Industries): "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? Subjected to periodic lie-detector tests? Trailed on business trips by company spies?"179 Rosen argues that the Supreme Court's rulings on hostile work environments provide a "strong incentive [for employers] to monitor and punish far more private speech and conduct than the law actually forbids."180

Analyzing rights to privacy in the modern workplace involves a number of dynamics. Employee rights to privacy are subservient to an employer property-rights regime,181 protecting the employer's physical and intellectual property, as well as protecting the employer from potential liability.182 Which aspect of work is monitored or searched can determine whether common, constitutional, or federal statutory law is applied. Regardless, though, the determination of an employee's right to privacy in any given situation begins with the employee's expectation of privacy.

182. See Marfkoff, supra note 2, at 2 (quoting Scott McNealy, Chairman and former CEO of Sun Microsystems discussing the technological evolution of monitoring devices:

If there were no audit trails and no fingerprints, there would be a lot more crime in this world. Audit trails deter lots of criminal activity. So all I'm suggesting, given that we all have ID cards anyhow, is to use the biometric and other forms of authentication that are way more powerful and way more accurate than the garbage we use today.);

see generally Doe v. XYC Corp., 887 A.2d 1156 (N.J. Super. Ct. App. Div. 2005), (representing one of the more extreme cases of potential employer liability). In Doe, the employer became aware that an employee was visiting pornographic websites while at work, for which the employee was admonished and instructed to stop. Id. at 1159-60. The Court found that the employer could have implemented monitoring software that would have revealed the exact nature of the employee's workplace web browsing, and that the employer failed to investigate the extent of the employee's "improper" Internet access while at work, Id. at 1164, the Superior Court reversed the lower court's granting of the employer's motion for summary judgment dismissing claims of negligence brought by the employee's wife against the employer resulting from the employee uploading onto the Internet nude photographs of the wife's daughter using his workplace computer. Id. at 1169-70.
A. General Workplace Rights to Privacy

The Fourth Amendment right to privacy applies directly only to public-sector employees.\textsuperscript{183} In the private sector, an employee is most likely to raise an intrusion upon seclusion claim.\textsuperscript{184} Both the constitutional and common law rights to privacy require an underlying expectation of privacy; so, in this regard, the analysis is the same in both the public and private employment scenario. Step one, therefore, is to determine whether the employee, public or private, has a reasonable expectation of privacy. If not, there is no potential wrongdoing by the employer. Whether an employee has a reasonable expectation of privacy must be decided on a case-by-case basis.\textsuperscript{185}

The analysis in \textit{Katz v. United States} controls. What a person \textit{knowingly exposes} to the public is not protected; what a person \textit{seeks to preserve} as private may be constitutionally protected.\textsuperscript{186} In determining whether there is a reasonable expectation of privacy, courts have emphasized the latter part of this formulation, focusing on what individuals successfully seek to preserve as private, to the point that even the potential for exposure defeats any expectation of privacy—creating an affirmative duty to ensure no possible exposure of that which one seeks to keep private.

For example, in \textit{Vega-Rodriguez v. Puerto Rico Telephone Company}, the First Circuit Court of Appeals held that employees had no expectation of privacy when monitored by video

\begin{enumerate}
\item \textsuperscript{183} \textit{See O'Connor}, 480 U.S. at 715 (plurality opinion) ("Searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment"); \textit{see also} Burdeau v. McDowell 256 U.S. 465, 475 (1921) (finding that the Fourth Amendment applies only to state action).
\item \textsuperscript{184} \textit{See supra} note 97 and accompanying text; Joan T.A. Gabel & Nancy R. Mansfield, \textit{The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace}, 40 AM. BUS. L.J. 301, 313 (2003) (noting that intrusion upon seclusion claims will become more common as workers become increasingly dependent upon technology to perform their jobs); \textit{Solove}, \textit{supra} note 27, at 162-63 (noting that intrusion often involves disclosure of personal information through intrusive information-gathering activities, such as surveillance or interrogation).
\item \textsuperscript{185} \textit{See Rosario v. United States}, 538 F. Supp. 2d 480, 494 (D. P.R. 2008) ("This determination is fact intensive and must be made after careful examination of the circumstances extant in the particular scenario under consideration."); Vega-Rodriguez v. P.R. Tel. Co., 110 F.3d 174, 178 (1st Cir. 1997) (holding that the Supreme Court "has not developed a routinized checklist that is capable of being applied across the board, and each case therefore must be judged according to its own scenario.").
\item \textsuperscript{186} \textit{Katz}, 389 U.S. at 351-52; \textit{see also} \textit{supra} note 132 and accompanying text.
\end{enumerate}
surveillance in open work areas. Further, the court was unimpressed that the monitoring was conducted by an "unremitting" camera that, "unlike the human eye, never blinks." Referencing Katz, the First Circuit stated that "persons cannot reasonably maintain an expectation of privacy in that which they display openly." This reasoning was taken to the extreme in Nelson v. Salem State College, in which a college employee was videotaped by a hidden camera while changing clothes and applying medication in a locked office. The Massachusetts Supreme Judicial Court held the office was public because any number of employees had a key to the office. The court found the employee could not have a reasonable expectation of privacy because there was no guarantee of privacy in her work space during office hours, despite the fact that the employee had locked the door as well as the fact that the hidden camera, set up to thwart after-hours thefts, was recording twenty-four hours per day.

In most workplaces, a reasonable expectation of privacy on the part of employees is controlled by either by the work environment or the employer. Areas set aside for personal activities or items are often given greater protection. For example, in Rosario v. United States, the District Court for the District of Puerto Rico held that employees had an expectation of privacy in regard to video surveillance of a locker-break room. In K-Mart Corp. v. Trotti, because the employer allowed employees to use their own locks to secure personal belongings in employer-provided lockers, an expectation of privacy was created in the contents of

187. 110 F.3d at 184.
188. Id. at 180. See Acosta v. Scott Labor LLC, 377 F. Supp. 2d 647, 650 (N.D. Ill. 2005) (citing Vega-Rodriguez, 110 F.3d at 181) ("It is of no moment whether the observation of openly displayed facts is accomplished by a video camera or the naked eye.").
189. Vega-Rodriguez, 110 F.3d at 181; see Doe 887 A.2d at 1166, (holding that employee had no expectation of privacy that would prevent his employer from accessing his computer to determine if he was using it to view adult or child pornography where employee's office did not have a door and his computer screen was visible from the hallway, unless he took affirmative action to block it, and employer had a policy prohibiting the use of the Internet for improper purposes).
191. Id. at 346.
192. See id. at 347 ("[E]ven if the plaintiff thought she was alone, there was no absolute guarantee, including when she locked the door to apply her medication or change her clothes for the evening.").
193. See id.
194. 538 F. Supp. 2d 480, 497 (D.P.R. 2008) ("The purpose of the room was inherently private. It was designated for a particular category of employees to safeguard their personal belongings and working instruments as well as to eat snacks.").
the lockers. In *Dorris v. Absher*, the Sixth Circuit Court of Appeals analyzed whether four employees who worked in an open work area had a reasonable expectation of privacy regarding their conversations which were critical of their supervisor, and which were secretly recorded by the supervisor. First, the court concluded the employees had a subjective expectation of privacy—"After all, no reasonable employee would harshly criticize the boss if the employee thought that the boss was listening." Second, the court concluded the employees' expectation of privacy was objectively reasonable because, despite the open work space, the employees "took great care to ensure that their conversations remained private." Finally, an employee can have a reasonable expectation in an office, desk, or file cabinet to which the employee is granted exclusive access. But when it comes to the use of modern workplace tools, such as computers, e-mail, the Internet, or the phones, employee expectations of privacy are minimally protected, at best.

**B. Employee Expectations of Privacy Related to Telephone Use**

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

---

195. 677 S.W.2d 632, 637 (Tex. App. 1984) ("Where...the employee purchases and uses his own lock on the lockers, with the employer's knowledge, the fact finder is justified in concluding that the employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference.").
196. 179 F.3d 420, 423-25 (6th Cir. 1999).
197. *Id.* at 425.
198. *Id.*
201. 18 U.S.C. § 2511(2)(c); see also United States v. Corona-Chavez, 328 F.3d 974, 978 (8th Cir. 2003) (holding that no violation of Title I occurs where a party to the communication consents to its interception). One court has held that the burden of showing consent should be on the party seeking the benefit of the exception—e.g., an employer. *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 19 (1st Cir. 2003).
ordinary course of business.\footnote{202}

Courts have held that employees have an expectation of privacy in personal telephone calls where the employer has made provisions for (or expressly allowed) such calls. But the extent of this zone of privacy is not absolute—the employer can still listen to the conversation, at least until it ascertains the conversation is personal and not work-related. For example, in \textit{Watkins v. L.M. Berry Co.}, a pre-ECPA case, sales employees were informed that their phone calls would be monitored to improve sales techniques.\footnote{203} However, the employer also allowed employees to use the same phones for personal calls, assuring employees their personal calls would not be monitored beyond the extent necessary to determine whether they were of a personal or business nature. The employer was found guilty of violating \textsection{605} of the Federal Communications Act of 1934\footnote{204} when its supervisor listened to a phone call an employee was having with her friend during lunch in which the friend inquired about the employee’s employment interview with a different company.\footnote{205} The employer argued that all employees had consented to having their calls monitored. The court noted though that the consent had been limited—it did not have to be “all or nothing.”\footnote{206} This same approach applies under the ECPA.\footnote{207}

\section*{C. Employee Expectations of Privacy Related to Computers}

As it has been applied in most cases, the SCA provides minimal privacy protection for employees. One reason for this result is that the SCA exempts seizures by providers of electronic communications services.\footnote{208} Two courts have interpreted this language to exempt employers who provided the e-mail system from which the messages were retrieved.\footnote{209}

\footnotetext[202]{18 U.S.C. \textsection{2510}(5)(a); \textit{see also} Sanders v. Robert Bosch Corp., 38 F.3d 736, 740-41 (4th Cir. 1994) (describing and analyzing the application of the “business use” exception to the facts of the case).}
\footnotetext[203]{704 F.2d 577, 579 (11th Cir. 1983).}
\footnotetext[204]{47 U.S.C. \textsection{605} (2006).}
\footnotetext[205]{\textit{See Watkins}, 704 F.2d at 583 ([A] personal call may be intercepted in the ordinary course of business to determine its nature but never its contents.)(footnote omitted).}
\footnotetext[206]{\textit{Id.} at 582.}
\footnotetext[207]{\textit{See} Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 923 (W.D. Wis. 2002) (“At the point defendants... determined that the [plaintiff’s] call was personal... they had an obligation to cease listening and hang up.”).}
\footnotetext[208]{18 U.S.C. \textsection{2701}(c)(1) (2006).}
\footnotetext[209]{\textit{See} Fraser, 352 F.3d at 114-15 (3rd Cir. 2004) (applying interpretation to private employer); \textit{see also} Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (applying interpretation to public employer); \textit{See also} Benjamin F. Sidbury, \textit{You’ve Got Mail... and Your Boss Knows It: Rethinking the Scope of the Employer E-mail Monitoring Exceptions to the Electronic}
Almost from the inception of workplace e-mail, employees have been fired for using it for inappropriate purposes.210 One of the earliest cases involving inappropriate e-mail is Bourke v. Nissan Motor Corporation, U.S.A., in which two employees were fired after their e-mail correspondence which contained sexual material was randomly chosen for display during a computer training session.211 Although the plaintiffs claimed they had a subjective expectation of privacy in their e-mail messages because they were given passwords to access the computer system, the court held they had no objective expectation of privacy in e-mail messages that could be read by others.212

Applying common law rights to privacy, courts have yet to find an invasion of employee privacy regarding workplace e-mail communications (where the employer maintains the e-mail system). For example, in Smyth v. Pillsbury Company, the plaintiff-employee was fired for transmitting inappropriate and unprofessional comments over the company's e-mail system, despite the company's assurances that all e-mail communications would remain confidential and privileged, and that they would not be intercepted and used by the company against its employees as grounds for termination.213 The court held that the 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."214 The court found no privacy interests when an employee voluntarily communicates unprofessional comments over a company e-mail system.215

A similar result was reached in the case of McLaren v. Microsoft.216 The employee, McLaren, brought claims of invasion of privacy (specifically, intrusion upon seclusion) based on the employer, Microsoft, accessing e-mail messages McLaren had initially received through the company e-mail system and then stored in a "personal" folder on McLaren's computer, protected by

Communications Privacy Act, 2001 UCLA J. L. & TECH. 5 (2001) ("[I]f an employer provides access to e-mail through a private in-house e-mail server, the employer is free to monitor an employee's stored e-mail.") (no pagination).
210. See, e.g., Janice C. Sipior & Burke T. Ward, The Dark Side of Employee Email, 42 COMM. ACM 88, 89 (July 1999) (reporting the rise during the 1990s in the use of e-mail to sexually harass co-workers).
212. Id.
214. Id. at 98 (applying Pennsylvania law).
215. See id. at 101.
a password known only to McLaren.\textsuperscript{217} The court concluded that "McLaren did not have a reasonable expectation of privacy in the contents of the e-mail messages such that Microsoft was precluded from reviewing the messages."\textsuperscript{218} Attempting to analogize to \textit{K-Mart Corporation v. Trotti},\textsuperscript{219} McLaren argued his situation was similar to one where an employer searches a personal locker—the area where McLaren stored the messages on his computer—secured by the employee's own lock—password-protecting the messages.\textsuperscript{220} The \textit{McLaren} court distinguished the facts from \textit{K-Mart}, noting: first, the locker scenario contained only personal items whereas in the instant case the e-mail messages were not McLaren's personal property because Microsoft supplied the e-mail system; and second, since the e-mail messages were delivered to Microsoft's computers, they were accessible by third parties.\textsuperscript{221}

Employers can also diminish employee expectations of privacy when using the employer's computers by notifying employees of monitoring.\textsuperscript{222} But the nature of the modern workplace may itself destroy any employee expectation of privacy. "Social norms suggest that employees are not entitled to privacy in the use of workplace computers, which belong to their employers and pose significant dangers in terms of diminished productivity and even employer liability."\textsuperscript{223} The Seventh Circuit Court of Appeals has gone so far as to state, "the abuse of access to workplace computers

\begin{itemize}
\item \textsuperscript{217} Id. at *2. McLaren's e-mail messages were reviewed as part of an investigation of improper employment-related conduct by McLaren. Id. at *1-2.
\item \textsuperscript{218} Id. at *4.
\item \textsuperscript{219} Supra note 195 and accompanying text.
\item \textsuperscript{220} McLaren, 1999 Tex. App. LEXIS 4103, at *11.
\item \textsuperscript{221} Id. at *11-12.
\item \textsuperscript{222} See, e.g., TBG Ins. Servs. Corp. v. Super. Ct., 117 Cal. Rptr. 2d 155, 162 (Cal. Ct. App. 2002) (holding "employers can diminish an individual employee's expectation of privacy by clearly stating in the policy that electronic communications are to be used solely for company business, and that the company reserves the right to monitor or access all employee Internet or e-mail usage"); United States v. Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002) (holding professor did not have a reasonable expectation of privacy regarding data downloaded from the Internet onto his university-provided office computer, in part, because: University computer-use policy reserved the right to randomly audit Internet use and to monitor specific individuals suspected of misusing University computers; policy explicitly cautioned computer users that information flowing through the University network was not confidential either in transit or in storage on a University computer; and University computer users should have been aware network administrators and others were free to view data downloaded from the Internet); Thygeson v. U.S. Bancorp, No. CV-03-467-ST, 2004 U.S. Dist. LEXIS 18863, at *72 (D. Or. Sept. 15, 2004) ("[W]hen . . . an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy.").
\item \textsuperscript{223} Ziegler, 456 F.3d at 1145-46, cert. denied, 128 S. Ct. 879 (2008).
\end{itemize}
is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible." As Mayer predicted, employee expectations of privacy are yielding to surveillance technologies that become generally available.

This technologically-fluid approach to expectation of privacy tracks exactly with the Supreme Court's approach. In *Kyllo v. United States*, the Supreme Court ruled that the use of thermal imaging technology to measure the heat emanating from a suspect's home, and to therefore ascertain whether the suspect was growing marijuana, was a Fourth Amendment search requiring a warrant. But the Court limited its holding, based on the fact that the technology used was not in general public use.

---

224. Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002) (holding employer's announcement that it could inspect computer laptops it furnished for use by its employees destroyed any reasonable expectation of privacy associated with the use of the laptops); see Doe v. XYC Corp., 887 A.2d 1156, 1166 (N.J. Super. Ct. App. Div. 2005) (employer's policy prohibiting the use of office e-mail or Internet access for improper purposes, with no evidence that employee was not aware of this policy, sufficient to eliminate any expectation of privacy as to employer accessing his computer to determine if he was using it to view adult or child pornography). However, there is a line of cases indicating that the employer must institute a policy of active monitoring and auditing to eliminate any expectation of privacy. See, Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (holding that employee had expectation of privacy regarding personal information kept on his public employer-provided computer since the employee was the only one who used the particular computer and the employer's anti-theft policy did not prevent the employee from storing personal files on his office computer; "infrequent and selective search for maintenance purposes or to retrieve a needed document, justified by reference to the 'special needs' of employers to pursue legitimate work-related objectives, does not destroy any underlying expectation of privacy that an employee could otherwise possess in the contents of an office computer."); United States v. Heckencamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding student did not lose his reasonable expectation of privacy in information stored on his computer where university's monitoring policy established limited instances in which university administrators may access a student's computer in order to protect the university's systems); Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 906 (9th Cir. 2008) rehearing, en banc, denied, 2009 U.S. App. LEXIS 2259 (9th Cir. Jan. 27, 2009) (holding employee had a reasonable expectation of privacy in text messages sent over employer-provided service where employer's informal policy was to not audit messages unless employees exceeded usage limits and refused to pay overage charges).


226. 533 U.S. at 34 ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search ... ") (citation and internal quotation marks omitted).

227. *Id.* In his majority opinion, Justice Scalia defended this rationale based
The problem with the Court's limitation, as Justice Stevens noted, is that its protection dissipates as technology develops and enters general public use.\textsuperscript{228} As a result, "the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."\textsuperscript{229}

**D. Employee Expectations of Privacy Beyond the Workplace**

Employees could be forgiven if they believe their employer could not take adverse employment actions against them based on personal phone calls occurring in their home. In *Karch v. Baybank FSB*, neighbors overheard a telephone conversation on their radio scanner between Karch and her friend, a co-worker, that took place on a Saturday evening, during non-work hours, involving mostly personal matters; however, some work-related comments were overheard.\textsuperscript{230} The neighbors turned over a recording of the conversation to Karch's employer, Baybank FSB, and Karch was reprimanded based on the contents of the recorded conversation.\textsuperscript{231} Karch ultimately resigned and brought a claim against her employer for invasions of seclusion.\textsuperscript{232} The New Hampshire Supreme Court upheld the lower court's dismissal of Karch's claim, ruling that it was the neighbors who had potentially intruded upon Karch's seclusion, not the Bank which had received the information and then acted upon it.\textsuperscript{233}

Employers have also been found to have not invaded employee privacy when they inquire into off-duty conduct among co-workers. For example, in *French v. United Parcel Service, Inc.*, the court ruled the employer had not violated an employee's privacy by questioning the employee about a co-worker's excessive drinking in the employee's home.\textsuperscript{234} The court held "there are circumstances in which it is legitimate for an employer to know some 'personal' information about its employees, so long as the information reasonably bears upon the employees' fitness for, or discharge of, their employment responsibilities."\textsuperscript{235} The court concluded that the employer had "articulated legitimate business

---

\textsuperscript{228} *California v. Ciraolo*, 476 U.S. 207, 215 (1986), which held that "[I]n an age where private and commercial flight in the public airways is routine, it is unreasonable...to expect that...marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet." (emphasis added). *Ciraolo* was not a factor, according to Scalia, because the use of thermal imaging is not "routine." *Kyllo*, 533 U.S. at 39 n.6.

\textsuperscript{229} *Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).

\textsuperscript{229} *Id.*

\textsuperscript{230} 794 A.2d 763, 768 (N.H. 2002).

\textsuperscript{231} *Id.* at 769.

\textsuperscript{232} *Id.*

\textsuperscript{233} *Id.* at 773.


\textsuperscript{235} *Id.* (citation omitted).
reasons for seeking information about the [drinking] incident, including concerns about the soundness of judgment exercised by its supervisory employees in regard to alcohol abuse generally as well as in a particular setting where all participants were . . . employees.236

These cases exemplify how off-duty conduct by employees may still be subject to some form of monitoring by their employers. State legislatures have addressed the notion that employees' off-site, off-hours conduct should be free from employer scrutiny. Most of this legislation, however, protects only employees' off-site consumption of lawful products, particularly tobacco, during nonworking hours.237

A few of these "off-duty conduct" statutes, those in California, Colorado, Connecticut, New York, and North Dakota, go beyond just lawful consumable products and protect off-duty conduct in general. However, although these statutes contain broad language,238 they have been interpreted in only a few limited circumstances.239 For the most part, as long as the employer can

236. Id.
237. See 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, 640-70 (2004) (discussing and analyzing these "off-duty" statutes); see also Jason Bosch, None of Your Business (Interest): The Argument for Protecting All Employee Behavior With No Business Impact, 76 S. CAL. L. REV. 639, 654-58 (2003) (describing the nature and benefits of "lifestyle protection statutes"); see, e.g., MONT. CODE ANN. § 39-2-313(2) (2007) (providing that an employer "may not discriminate against an individual with respect to compensation, promotion, or the terms, conditions, or privileges of employment because the individual legally uses a lawful product off the employer's premises during nonworking hours."); WYO. STAT. ANN. § 27-9-105(a)(iv) (2008) (prohibiting, in part, employers from requiring "as a condition of employment that any employee or prospective employee use or refrain from using tobacco products outside the course of his employment . . . .").
238. See CAL. LAB. CODE § 96(k) (West 2008) (authorizing the Labor Commissioner to take assignments of ["claims for loss of wages as the result of demotion, suspension, or discharge from employment for lawful conduct occurring during nonworking hours away from the employer's premises"]; COLO. REV. STAT. ANN. § 24-34-402.5(1) (West 2007) (prohibiting an employer from terminating "the employment of any employee due to that employee's engaging in any lawful activity off the premises of the employer during nonworking hours . . . ."); CONN. GEN. STAT. ANN. § 31-51q (West 2008) (protecting employees who exercise state or federal first amendment rights); N.Y. LAB. LAW § 201-d(2)(d) (McKinney 2008) (prohibiting employers from discriminating against employees on the basis of their legal political activities, legal use of consumable products, and legal recreational activities—all off-site, outside of work hours without the use of the employer's equipment or other property); N.D. CENT. CODE § 14-02-4-03 (2008) (prohibiting discrimination by an employer, in part, based on an employee's "participation in lawful activity off the employer's premises during nonworking hours which is not in direct conflict with the essential business-related interests of the employer.").
239. See, e.g., Barbee v. Household Auto. Fin. Corp., 6 Cal. Rptr. 3d 406, 411-
establish some sort of business interest in employees' off-site, off-hour behavior, the employee will not have an actionable claim.

E. The Affirmative Duty to Preserve the Expectation of Privacy

In *Katz v. United States*, the Supreme Court established the maxim, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." This is a corollary to the common law right to privacy restriction of only that which is private can be protected. Courts have, however, taken a very liberal view of when one knowingly exposes otherwise private material to the public.

In *Florida v. Riley*, a plurality of the Supreme Court concluded there was no expectation of privacy in marijuana growing in a greenhouse that could be observed by police flying overhead in a helicopter. In her concurrence, Justice O'Connor noted that the subject of a Fourth Amendment search has the burden of proving that his or her expectation of privacy was a reasonable one. Justice Brennan took issue with the plurality's approach. The point of not protecting that which is knowingly exposed to the public is that there should be no expectation of privacy in that which can be readily observed by, say, a passerby. Under the *Florida v. Riley* plurality's approach, the

---

12 (Cal. Ct. App. 2003) (rejecting an employee's claim that his employer violated his right of privacy when the employer discharged him as a result of his intimate relationship with a co-worker; concluding the employee had no reasonable expectation of privacy as to the relationship because he was on notice of the employer's policy discouraging such relationships and the employer was aware of the relationship); Marsh v. Delta Air Lines, Inc., 952 F. Supp. 1458, 1463 (D. Colo. 1997) (holding employee who published a letter critical of management in the newspaper violated his duty of loyalty to his employer by trying to settle publicly a private dispute with management); Daley v. Aetna Life & Cas. Co., 734 A.2d 112, 112-13 (Conn. 1999) (limiting application of Connecticut's statute to speech relating to matters of public concern, and "internal employment policies are not a matter of public concern."); Hougum v. Valley Mem'l Homes, 574 N.W.2d 812, 820 (N.D. 1998) (applying North Dakota's statute, holding it was a disputed issue of fact whether a chaplain who was discovered engaging in unseemly behavior in a Sears store bathroom was terminated for participating in lawful activity off the employer's premises during nonworking hours). But see Cavanaugh v. Doherty, 675 N.Y.S.2d 143 (N.Y. App. Div. 1998) (holding an employee who was terminated as a result of a discussion during recreational activities—dinner at a restaurant—outside of the workplace in which her political affiliations became an issue, stated a cause of action for a violation of New York's statute).

240. 389 U.S. at 351.

241. See supra notes 103-105 and accompanying text (describing the origins of common law privacy in trespass).


243. Id. at 455 (O'Connor, J., concurring).

244. Id. at 457 (Brennan, J., dissenting).
The expectation of privacy is defeated if a single member of the public could conceivably position herself to see into the area in question without doing anything illegal. It is defeated whatever the difficulty a person would have in so positioning herself, and however infrequently anyone would in fact do so.\(^{245}\)

Ultimately, to avoid knowingly exposing any private matter to anyone, one must take affirmative steps to prevent access to the private material.\(^{246}\) For example, in *U.S. v. Barrows*, the United States Court of Appeals for the Tenth Circuit concluded that an employee who connected his personal computer (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, had no expectation of privacy in any files observed by coworkers.\(^{247}\) The court ruled that while the employee may have had "a subjective expectation of privacy, his failure to take affirmative measures to limit other employees' access makes that expectation unreasonable."\(^{248}\) Similarly, in *Commonwealth of Pennsylvania v. Sodomsky*, the Pennsylvania Superior Court found no privacy interest in computer files when employees of a Circuit City store, while performing routine diagnostic tests to verify whether their installation of a DVD drive in Sodomsky's computer was successful, discovered what appeared to be child pornography video files on Sodomsky's computer and notified police.\(^{249}\) The *Sodomsky* court ruled Sodomsky did not have a reasonable expectation of privacy in his video computer files since he was informed Circuit City employees would test the operability of the installed DVD drive and he took no steps to restrict access to any of his computer's files.\(^{250}\) The *Sodomsky* court's approach reflects that of most courts—individuals must take affirmative steps to prevent disclosure. "If a person is aware of, or freely grants to a third party, potential access to his computer contents, he has knowingly exposed the contents of his computer to the public and has lost any reasonable expectation of privacy in those

\(^{245}\) Id.

\(^{246}\) And even that may not be enough. Recall the employee in *Nelson*, who, despite locking the door, was still not considered to have an expectation of privacy during the workday from being recorded by a hidden camera that, despite being installed to thwart after-hours thefts, was recoding 24-hours per day, because other employees had keys to the office. See supra notes 190-193 and accompanying text (discussing *Nelson*).

\(^{247}\) 481 F.3d 1246, 1249 (10th Cir. 2007).

\(^{248}\) Id. (citations omitted) (emphasis added). "Those who bring personal material into public spaces, making no effort to shield that material from public view, cannot reasonably expect their personal materials to remain private." Id.


\(^{250}\) See id. at 368.
F. Additional Obstacles to Employee Workplace Privacy

Even where an employee has a reasonable expectation of privacy, he has no guarantee the employee's privacy interest won't be invaded by the employer. Under the common law, there is no wrongful invasion unless it is highly offensive. For example, though the Texas Court of Appeals found the employee had an expectation of privacy in *K-Mart Corporation v. Trotti* because the employer allowed the employee to store her personal belongings in an employer-provided locker secured by the employee's own lock, the court left it to a jury to decide whether the employer's search of the employee's personal belongings stored in the locker was a highly offensive invasion of privacy.252

And just as there is no bright-line test to establish an expectation of privacy, there is no definitive answer for what is a highly offensive invasion of privacy. In determining what is highly offensive, a court must "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."253 The complexity of this analysis is demonstrated when, for example, an employer's "intrusive and coercive sexual demands" of an employee is an invasion of privacy,254 whereas, in a different context, an employer's question regarding an employee's sexual preference is not.255 But one court has found a material

---

251. *Id.* at 369 (citations omitted) (emphasis added); see also United States v. King, No. 2:05cr301-A, 2006 U.S. Dist. LEXIS 86370 at 5-7 (N.D. Al. Nov. 28, 2006) (holding that the defendant had no reasonable expectation of privacy in computer files located on a personal computer in a private dorm room after defendant connected computer to Air Base's network, knowing files could be viewed by others on network, even though defendant attempted to hide files with security settings that failed to hide the files). Taken to its logical limits, this could mean that a person who voluntarily appears nude before someone else cannot have a reasonable expectation of privacy as to surreptitious photographs that person has taken simply because the nude person did not take affirmative steps to ensure no photographs were taken. See Brief and Argument for Appellant, *supra* note 28, at 6-12 (discussing the implications of a narrow expectation of privacy).

252. 677 S.W.2d 632, 637 (Tex. App. 1984); see also *supra* note 195 and accompanying text (discussing the invasion of privacy at common law).


255. See Morenz v. Progressive Cas. Ins. Co., No. CV-402230, 2002 Ohio App. LEXIS 2474, at *12 (Ohio Ct. App. May 23, 2002) (finding no invasion of privacy where employer asked employee if he was gay; concluding purpose of question, asked in private, was merely to ascertain employee's job satisfaction
issue of fact as to whether an employer's clandestine investigation into employee behavior, which included intimate details of employees' private lives, was an "objectionable intrusion." Finally, monitoring employees while in the bathroom or a dressing room will probably constitute a highly offensive intrusion.

These examples most likely reflect community norms of what constitutes outrageous behavior. Short of highly personal invasions, the highly offensive requirement emphasizes the importance of the objective context of the alleged invasion, including: (1) the likelihood of serious harm, particularly to the emotional sensibilities of the victim; and (2) the presence or absence of countervailing interests based on competing social norms which may render defendant's conduct inoffensive, e.g., a legitimate public interest in exposing and prosecuting serious crime that might justify publication of otherwise private information or behavior.

In the workplace, the "legitimate public interest" translates to a legitimate business interest. In other words, whether an employer's invasion of privacy is highly offensive depends on whether the employer has a legitimate business interest justifying the intrusion.

For example, in *Smyth v. Pillsbury Company*, the District Court held that even if an employee had a reasonable expectation of comfort living in the south; *see also* Pagnattaro, supra note 237, at 632-33 (discussing same).

256. Johnson v. K Mart Corp., 723 N.E.2d 1192, 1197 (Ill. App. 3d. 2000); *see also*, Pagnattaro, supra note 237, at 633 (suggesting the employer's invasive methods to collect non-business related information substantially contributed to the finding of a material issue of fact as to whether there was an invasion of privacy).


259. Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 648 (Cal. 1994) (footnote omitted); *see also*, Shulman v. Group W Prods., Inc., 955 P.2d 469, 493 (Cal. 1998) (stating that whether a reporter's intrusion was "offensive" depends on the extent to which the intrusion was justified by a legitimate motive; "Information-collecting techniques that may be highly offensive when done for socially unprotected reasons—for purposes of harassment, blackmail or prurient curiosity, for example—may not be offensive to a reasonable person when employed by journalists in pursuit of a socially or politically important story.")


of privacy in e-mail messages, the employer's reading those messages would not be a highly offensive invasion of privacy because:

[(1)] by intercepting such communications, the company is not . . . requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects[; and (2)] . . . the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments.260

In contrast, courts have found invasions of privacy under Title I of the ECPA where employers could not justify with a legitimate business purpose the continuous monitoring of employee telephone calls on a near twenty-four hours per day, seven days per week basis.261

The courts take a similar approach in applying the Fourth Amendment to workplace searches. For example, in Schowengerdt v. General Dynamics Corporation, the Ninth Circuit Court of Appeals stated an employee had "a constitutional right to be free from unnecessary, overbroad, or unregulated employer investigations into his sexual practices, [and therefore] the search of his desk and credenza to find and seize materials relating to such matters would be reasonable only if relevant to his job as a naval engineer."262 A search of a public 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 non-investigatory work-related purpose such as to retrieve a needed file."263

261. See, e.g., Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992) (finding no express or implied consent to tapping); Sanders v. Robert Bosch Corp., 38 F.3d 736, 741-42 (4th Cir. 1994) (finding that recordings violated the Federal Wiretapping Act).
262. 823 F.2d 1328, 1336 (9th Cir. 1987); see also id. at n.9 (citing cases upholding a "work-relatedness" requirement for reasonable workplace searches).
263. O'Connor, 480 U.S. at 726 (internal quotation marks omitted). See also Engquist v. Oregon Dept. Agric., 128 S. Ct. 2146, 2151 (2008) (holding that the Court has "often recognized that government has significantly greater leeway in its dealings with citizen employees than it does when it brings its sovereign power to bear on citizens at large"); United States v. Knights, 534 U.S. 112, 118-19 (2001) ("The touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined by assessing . . . the degree to which it intrudes upon an individual's privacy [versus] the degree to which it is needed for the promotion of legitimate governmental interests.") (citation and internal quotation marks omitted).
Further, an important theme running throughout the "lawful product" and "off-duty conduct" statutes\(^{264}\) is that the products or activities must be completely divorced from the employer—they must take place (or be consumed) off-site, during non-working hours, and have no relationship to the employer's interests. In other words, the statutes do not apply if a legitimate business interest of the employer is involved. Therefore, as long as the employer can establish a legitimate business interest in offsite monitoring, it will defeat any claim of invasion of privacy.

Finally, even when an employee may have an expectation of privacy in the contents of his computer, the employer may still consent to its search by law enforcement officials. For example, in *United States v. Ziegler*, the Ninth Circuit Court of Appeals concluded that an employee did have a reasonable expectation of privacy in his locked office that he did not share.\(^{265}\) However, the court concluded the employee’s privacy was not invaded, for Fourth Amendment purposes, when the employer consented to the search of the employee’s computer by government agents, “because the computer is the type of workplace property that remains within the control of the employer ‘even if the employee has placed personal items in [it].’”\(^{266}\)

V. THE FINAL DE-EVOLUTION OF EMPLOYEE PRIVACY

Expectations of privacy are established by social norms.\(^{267}\) At least one court has determined that "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."\(^{268}\) In the modern work environment, particularly when employees spend long hours at work or continue their work at home, this approach creates a conflict between personal and work-related norms.\(^{269}\) Regardless

---

264. See supra notes 237-239 and accompanying text.
265. 474 F.3d 1184, 1189-90 (9th Cir. 2007).
266. See id. at 1191 (quoting O'Connor, 480 U.S. at 716).
269. Findlay & McKinlay, supra note 171, at 307 (stating Developments in the nature of work and organization are... blurring the boundary between work and home, between public and private. It is becoming more difficult to distinguish clear and unambiguous boundaries between work and private life as people work longer hours, work from home on computers owned by their employer, and work on call.);
see also ROSEN, supra note 180, at 84 ("The Internet has blurred the distinction between the home and the office, as Americans are spending more time at the office and are using company-owned computers and Internet servers to do their work from home."); Carol Hymowitz, *Personal Boundaries*
The De-Evolution of Privacy for American Employees

of its "location," it is arguable personal information should receive greater protection. Yet, at least one other court also agrees there should be diminished expectations when employees use an employer's computers: "Social norms suggest that employees are not entitled to privacy in the use of workplace computers, which belong to their employers and pose significant dangers in terms of diminished productivity and even employer liability." Fundamentally, this means employers' property interests trump employees' personal embarrassments and indignities.

This priority between conflicting interests traces back to determinations of expectation of privacy and the offensiveness or unreasonableness associated with its invasion. First, because employers regularly monitor the workplace, and, in particular, computer usage, employees must assume they have no reasonable expectation of privacy. The issue is not whether they should have any privacy—the approach by the courts is that because an employer can monitor, there is no privacy.

Yes, employers have property interests and potential liabilities at stake. But, with few exceptions, those interests trump entirely any potential employee right to privacy in the workplace. It does not help that a leading jurisdiction in employment-related privacy issues, California, has provided conflicting guidance. On the one hand, it is California courts, or

Shrink as Companies Punish Bad Behavior, WALL ST. J., June 18, 2007, at B1 (noting that one reason companies are taking more interest in their workers' personal behavior is because of "the increasingly blurred line between work and home"); Rachel Konrad, IBM Rules Govern Workers in Virtual Worlds, AP, MSNBC, July 26, 2007, available at http://www.msnbc.msn.com/id/19982107/ (discussing reaction to IBM instituting rules for its employees who use Second Life, an online virtual community; although the employees use Second Life for business purposes, concern was expressed that since Second Life users have multiple personas (avatars), there is the propensity for confusion between personal and professional use); Rob Pegoraro, Friend? Not? It's One or the Other, WASH. POST, July 19, 2007, at D1 (discussing the rise in the use by companies of social networking sites, resulting in workers having difficulty differentiating between their private and professional personas on such sites).

270. See, e.g., Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 654 (Cal. 1994) ("A particular class of information is private when well-established social norms recognize the need to maximize individual control over its dissemination and use to prevent unjustified embarrassment or indignity."); see also Brenner, supra note 29, at 83 (noting that: "[t]he physical and informational barriers we once used to differentiate between our "private" and "public" selves are being eroded by technology, and the erosion is accelerating. If we persist in utilizing a zero-sum, spatial conception of privacy to implement the Fourth Amendment, we will render it ineffective as a guarantor of privacy in the face of arbitrary government action.").

271. Ziegler, 456 F. 3d at 1146.

272. See Muick, 280 F3d at 743 (finding no reasonable expectation of privacy when an employee uses his or her workplace computer for personal purposes); supra note 224 and accompanying text.

273. See supra notes 171-180 and accompanying text.
courts applying California law, that have argued the social norm of highly diminished expectations of privacy in the workplace.\textsuperscript{274} Yet, courts in that jurisdiction have also preserved some expectation of privacy in cases where the employer has not expressly stated a policy of active monitoring and auditing.\textsuperscript{275} In other words, some cases hold it should be assumed there is no expectation of privacy because the modern workplace is usually monitored and audited, yet other cases hold that there still may be some expectation of privacy if the employer has not expressly stated monitoring and auditing is occurring.

Further, even when an employee has a reasonable expectation of privacy, it is protected against only an offensive invasion, or, in constitutional parlance, an unreasonable search. What both these standards truly apply to is whether the employer has a legitimate business interest underlying the search or monitoring. This has implications when the employee is working from home. With the merger of office and home life,\textsuperscript{276} employers can more easily argue for a business need in monitoring employee conduct offsite. A growing number of employees now work in a virtual workplace—not in the office, but on the road or at home.\textsuperscript{277} Since there is less face-to-face interaction among workers, there is a greater reliance on electronic communications.\textsuperscript{278}

Technological trends are promising increased employer monitoring. GPS technology allows employers "to watch everybody all the time and scrutinize every movement."\textsuperscript{279} Many

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{275} See U.S. v. Heckencamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding that a student didn't lose his reasonable expectation of privacy in information stored on his computer where University's monitoring policy established limited instances in which University administrators may access a student's computer in order to protect the University's systems); Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 905-06 (9th Cir. 2008), rehearing, en banc, denied, 2009 U.S. App. LEXIS 2259 (9th Cir. Jan. 27, 2009) (holding employee had a reasonable expectation of privacy in text messages sent over employer provided service where employer's informal policy was not to audit messages unless employees exceeded usage limits and refused to pay overage charges).
\item \textsuperscript{276} See supra note 269 (listing authorities that discuss the blurred line between the home and office).
\item \textsuperscript{277} See Michelle A. Travis, Equality in the Virtual Workplace, 24 BERKELEY J. EMP. & LAB. L. 283, 291 (2003) (noting that by the end of the twentieth century, nearly 10\% of the U.S. workforce were telecommuters); Gabel & Mansfield, supra note 184, at 302 (estimating that the number of people working from home would rise to 40 million by 2004).
\item \textsuperscript{278} Wayne F. Cascio, Managing a Virtual Workplace, 14 ACAD. MGMT. EXECUTIVE 81 (2000).
\end{itemize}
\end{footnotesize}
cell phones are GPS-enabled, allowing employers to track the whereabouts of the phones they provide to employees, as well as the employees carrying those phones.\textsuperscript{280} The same can be said for company-provided cars that include a GPS tracking device.\textsuperscript{281} And, as noted above, employers may soon hope to use RFID chips to constantly monitor the whereabouts of their employees, whether at home or in the office.\textsuperscript{282}

The historical prejudice of protecting privacy in the home\textsuperscript{283} provides little comfort when employers can invade that privacy by arguing a legitimate business interest. As these off-site monitoring capabilities become more routine, the consequent social norm will presume no expectation of privacy. With the exception, perhaps, of intrusions into highly personal affairs of employees, such as their sex lives, with no underlying business rationale, employees' lives—on-and off-site—will be an open book to employers.

\textbf{A. Specific Recommendations to Better Protect Employee Privacy}

There are specific approaches to privacy that can be taken to strengthen rights to privacy for employees. First, because of the comingling of home life and work, courts should maintain the historical prejudice of protecting the sanctity of the home.\textsuperscript{284} As such, any monitoring of employees which involves home, family, and/or personal life should be justified only with a substantial, as opposed to reasonable, business need by the employer. Further, it should be the employer's burden to establish what constitutes a substantial business need.\textsuperscript{285}

Second, expectations of privacy should be strengthened. Contrary to the sentiment expressed by the Supreme Court, it should not be the employee's obligation to establish a reasonable expectation of privacy,\textsuperscript{286} but the employer's obligation to establish

\textsuperscript{280} Id. at 173.
\textsuperscript{281} Id.
\textsuperscript{282} See, e.g., Todd Lewan, \textit{Chips: High Tech Aids or Tracking Tools?}, MSNBC.COM, Jul. 23, 2007, http://www.msnbc.msn.com/id/19904543 (discussing two employees of a provider of surveillance equipment injecting RFID tags into themselves to demonstrate "chipping" as a surveillance technique); see supra note 16 and accompanying text (discussing the legality of the use of RFID chips to monitor employees' whereabouts).
\textsuperscript{283} See supra note 33 (listing cases that have upheld the right of privacy in the home).
\textsuperscript{284} See supra notes 44 & 48 and accompanying text (noting the historic recognition of privacy in the home).
\textsuperscript{285} A substantial business need would be a matter critical to the employer's business which supersedes the rights of the employee; cf. Woodworth v. Concord Mgmt. Ltd., 164 F. Supp. 2d 978, 984 (S.D. Ohio 2000) (providing as an example of a critical business need operating a business with a full staff—i.e., necessary for the continued productive operation of the business).
\textsuperscript{286} See supra note 243 and accompanying text (referring to a concurring
that it does not exist in a particular situation. This also includes a return to the original notion of what cannot be considered private—what is plainly open for public view; and not defeating the expectation of privacy "if a single member of the public could conceivably position herself to see into the area in question without doing anything illegal[,] . . . whatever the difficulty a person would have in so positioning herself, and however infrequently anyone would in fact do so." Similarly, the courts must abandon their attitude that if there is a potential for disclosure, despite an individual's efforts to prevent one, there still can be no reasonable expectation of privacy.

Finally, if an employer wishes to eliminate employees' expectations of privacy, it must be done so expressly, with clear acknowledgement by the employees, and limited, again, only to legitimate business needs (and substantial needs if the monitoring is to take place off-site). The social norm that since an employer should monitor, therefore employees should have no expectation of privacy, should be abandoned. This approach would specifically reject the holdings in: 

Smyth v. Pillsbury Company, that even if an employee had a reasonable expectation of privacy in e-mails sent on the company's system, particularly since the company had clearly stated it would not monitor e-mail messages, the company's interest in the content of those messages outweighs employees' privacy interests; and Doe v. XYC Corporation, that the employer's policy prohibiting the use of office e-mail or Internet access for improper purposes was sufficient to eliminate any expectation of privacy as to the employer accessing an employee's computer to determine if he was using it to view adult or child pornography—where there was no evidence the employee was expressly aware of the employer's policy, but instead, no evidence that he was unaware of it. Instead, courts should follow the holding in Quon v. Arch Wireless Operating Company, Inc., that an employee had a reasonable expectation of privacy in text messages

opinion).

287. This would be analogous to the court ruling that it is the one, such as an employer, seeking an exemption to liability for listening to telephone conversations under the ECPA that has the burden of establishing that the person involved in the conversation consented to its monitoring. See supra note 201 (providing instances in which courts have placed the burden on the employer).


289. See supra notes 247-251 and accompanying text (discussing various judicial rulings regarding the reasonable expectation of privacy).

290. See supra notes 223-225 and accompanying text (referring to cases and other authorities that fail to recognize employee privacy).


sent over the employer-provided service where the employer's informal policy was to not audit messages unless employees exceeded usage limits and refused to pay overage charges. In other words, the expectation of privacy is retained absent an express and acknowledged notice that messages (and conversations) will be regularly monitored and audited.

These recommendations do not radically change the historic approach the United States has taken regarding the right to privacy, particularly for employees. Rather than fundamentally change the approach to privacy protection as some commentators have argued, these suggestions retain the fundamental aspects of the right to privacy as they have developed in the United States for over a century—making only slight adjustments to their implementation. These adjustments may only be "slight," but they can have a profound effect on re-balancing the interests between employee privacy and employer property rights.

VI. CONCLUSION

Since the latter part of the twentieth century, the critical determinant of whether a person has a right to privacy is whether that person has a reasonable expectation of privacy in the situation at hand. Judicial applications of this rule have emphasized that the potential for disclosure eliminates any expectation of privacy—and hence, any right to privacy. Social norms also dictate the expectation of privacy and the trend in workplace privacy rights has been to assume that because an employer can monitor, the employee should have no reasonable expectation of privacy.

Even in situations in which an employee has a reasonable expectation of privacy, it may still be invaded if the employer can establish a legitimate business interest in the intrusion. As a result, employer property rights trump employee privacy rights. This situation is exacerbated by the increasing use by employees of their employers' communications equipment to perform their jobs.

293. 529 F.3d 892, 906-08 (9th Cir. 2008), rehearing, en banc, denied, 2009 U.S. App. LEXIS 2259 (9th Cir. Jan. 27, 2009).
294. See supra note 224 (listing cases with similar holdings).
295. See generally Richards & Solove, supra note 61 (arguing that Warren & Brandeis' The Right to Privacy shifted the analysis away from already-established notions of confidentiality in English common law); Comment, Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?, 95 CAL. L. REV. 1115 (2007) (arguing employee privacy rights could be strengthened by amending the ECPA by adopting European and English privacy standards); Rustad & Paulsson, supra note 181 at 899-900 (asserting the ECPA should be amended to incorporate the European human rights approach for electronic monitoring).
Unless the courts abandon the approach that any potential disclosure eliminates the right to privacy, and rebalance the priority of employer property rights versus employee privacy rights, employees will have no right to privacy as to their employers—at work or at home.