2009

Employers Cannot Get the Message: Text Messaging and Employee Privacy

Amanda J. Lavis

Follow this and additional works at: https://digitalcommons.law.villanova.edu/vlr

Part of the Labor and Employment Law Commons

Recommended Citation
Available at: https://digitalcommons.law.villanova.edu/vlr/vol54/iss3/5

This Note is brought to you for free and open access by Villanova University Charles Widger School of Law Digital Repository. It has been accepted for inclusion in Villanova Law Review by an authorized editor of Villanova University Charles Widger School of Law Digital Repository.
EMPLOYERS CANNOT GET THE MESSAGE:  
TEXT MESSAGING AND EMPLOYEE PRIVACY

“The extent to which the Fourth Amendment provides protection for the 
contents of electronic communications in the Internet age is an open 
question.”1

I. INTRODUCTION: IT’S A TEXTUAL WORLD

Millions of Americans have used them to vote for their favorite 
“American Idol” contestant.2 Colleges and universities use them to inform 
students of security alerts or weather warnings.3 Barack Obama used one 
to announce his vice-presidential candidate.4 Kobe Bryant used them to 
assert his innocence in his sexual assault case.5 Many people use them to

1. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008) 
   (evaluating employee privacy rights in text communications), reh’g en banc 
denied, 554 F.3d 769 (9th Cir. 2009).
   2008/05/22/americain-dol-cook-ed-by-txt-messages/ (May 22, 2008, 14:24 PM 
PST) (“[T]he most recent season of “American Idol” show generated 78 million 
text messages—up from 67 million last season.”).
3. See Alison Go, Text Message Alerts—A First Look, U.S. NEWS & WORLD 
   01/03/text-message-alerts—a-first-look.html (noting use of text messages to 
   update students on weather alerts or power failures); Clifford M. Marks, 
   university campuses has expanded dramatically since the Virginia Tech shooting . . .“). In the wake of recent school shootings, numerous universities have 
   implemented text messaging alert systems to warn students of danger. See Marks, 
   supra (outlining increase in text messaging alert systems). “[W]hile hundreds of 
   campuses have adopted text alerts, most students are not embracing the system— 
   even in an age when they consider their mobile phones indispensable.” Alan 
   Scher Zagier, College Students Slow to Embrace Text Alerts, USA TODAY, Feb. 28, 2008, 
   phone-alerts_N.htm. Some campus participation rates are lower than 30%. See id. 
   (comparing participation rates among universities with text messaging alert sys-
   tems). Even more telling is the fact that “at Virginia Tech, where a gunman killed 
   32 people and himself . . . four in 10 students still have not signed up for emer-
   gency text alerts.” Id. Nevertheless, campus officials are relying on younger 
   generations, who are more integrated with text messaging and mobile communication, 
   to increase participation in the programs. See, e.g., id. (“At Princeton, 90% of first-
   year students are enrolled, compared with an overall rate of 64% for all undergraduates.”).
4. See Jessica Yellin, Campaign: Obama’s VP Choice to Be Announced Saturday, 
   (“Sen. Barack Obama’s choice for running mate will be announced to supporters 
in a text message Saturday morning . . .“). For further discussion of the impor-
   tance of text messaging in politics, see infra note 13.
   cbsnews.com/stories/2004/06/21/national/main624983.shtml (noting text
messages “might impeach statements or testimony, making them potentially ‘highly relevant’
[Text messaging] is fast and direct, screening out the pleasantries that even standard e-mail messages call for, like ‘how are you.’ It is used to blast information among co-workers and inform parents of their children’s whereabouts, and, as Kwame M. Kilpatrick demonstrated en route to his downfall as mayor of Detroit, is useful in expressing feelings of romantic desire.
Id.
Once the territory of teenagers, text messaging is becoming a major means of communications around the world and a tool utilized by many businesses. In the United States alone, an astonishing 189 billion text messages were sent in 2007, with a projected 301 billion to be sent in 2008. When expanded to major markets worldwide, the number balloons to 2.3 trillion messages. Due to the rapid growth and integration of text messaging into corporate America, the issue of mobile privacy has

9. See Steinhauer & Holson, supra note 8, at A1, (reporting that thirteen to seventeen year-olds send average of 1,742 text messages per month). The digital generation gap is particularly pronounced in the area of text messaging. See id. (reporting age differential in text messaging usage). For example, one sixty-two year-old retired physician's assistant "found herself flummoxed when her two granddaughters sent her text messages she did not know how to retrieve." Id. That woman attended a class sponsored by AT&T at a local senior's center to learn how to open and utilize text-messaging services. See id.; see also Jenna Ross, Cell Phone Classes at Senior Center? Texting Included, STAR TRIB., Sept. 19, 2008, at A1, available at http://www.startribune.com/local/west/28634809.html?page=1&c=y (describing senior citizen cell phone classes); Text Message Classes for Over 50s, BBC News, July 23, 2004, http://news.bbc.co.uk/1/hi/scotland/3917665.stm (describing senior text messaging classes in United Kingdom). Even though many seniors remain open to mobile communications such as cell phones and text messaging, some seniors resist technological advances. See Ross, supra ("That's stupid for an 84-year-old man to go around with a Bluetooth. . . . Besides that, I've got hearing aids, so there's no room." (quoting senior citizen considering purchase of advanced cell phone technology)). For a further discussion of teenage text messaging, see supra note 7 and accompanying text (discussing teenage preference of texting over talking).

10. See Tom Van Riper, Text-Messaging Generation Entering Workplace, MSNBC, Aug. 30, 2006, http://www.msnbc.msn.com/id/14576541/ (discussing changes emerging in workplace behavior between young professionals, coworkers, and clients caused by availability of new technology). As the popularity of mobile messaging services continue to grow, Gartner, Inc. forecasts 2.3 trillion messages will be sent across major markets worldwide in 2008. See Press Release, Gartner, Inc., supra note 8 (discussing text message statistics and recent trends). This estimate reflects a 19% increase from the 2007 total of 1.9 trillion messages. See id. (same). Further, text messaging is not only a new technology, but it is also a new language. See Van Riper, supra ("For folks over 40, the following instant message may look like nothing more than gobbledygook: '#s look gd . . . Inch @ 1/ back l8r.' But for younger employees, it's just simple shorthand for: 'The numbers look good. I'm leaving for lunch at 1 p.m., and I'll be back later.").

The legal field is particularly reliant on mobile forms of communications. See Edward A. Adams, Web 2.0 Still a No-Go, A.B.A.J., Sept. 2008, at 55-56, available at http://abajournal.com/magazine/web_20_still_a_no_go/ (noting lawyers' dependence on mobile communications). For example, in 2008, 76% of law firms provided attorneys with smart phones or Blackberrys—a 49% increase from 2007. See id. at 55 (outlining usage statistics among lawyers). Further, 75% of attorneys use a Blackberry or smart phone for e-mail, while 32% utilize the device for Internet access. See id. (same).

11. See Resende, supra note 8 (discussing research firm Gartner's text message estimate); see also Press Release, Gartner, Inc., supra note 8 (announcing Gartner's study).

12. See Press Release, Gartner, Inc., supra note 8 (discussing text messaging statistics). For a further discussion of the emergence of text messaging as a major means of communication, see supra notes 10-11 and accompanying text.
increasingly become "a political and legal battleground."\(^{13}\) As the digital generation enters the workforce, the number of text messages sent and received in the course of business will exponentially increase.\(^{14}\)

Although the issue of privacy and e-mail usage in the workplace is well-settled,\(^{15}\) "there are no clear rules in the crazy quilt of the mobile communications systems."\(^{16}\) The confusion surrounding mobile communication privacy has only been heightened with the recent Court of Ap-


Text messaging and politics merged again when then-Senator Barack Obama announced that his choice for running mate would be made to supporters via a text message. *See Yellin, supra* note 4 (discussing unusual role of text messaging in announcement). The relevance of text messaging and mobile communication in today's political sphere is further highlighted by the fact that "47 percent of non-Hispanic whites use the Internet, e-mail or text messaging to get political news or exchange their views, compared with 43 percent of non-Hispanic blacks and 50 percent of English-speaking Hispanics." *See How Technology Is Revolutionizing Democracy*, CNN, June 26, 2008, http://www.cnn.com/2008/POLITICS/06/26/technology.election/#cnnSTCText (noting use of text messaging to obtain political news).

14. See In U.S., SMS Text Messaging Tops Mobile Phone Calling, *supra* note 8 (noting average number of text messages sent or received has increased 450% since first quarter of 2006).

15. *See generally* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (discussing privacy law applicable to e-mail maintained by corporation concerning termination of at-will employee). Many states have adopted a strict rule declining to apply a reasonable expectation of privacy for employees in the workplace, especially regarding the use of e-mail. *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 719 (1987) (holding expectation of privacy would not be reasonable if employer "had established any reasonable regulation or policy discouraging employees . . . from storing personal papers and effects in their desks or file cabinets"); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir. 1987) (finding no reasonable expectation of privacy where employee was on notice that employer may conduct searches for work-related purposes); Smyth, 914 F. Supp. at 101 (holding, notwithstanding repeated assurances that employer would not monitor and/or intercept employee e-mails, that employee does not have reasonable expectation of privacy in e-mails that are sent, stored, or received at work); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4-5 (Tex. App. May 28, 1999) (not designated for publication) (holding that employee did not have reasonable expectation of privacy in contents of e-mail messages stored in password-protected "personal" folder on employer's work computer).

peals for the Ninth Circuit’s ruling in *Quon v. Arch Wireless Operating Company*, which concluded that, in certain circumstances, an employee sending text messages from an employer’s device has a reasonable expectation of privacy under the Fourth Amendment. This ruling conflicts with current employee privacy law in other technological areas, such as e-mail, where employees generally have no reasonable expectation of privacy.

In examining *Quon*’s importance, this Note discusses the development of the law concerning employee privacy in the workplace and outlines the apparent conflict between the *Quon* ruling and current employee privacy common law. Part II discusses the evolution of the Fourth Amendment in relation to privacy in the technological workplace and text messaging as a rapidly emerging means of communication. Next, Part III analyzes how the Ninth Circuit recognized a right to privacy in employee text messages and the court’s legal reasoning. Part IV examines the apparent conflict between current e-mail privacy common law and the *Quon* ruling. Finally, Parts V and VI discuss the impact of the Ninth Circuit’s holding in *Quon* and explain the important ways that employers can avoid privacy issues and text messaging.

---

17. 529 F.3d 892 (9th Cir. 2008), *reh’g en banc denied*, 554 F.3d 769 (9th Cir. 2009).

18. *See id.* at 906 (holding, as matter of law, employee had reasonable expectation of privacy).


20. For a further discussion of the evolution of employee privacy laws and the apparent conflict between *Quon* and existing employee privacy common law, see *infra* notes 31-132 and accompanying text.

21. For a further discussion of employee privacy concerning electronic communications and the Fourth Amendment, see *infra* notes 31-68 and accompanying text. For an examination of the emergence of text messaging as a form of communication, see *infra* notes 69-86 and accompanying text.

22. For a further discussion of the facts and reasoning in *Quon*, see *infra* notes 90-111 and accompanying text.

23. For a further discussion of the apparent conflict between e-mail privacy and text messaging privacy, see *infra* notes 113-132 and accompanying text.

24. For a further discussion of the impact of *Quon* on the Fourth Amendment and employee privacy in the workplace, e-mail, and text messaging, see *infra* notes 134-168 and accompanying text.
II. BACKGROUND: THE RIGHT TO PRIVACY IN THE INFORMATION AGE

"Relying on the government to protect your privacy is like asking a peeping tom to install your window blinds."

—John Perry Barlow

In an era where mobile communication is pervasive and necessary, the law regarding privacy and emerging technologies must constantly evolve and adapt to reflect the various new capabilities and forms of communication. Today, courts must apply decades-old law and the Fourth Amendment right to privacy to an increasingly technological world. E-mail, the Internet, cell phones, and text messages have all revolutionized communications in the new digital workplace. As more companies and employers integrate these emerging means of communications, the conflict between text messaging use and workplace privacy will continue to


26. See U.S. CENSUS BUREAU, STATISTICAL ABSTRACT OF THE UNITED STATES 714 (2007), available at http://www.census.gov/prod/2007pubs/08abstract/info comm.pdf (noting over 233 million Americans subscribed to cellular phone service in 2006); see also Press Release, IDC, Inc., IDC Finds More of the World’s Population Connecting to the Internet in New Ways and Embracing Web 2.0 Activities (June 25, 2008), http://www.idc.com/getdoc.jsp?containerld=prUS21303808 (“Nearly a quarter of the world’s population—roughly 1.4 billion people—will use the Internet on a regular basis in 2008[,] and [t]his number is expected to surpass 1.9 billion unique users, or 30% of the world’s population, in 2012 . . . ”). Worldwide, over 1.15 billion Mobile Phones were sold in 2007. See 1.15 Billion Mobile Phones Sold In 2007. 2008? Not So Much, http://www.informationweek.com/blog/main/archives/2008/01/115_billion_mob.html (Jan. 25, 2008, 11:27 EST) (examining cell phone sales statistics). Including these more recent sales figures, this means that over half the world now has a cell phone. See id. (same). Of these users, some utilize smart phones. For a further discussion of smart phones, see infra note 69 (discussing use of smart phones in corporate America). Further, cell phone users in the United States are growing increasingly addicted to using their cell phones. See New Mobile Lifestyle Survey Finds ‘Must Have’ Features Include Mobile Mapping, Messaging, E-Mail, Search and More, BUS. WIRE, Apr. 3, 2006, http://findarticles.com/p/articles/mi_m0EIN/is_2006_April_3/ai_n16116502?tag=content; coll (examining cell phone addiction). One recent survey revealed that 52% of the adults surveyed “keep their cell phone turned on all the time,” while 40% of those aged eighteen to twenty-nine are “likely to drop their landline once and for all.” See id.

27. See Katz v. United States, 389 U.S. 347, 352 (1967) (applying Fourth Amendment test to telephone conversations); United States v. Angevine, 281 F.3d 1130, 1135 (10th Cir. 2002) (examining Fourth Amendment’s application to computer files); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (discussing Fourth Amendment test concerning use of e-mail); see also Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904 (9th Cir. 2008), (“The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in Fourth Amendment jurisprudence that has been little explored.”), reh’g en banc denied, 554 F.3d 769 (9th Cir. 2009).

28. For further discussion on text messaging in the workplace, see infra notes 82 & 86 and accompanying text.

https://digitalcommons.law.villanova.edu/vlr/vol54/iss3/5
grow. Therefore, employers must carefully balance employee privacy with corporate interests.

A. The Fourth Amendment: Reasonable Privacy Expectations in a Digital World

Presently, employers have the ability to examine almost every aspect of an employee’s activities at work. Though there is a modern trend toward recognizing the right to privacy in many areas of American life, courts have not extended the right to privacy substantively in the American workplace. The Supreme Court did not recognize the legitimate interest in privacy in electronic communications until 1967. Over time, courts have, in varying degrees, found that privacy exists in the workplace.

In the case of public employees, the Fourth Amendment protects the expectation of privacy. The Fourth Amendment protects the “right of

29. For a further discussion of the increasing tension between employee privacy rights and corporate interests, see infra notes 113-132 and accompanying text.

34. See, e.g., O’Connor v. Ortega, 480 U.S. 709, 718-19 (1987) (finding expectation of privacy in cases where operational realities of workplace permit such expectation of privacy); Leventhal v. Knapek, 266 F.3d 64, 73-74 (2d Cir. 2001) (finding reasonable expectation of privacy for computer files); Shields v. Burge, 874 F.2d 1201, 1203-04 (7th Cir. 1989) (finding search of employee workspace reasonable); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1928, 1335 (9th Cir. 1987) (finding no reasonable expectation of privacy where employer was on notice that employer may conduct searches for work-related purposes); Gillard v. Schmidt, 579 F.2d 825, 828 (3d Cir. 1978) (holding search of employee’s desk was unreasonable due to expectation of privacy); State v. Young, 974 So. 2d 601, 609 (Fla. Dist. Ct. App. 2008) (recognizing employee’s expectation of privacy where employer provided special lock and key for office); K-Mart Corp. Store No. 7441 v. Troetti, 677 S.W.2d 632, 637-38 (Tex. App. 1984) (finding expectation of privacy when employee provided own lock to secure employer owned locker). But see United States v. Taketa, 923 F.2d 665, 670-71 (9th Cir. 1991) (finding no objectively reasonable expectation of privacy in area of non-exclusive use).
35. See U.S. Const. amend. IV. The Fourteenth Amendment states: All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due
the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.\textsuperscript{36} It is well settled, however, that the Fourth Amendment "protects people, not places."\textsuperscript{37} Thus, where a person is employed by the state, the Fourth Amendment controls searches and seizures by government employers.\textsuperscript{38} Critically, however, "[i]ndividuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer."\textsuperscript{39}

Although the Fourth Amendment only applies to actions by government employers, several states have expressly codified the right to privacy in their constitutions.\textsuperscript{40} Courts in these states recognize a distinct process of law; nor deny to any person within its jurisdiction the equal protection of the laws.

\textit{Id.}

\textsuperscript{36} Id.

\textsuperscript{37} \textit{See Katz}, 389 U.S. at 351 (noting publicly accessible areas may still be private).

\textsuperscript{38} \textit{See O'Connor}, 480 U.S. at 715; \textit{see also} United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) ("The Fourth Amendment prohibits 'unreasonable searches and seizures' by government agents, including governmental employers or supervisors.").

\textsuperscript{39} \textit{O'Connor}, 480 U.S. at 717 (concluding that government employees have reasonable expectation of privacy at work, but "operational realities" may reduce reasonableness of expectation of privacy). Courts have also applied the "reasonable expectation of privacy" test in the context of private employers. \textit{See Smyth v. Pillsbury Co.}, 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding that, once employee communicated comment over e-mail system that was apparently utilized by entire company, reasonable expectation of privacy was lost, and reasonable person would not have considered employer’s interception of communications to be substantial and highly offensive invasion privacy); \textit{Dir. of Office of Thrift Supervision v. Ernst & Young}, 795 F. Supp. 7, 10 (D.D.C. 1992) (applying \textit{O'Connor} standard to question of employee privacy in diaries containing personal and company data).

In \textit{Smyth}, the United States District Court for the Eastern District Court of Pennsylvania held that there is no "reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system." \textit{See Smyth}, 914 F. Supp. at 101. Notably, the \textit{Smyth} ruling is further bolstered when the employer has issued an Internet or e-mail use policy to its employees providing notice of monitoring by the employer. \textit{See, e.g., Simons}, 206 F.3d at 398-99 (ruling employee lacked reasonable expectation of privacy in light of employer’s specific policy addressing internet usage); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (finding no reasonable expectation of privacy where employee consented to employer monitoring). \textit{But cf. Michael Rustad & Cyrus Daftary, E-BUSINESS LEGAL HANDBOOK § 9.02(D) (2001)} (noting company’s failure to enforce Internet policy could create estoppel argument for employee).

\textsuperscript{40} \textit{See generally} ALASKA CONST. art. I, § 22 (1972) ("The right of the people to privacy is recognized and shall not be infringed."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); CAL. CONST. art. I, §§ 3, 24 (establishing privacy rights); FLA. CONST. art. I, § 23 (amended 1998) ("Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein."); IDAHO CONST. art. I, § 22 (extending right to privacy to crime victims); ILL. CONST. art. I, § 6 ("The people shall have the
tional right to privacy.41 Like the Constitution, state constitutions only protect public employees; the protection does not extend to the private sector.42 The only significant exception to this rule is the California constitution, which extends protection of privacy to private as well as public employees.43 Other states, moreover, provide a statutory right to pri-

right to be secure in their persons, houses, papers and other possessions against unreasonable searches, seizures, invasions of privacy or interceptions of communications by eavesdropping devices or other means."; HAW. CONST. art. I, § 6 ("The right of the people to privacy is recognized and shall not be infringed without the showing of a compelling state interest. The legislature shall take affirmative steps to implement this right."); HAW. CONST. art. I, § 7 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches, seizures and invasions of privacy shall not be violated ...."); LA. CONST. art. I, § 5 ("Every person shall be secure in his ... communications ... against unreasonable searches, seizures, or invasions of privacy. ... Any person adversely affected by a search or seizure conducted in violation of this Section shall have standing to raise its illegality in the appropriate court."); MICH. CONST. art. I, § 24 (establishing right to privacy for crime victims); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); Wis. Const. art. I, § 9(m) (finding right to privacy for vic-
tims of crime).


43. See id. (stating California "has extended its state constitution's protection of privacy as well as public employees"). In California, there may be a state constitutional violation of the right to privacy even when there is no state action. See Porten v. Univ. of S.F., 134 Cal. Rptr. 839, 842 (Ct. App. 1976) ("Privacy is protected not merely against state action; it is considered an inalienable right which may not be violated by anyone."). California courts, however, require that
Privacy. These state privacy laws extend to both public and private employers.

In some instances, the "operational realities" of the workplace dictate whether or not an employee has a reasonable expectation of privacy. By virtue of actual office practices, procedures, or regulations, an employer may reduce or eliminate an employee's expectation of privacy. In one instance, the Supreme Court recognized that, "[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." Generally, restricting an employer's access to

an employer show a compelling interest to overcome an employee's reasonable expectation of privacy. See White v. Davis, 533 P.2d 222, 234-35 (Cal. 1975) (holding employee had constitutional privacy claim where employer failed to show compelling interest); Luck v. S. Pac. Trans. Co., 267 Cal. Rptr. 618, 632 (Ct. App. 1990) (ruling private company did not prove compelling interest for employee drug testing). Despite the application of privacy law to both public and private employers, the privacy protected by the California constitution, "is no broader in the area of search and seizure than the 'privacy' protected by the Fourth Amendment." Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 903 (9th Cir. 2008) (quoting Hill v. Nat'l Collegiate Athletic Ass'n, 865 P.2d 633, 650 n.9 (Cal. 1994)), reh'g en banc denied, 554 F.3d 769 (9th Cir. 2009).


47. See id. (describing various instances where privacy expectations are unreasonable).

48. Id. at 718; see also Katz v. United States, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").
puter files by using passwords and locking office doors evidences the employee’s subjective expectation of privacy in those files.\(^{49}\) If the employee is unable to establish a reasonable expectation of privacy, the Fourth Amendment claim will not succeed.\(^{50}\)

If, on the other hand, an employee establishes a reasonable expectation of privacy in the workplace, the employee must also demonstrate that the search was unreasonable in order to claim a violation of the Fourth Amendment.\(^{51}\) Under a Fourth Amendment reasonableness evaluation, the totality of the circumstances determines whether a search is reasonable.\(^{52}\) A court will balance “on the one hand, the degree to which [the search] intrudes upon an individual’s privacy and, on the other, the degree to which [the search] is needed for the promotion of legitimate governmental interests.”\(^{53}\)

When applying the Fourth Amendment’s reasonable expectation test to electronic means of communication—such as e-mail, instant messages, Internet use, or text messages—many courts will look to see whether or not an employer has an established policy addressing an employee’s privacy expectations.\(^{54}\) Some courts have even held that the policies do not...

---

49. See United States v. Slanina, 283 F.3d 670, 676-77 (5th Cir. 2002) (upholding search of government computer, but finding that employee had reasonable expectation of privacy due to lack of policy), vacated on other grounds, 537 U.S. 802 (2002).

50. See Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (rejecting Fourth Amendment privacy claim where person had no reasonable expectation of privacy); United States v. Kriesel, 508 F.3d 941, 947 (9th Cir. 2007) (“[T]he touchstone of the Fourth Amendment is reasonableness.” (quoting Samson v. California, 547 U.S. 843, 854 n.4 (2006))).

51. See O’Connor, 480 U.S. at 725-26 (“[P]ublic employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.”). Under this standard, a court must evaluate whether the search was “justified at its inception,” and whether it “was reasonably related in scope to the circumstances which justified the interference in the first place.” Id. at 726 (citations omitted). Notably, one district court has held that a private employer’s interest in preventing inappropriate and unprofessional comments in its e-mail system far outweighed any privacy interest that an employee may have in his or her e-mail. See Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding no reasonable expectation of privacy for private employee).

52. See O’Connor, 480 U.S. at 726 (articulating totality of circumstances test).


54. See, e.g., Biby v. Bd. of Regents, 419 F.3d 845, 850 (8th Cir. 2005) (considering existence of policy and holding that warrantless search of employee’s computer for work-related materials is not constitutional violation); United States v. Thorn, 375 F.3d 679, 683-84 (8th Cir. 2004) (upholding warrantless search of computer because of presence of computer monitoring policy), vacated, 543 U.S. 1112 (2005), reinstated en banc, 413 F.3d 820 (8th Cir. 2005); United States v. Angeline, 281 F.3d 1130, 1134 (10th Cir. 2002) (holding that monitoring policy defeated employee privacy claim); Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002) (ruling that employer announcement reserving right to inspect company
even need to be reasonable. An express policy that discloses that the employer may inspect the property, information, or data at any time may defeat an employee’s expectation of privacy. An express policy is critical due to the integration of technology into the workplace. Conversely, where the employer has no policy notifying employees that their computer use could be monitored, and there is no indication that the employer directs others to routinely access the employees’ computers, the employees’ subjective beliefs that their computer files are private may be objectively reasonable.

Such monitoring policies are critical, as e-mails have exposed employers to a multitude of unexpected problems, including sexual harassment liability. Access to e-mail and text messages is crucial to employers and

provided computers "destroyed any reasonable expectation of privacy"); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (same); United States v. Bailey, 272 F. Supp. 2d 822, 824 (D. Neb. 2003) (finding that disclosure of monitoring and computer policy in employee handbook and on intranet defeated any claim of privacy regarding computer records by employee) (citations omitted); Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 WL 974676, at *2 (D. Mass. May 7, 2002) (finding employee’s knowledge that employer had technical ability to monitor e-mail defeated privacy claim); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (holding sergeant had no reasonable expectation of privacy in his government e-mail account because e-mail use was reserved for official business and network banner informed each user upon logging on to network that use was subject to monitoring).

55. Cf. Bailey, 272 F. Supp. 2d at 836 ("A company can legitimately regulate the use of its property and is entitled to adopt policies and practices which place restrictions and conditions on the personal use of computer equipment.").

56. See, e.g., O’Connor, 480 U.S. at 717 ("Public employees’ expectations of privacy . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."); Simons, 206 F.3d at 398-99 (holding employee lacked reasonable expectation of privacy in light of employer’s specific policy addressing internet usage); Schowengerdt v. United States, 944 F.2d 483, 488-89 (9th Cir. 1991) (finding no Fourth Amendment violation when employee knew searches would occur "from time to time"); see also Gossmeyer v. McDonald, 128 F.3d 481, 490 (7th Cir. 1997) (finding no privacy interest in furniture that was part of "workplace"); Sheppard v. Beerman, 18 F.3d 147, 152 (2d Cir. 1994) (holding employee had no privacy interest in judge’s "appurtenances, embracing desks, file cabinets or other work areas"); Am. Postal Workers Union, Local AFL-CIO v. U.S. Postal Serv., 871 F.2d 556, 560 (6th Cir. 1989) (permitting search of employee lockers where policy permitted inspection); United States v. Bunkers, 521 F.2d 1217, 1220 (9th Cir. 1975) (holding no expectation of privacy in work-related locker); Wasson v. Sonoma County Junior Coll. Dist., 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (defeating privacy claim due to monitoring and disclosure policy), aff’d on other grounds, 203 F.3d 659 (9th Cir. 2000).

57. For a further discussion on the importance of usage policies, see infra notes 141-149 and accompanying text.


59. See, e.g., Emily Madoff, E-Mail’s Role in Hostile Work Environment, N.Y.L.J., Aug. 23, 1999, at S6 ("E-mail is a perfect vehicle for harassment.").
often plays a key role in litigation.\textsuperscript{60} Specifically, e-mail communications are discoverable evidence during a civil or criminal proceeding against an employer.\textsuperscript{61}

Often, employer liability hinges on key facts found in e-mails or other forms of electronic communication.\textsuperscript{62} For example, Chevron agreed to pay $2.2 million to settle sexual harassment charges lodged against the corporation based on, among other things, an e-mail that had circulated about "25 Reasons Why Beer Is Better than Women."\textsuperscript{63} E-mails may also be the basis for workplace racial discrimination cases.\textsuperscript{64} At Morgan Stanley, two African American employees claimed they were professionally iso-

\textsuperscript{60} See Patricia C. Borstorff, Glenn Graham & Michael B. Marker, E-Harassment: Employee Perceptions of E-Technology as a Source of Harassment, 12 J. APPLIED MGMT. & ENTREPRENEURSHIP 44, 47 (2007) (stating e-mail has played strategic role as evidence in 70% of all employer-employee cases). A study by the American Management Association and the ePolicy Institute found that over 20% of employers have been ordered by a court or administrative agency to produce copies of employee e-mails. See Am. MGMT. ASS'N & EPOLY INST., 2004 WORKPLACE E-MAIL AND INSTANT MESSAGING SURVEY SUMMARY 1 (2004), \textit{available at} http://www.epolicy-institute.com/survey/survey04.pdf (surveying 840 U.S. businesses). Astoundingly, 13% of companies have gone to court to battle lawsuits triggered by employee e-mail. \textit{See id.}

\textsuperscript{61} See Ellen Forman, \textit{That Office E-mail You Deleted Could End Up in Court}, S. FLA. SUN-SENTINEL, Mar. 25, 1997, at 1A ("[I]f you're an employer, E-mail can be subpoenaed by a plaintiff's lawyer and dragged out of the computer in case of a lawsuit."); Karen Brune Mathis, \textit{Eyes on Your E-Mail: Messages Workers Send on Company Computers Are Often Monitored}, FLA. TIMES-UNION, July 15, 1996, at 10 ("[E]-mail creates a permanent record of what's said, providing evidence in criminal and civil suits. The 'delete' key doesn't erase the message from back-up files."). E-mail messages are both troublesome and damaging in litigation because they are a "hybrid written memo and telephone conversation." \textit{See id.} Viewing e-mails as instant communications, employees often rush sending emails and often spend little time drafting or revising e-mail messages, as evidenced by their tendency to be "short, punchy, poorly punctuated—and potentially harmful." \textit{Id.}

E-mail communications are becoming a particular concern in the health services industry. \textit{See Jeffrey A. Van Doren, If You Monitor E-Mail, Have a Policy, HEALTH CARE SUPERVISOR,} Sept. 1996, at 12 ("Use of electronic mail . . . in health care institutions is a new cause for concern in maintaining confidentiality."). If an employee transmits an e-mail message violating the employer's patient confidentiality policy, the employer could be held liable and "the e-mail communication could be the proverbial smoking gun." \textit{Id.} In addition, the use of e-mail communications in law firms is raising new issues. For a thorough discussion of the attorney-client privilege and the use of e-mail communications in the legal setting, see William P. Matthews, Comment, \textit{Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege,} 45 U. KAN. L. REV. 273, 285-95 (1996).


\textsuperscript{63} See Madoff, \textit{supra note 59,} at 56

\textsuperscript{64} For a description of several racial discrimination suits, see \textit{infra} note 65 and accompanying text.
lated and denied advancement after an e-mail containing racist jokes circulated through the company's computer system.\textsuperscript{65}

Because of the prevalence and importance of e-mail and other forms of workplace communications, courts have allowed both public and private employers to defeat employees' expectation of privacy by establishing a formal policy.\textsuperscript{66} The presence of a formal policy dictating that an employer may inspect e-mails and other forms of electronic communication is important in defeating employees' privacy expectations.\textsuperscript{67} Thus, in these workplaces, employees generally do not have a reasonable expectation of privacy concerning e-mail.\textsuperscript{68}

B. TLK2UL8R: The Rapid Emergence of Texting

With the integration of e-mail, Internet, chat, and text messaging into small devices such as smart-phones, employers now must face the complex issue of employee privacy in a mobile digital world.\textsuperscript{69} Privacy issues are


\textsuperscript{66} See, e.g., Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (finding company's interest in preventing inappropriate e-mail activity on its systems outweighed any employee privacy interest); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4-5 (Tex. App. May 28, 1999) (not designated for publication) (discussing in dicta no expectation of privacy despite password protecting e-mail folder); see also Paul M. Schwartz, Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Informational Practices, 2000 Wis. L. Rev. 743, 770 (2000) ("Most participants in the American workplace leave their informational privacy at the door of work."); Larry Armstrong, Someone to Watch Over You, BUS. WEEK, July 10, 2000, at 189 ("When it comes to privacy in the workplace, you don't have any.").

Regardless of Smyth, employers should be mindful of the statutory provisions that prohibit the interception of certain electronic communications. Like e-mails, text messages are subject to the Electronic Communications Privacy Act of 1986. See 18 U.S.C. §§ 2510(14), 2511(1) (2008) [hereinafter ECPA]. The ECPA is an extension of the Federal Wiretapping Act and prohibits the intentional and non-consensual interception of any electronic communication, the unauthorized access of stored communications, or the disclosure or use of any information from an illegally intercepted communication. See Lisa Smith-Butler, Workplace Privacy: We'll Be Watching You, 35 OHIO N.U. L. REV. 53, 67-68 (2009). The ECPA provides employers with three main exceptions permitting the employer, under certain circumstances, to monitor his or her employees' communications. See 18 U.S.C. § 2511(2)(a)(i) (providing service provider exception); 18 U.S.C. § 2511(2)(d) (providing consent exception where employer has obtained prior consent); 18 U.S.C. § 2511(5) (permitting monitoring for certain types of equipment furnished and used during ordinary course of business).

\textsuperscript{67} See HUBBARTT, supra note 44, 147-48 (listing sample e-mail use policy).

\textsuperscript{68} For a further discussion of e-mail privacy case law, see supra note 19 and accompanying text. For a specific discussion of e-mail privacy concerning company email systems, see Brown, supra note 19, at 66.

\textsuperscript{69} For an overview of the smartphone capabilities, see Liane Cassovoy, What Makes a Smart Phone Smart?, http://smartphones.about.com/od/smartphone
especially complex in the realm of employee use of employer hardware and software during work hours.\textsuperscript{70} Specifically, "[t]ext messages are a particularly difficult subject because they do not reside on a company's server system. . . . The messages reside in the memory of each user's phone. Therefore, centralized storage of such messages is difficult without con-

---


70. \textit{See} Dyland McClain, \textit{I'll Be Right with You, Boss, As Soon As I Finish My Shopping}, \textit{N.Y. Times}, Jan. 10, 2001, at G-1. Studies have shown that 90% of employees look at non-work-related Internet sites at least once per day. \textit{See id.} The average worker will spend over two hours per day surfing the Internet for personal use. \textit{See} Press Release, \textit{Salary.com, Americans Waste More Than 2 Hours a Day at Work} (July 11, 2005), http://www.salary.com/aboutus/layoutscripts/abtl\_default.asp?tab=abt&cat=cato122&ser=ser041\&part=Par485. A more disturbing statistic is that 70% of all pornography access occurs during the work hours of 9:00 a.m. to 5:00 p.m., indicating most pornography viewers watch it at work. \textit{See} Pornography Statistics - Pornography at Work, http://www.lightedcandle.org/pornstats/porn\_at\_work.asp (last visited Mar. 14, 2008) (discussing pornography usage statistics); \textit{see also} GERALD A. JUHNKE \& W. BRYCE HAGEDORN, \textit{COUNSELING ADDICTED FAMILIES} 28 (2006) (discussing lost productivity in workplace due to online pornography viewing). Aside from viewing pornography, shopping online, and checking investments and the news, the following categories are the most popular Internet activities for employees: banking (34%); arranging child care (16%); shopping for groceries (12%); researching health care (12%); making appointments (7%); and planning social events (6%). \textit{See} Mark Harrington, \textit{At Work, Surf City: Poll Shows Employees' Internet Habits}, \textit{Newsday} (New York), Apr. 7, 2000, at A06 (discussing online surfing statistics). Despite using more than ten hours per week for personal use, most employees do not find checking their e-mail, online shopping, or personal Internet surfing unethical. \textit{See} Vivian Marino, \textit{Confessions of Workers at Play on the Computer}, \textit{N.Y. Times}, July 15, 2001, http://www.nytimes.com/2001/07/15/business/personal-business-diary-confessions-of-workers-at-play-on-the-computer.html?scp=1&sq=Confessions\%20of\%20Workers\%20at\%20Play\%20on\%20the\%20Computer&st=cse (discussing survey of employee attitudes concerning Internet use).

"More than one-fourth of employers have fired workers for misusing e-mail and nearly one-third have fired employees for misusing the Internet." AM. MGMT. ASS'N \& ePOLY INST., 2007 \textit{ELECTRONIC MONITORING SURVEILLANCE SURVEY} 1 (2008), http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.pdf. Companies who have fired employees for e-mail misuse cite the following reasons: "violation of any company policy (64%); inappropriate or offensive language (62%); excessive personal use (26%); breach of confidentiality rules (22%); other (12%)." \textit{Id.} Companies further cite the following reasons for termination for Internet misuse: "viewing, downloading, or uploading inappropriate/offensive content (84%); violation of any company policy (48%); excessive personal use (34%); other (9%)." \textit{Id.}
trolling the user’s phone.”71 Monitoring text-messaging devices presents
two competing interests in the employment privacy context: “the em-
ployer’s right to conduct business in a self-determined manner is matched
against the employee’s privacy interests or the right to be let alone.”72

Although many employers currently lack monitoring polices for text
messaging, the issue of privacy and mobile communication in the work-
place should be critically important to employers.73 In 2008, Nielsen re-
leased data showing that U.S. wireless subscribers now send and receive
more text messages than mobile phone calls.74 During the second quarter
of 2008 alone—when the Ninth Circuit in Quon declared that employees
had a reasonable expectation of privacy75—cell phone users sent an aver-
age of 357 text messages per month.76 Adding further complexity, a re-
cent study found that 19% of smart phone users work more than fifty
hours per week and one-third of users think smart phones “enslave them
to work.”77 Thus, the use of text messaging in the workplace is an issue
that employers should quickly address.78

Text messages and instant messages, which are similar to e-mails and
letters, are also becoming important elements of litigation.79 Unfortu-

71. Marcus R. Jones & Hugh H. Makes, Traps in Electronic Communications, 8 J.
72. Kevin J. Baum, Comment, E-Mail in the Workplace and the Right of Privacy, 42
73. For examples describing the intersection of privacy and mobile communica-
tion in the workplace, see infra note 79.
74. See In U.S., SMS Text Messaging Tops Mobile Phone Calling, supra note 8
(noting in second quarter of 2008, typical subscriber sent or received 357 text
messages, compared to 204 phone calls); see also Marguerite Reardon, Americans
8301-1035_3-10048257-94.html (discussing Nielsen survey results). Nielsen is a
global information and media company that measures markets and trends. See gen-
13, 2008).
75. For a more in depth discussion of Quon, see infra notes 90-111 and accompa-
nying text.
76. See In U.S., SMS Text Messaging Tops Mobile Phone Calling, supra note 8
(discussing text messaging statistics).
77. See Smartphone Users Have Longer Workdays, Make More Money, And
2007/02/smartphone_user.html (Feb. 23, 2007, 15:50 EST) (noting smart phone
users’ work habits).
78. For a further discussion of employer monitoring policies, see infra notes
139-153 and accompanying text.
resources/recruiting/articles/20070901/ncooper.html (last visited Apr. 13, 2009)
(explaining legal liability risks for accidents caused by employees using cell phones
for work-related calls while driving); Engineer Sent Text 22 Seconds Before Fatal Train
probe/index.html?iref=newssearch (noting train conductor sent text message
twenty-two seconds before crash which killed twenty-five people); Christy Oglesby,
com/2008/CRIME/01/11/teachers.charged/index.html?iref=newssearch (noting
nately for employers, most text messaging is not solely limited to personal use.\textsuperscript{80} With as many as two-thirds of people utilizing text messaging for both personal and business reasons, an employee’s expectation of privacy regarding those text messages is a critical issue for both employers as well as labor and employment litigators.\textsuperscript{81}

Businesses have “entered a new frontier with sexual harassment, and in terms of the [I]nternet, e[-]mail, text messaging, Facebook, social networking, all those sites . . . can create new forums for sexual harassment to occur.”\textsuperscript{82} Compounding the concern for liability, a recent study indicates that over 25\% of people have sent a personal or sexually explicit text message to the wrong person. \textsuperscript{83} In one case, a company employee received a sexually explicit text message from her boss at two o’clock in the morning.\textsuperscript{84} The boss denied sending it, “claiming a friend used his phone that night without telling him.”\textsuperscript{85} Nevertheless, the company paid approximately $50,000 in damages.\textsuperscript{86}

Employers, for a variety of reasons, may want to review employees’ text messages,\textsuperscript{87} yet the privacy rules regarding this monitoring are far
from established. Thus, Quon’s holding is a critical ruling in the area of employee privacy rights in mobile communication.88

III. TXT MSGS R PRVT: HOW QUON ESTABLISHES A REASONABLE EXPECTATION OF PRIVACY FOR TEXT MESSAGES

“Logic is a poor guide compared with custom.”

—Winston Churchill 89

Until Quon, no circuit court had specifically addressed the issue of employee privacy in the context of using an employer’s mobile device to transmit or receive text messages.90 In Quon, the Ninth Circuit held that a


90. See Hsieh, supra note 88, at 18 (noting that Ninth Circuit is “the first circuit to address the issue”). In the context of the reasonable expectation of privacy against a law enforcement search, however, numerous courts have recognized that for the purpose of the Fourth Amendment, the person using the device has no reasonable expectation of privacy. See United States v. Meriwether, 917 F.2d 955, 958-59 (6th Cir. 1990) (stating, in dicta, that individual who transmits text message to another person’s pager has no reasonable expectation of privacy in that message); Black v. City of Honolulu, 112 F. Supp. 2d 1041, 1054 (D. Haw. 2000) (noting if state issued employee’s pager, then employee could not have had reasonable expectation of privacy under state constitution); Adams v. City of Battle Creek, No. 1:98-CV-233, 1999 WL 425885 (W.D. Mich. Apr. 28, 1999), (holding governmental employee had no reasonable expectation of privacy for pager that employer “cloned” to monitor communications) aff’d in part and rev’d in part on other grounds, 250 F.3d 980 (6th Cir. 2001); Yu v. United States, No. 97 CIV. 2736, 1997 WL 423070, at *2 (S.D.N.Y. July 29, 1997) (finding no reasonable expectation of privacy for information stored on co-conspirator’s pager); Bohach v. City of Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (holding no expectation of privacy for messages sent over alphanumeric paging system); Giles v. State, No. 01-95-01145-CR, 1998 WL 704021, at *5-6 (Tex. App. Sept. 10, 1998) (finding no expectation of privacy for two defendants whose own telephone numbers were stored in codefendant’s pager); State v. Wojtyna, 855 P.2d 315, 317-19 (Wash. Ct. App. 1993) (applying reasonable expectation of privacy rule for person who sent message to pager).

Conversely, some courts have found that a defendant has a reasonable expectation of privacy on an employer’s cell phone from searches by law enforcement. See United States v. Hunter, No. 96-4259, 1998 WL 887289, at *3 (4th Cir. Oct. 29, 1998) (noting presumable expectation of privacy for pager seized by police officers when defendant was arrested); United States v. Ortiz, 84 F.3d 977, 984 (7th Cir. 1996) (discussing case law concerning defendant’s reasonable expectation of privacy concerning pager found on defendant’s person when arrested); United States v. Stroud, No. 93-30445, 1994 WL 711908, at *2 (9th Cir. Dec. 21, 1994) (finding expectation of privacy for pager police seized from automobile in which defendant was passenger); United States v. Brooks, No. CRIM 2004-0154, 2005 WL 1940124, at *3 (D.V.I. 2005) (finding expectation of privacy for pager seized from defendant’s person at time of his arrest by Drug Enforcement Administration agents); United States v. Morales-Ortiz, 376 F. Supp. 2d 1131, 1135-36, 1139-42 (D.N.M. 2004) (finding expectation of privacy for pager seized from upstairs bedroom of
City of Ontario Police Department employee had a reasonable expectation of privacy for text messages sent on employer-issued alphanumeric pagers.91

The police department in \textit{Quon} informed its officers that use of the pagers for personal matters was a violation of City policy and the department thus reserved the right to audit the messages at any time.92 Employees were also informed that if they exceeded the monthly character limit allotted for text messaging, they would be responsible for paying the resulting additional charges.93 Because the City implemented this policy before purchasing the pagers, the policy did not explicitly reference text messages.94 The department did, however, notify all employees during a meeting that the department's monitoring policy applied to the use of the pagers.95

Despite the formal usage policy, Quon's superiors informed him that the informal policy and practice was that if he paid the overage fees, his messages would not be audited.96 Officer Quon used his pager to send

---

91. See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-08 (9th Cir. 2008) (concluding that employee had reasonable expectation of privacy given employer's informal monitoring policy), 

92. See id. at 906. Specifically, the policy provided:
C. Access to all sites on the Internet is recorded and will be periodically reviewed by the City. The City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.
D. Access to the Internet and the e-mail system is not confidential; and information produced either in hard copy or in electronic form is considered City property. As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.
E. The use of inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail system will not be tolerated.

Id. at 896.

93. See id. at 897 (describing monitoring policy).
94. See id. at 896 (same).
95. See id. (same).
96. See id. at 897 (noting presence of informal policy).
both business and personal messages, including numerous messages that were sexually explicit. Because numerous officers were consistently going over the monthly character limit, the department decided to audit officers' messages and asked the department's text provider, defendant Arch Wireless, to deliver the contents of the officers' text messages. Arch Wireless printed out copies of the messages and delivered them to the police department officials. Quon sued Arch Wireless for violating the Stored Communications Act and the police department for violating the Fourth Amendment.

After conducting a reasonable expectation of privacy balancing test, the Ninth Circuit determined that Officer Quon had a reasonable expectation of privacy. The court reasoned that text messages are similar to letters and e-mails. Thus, while the address information and the size of the text message would not be protected under the Fourth Amendment, the content of the text messages would. In today's business world, where electronic communication has largely supplanted the telephone and

The practice was, if there was overage, that the employee would pay for the overage that the City had... [Quon's supervisors] would usually call the employee and say, 'Hey, look, you're over X amount of characters. It comes out to X amount of dollars. Can you write me a check for your overage?'

Id. Quon's supervisor created this informal policy. See id. (describing Lieutenant Duke's practice of collecting overage fees). Even though Quon's supervisor was not the "official policymaker," that fact did not diminish Quon's reasonable expectation. See id. at 907 (noting that Lieutenant Duke's statements as supervisor carry great deal of weight).

97. See id. at 898 (describing Officer Quon's text message use).
98. See id. at 897-98 (noting acquisition of records).
99. See id. at 898 (same).
100. See id. (outlining claims).
101. See id. at 908-09 (analyzing expectation of privacy under Fourth Amendment reasonableness test). For further discussion of the Fourth Amendment reasonableness test, see supra notes 52-55 and accompanying text.
102. See id. at 905. It is well-settled that, "since 1878, . . . the Fourth Amendment's protection against 'unreasonable searches and seizures' protects a citizen against the warrantless opening of sealed letters and packages addressed to him in order to examine the contents," United States v. Choate, 576 F.2d 165, 174 (9th Cir. 1978) (citing Ex parte Jackson, 96 U.S. 727, 732-33 (1877)); see also United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy . . . ."). By contrast, individuals do not enjoy a reasonable expectation of privacy in what they write on the outside of an envelope. See United States v. Hernandez, 313 F.3d 1206, 1209-10 (9th Cir. 2002) ("Although a person has a legitimate interest that a mailed package will not be opened and searched en route, . . . there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior.").
103. See Quon, 529 F.3d at 905 (analogizing text messages to letters and e-mails).
hardcopy letter as the principal form of communication, such an analogy is particularly relevant.  

The Ninth Circuit specifically highlighted the importance of a monitoring policy that addresses text messaging and other electronic forms of communication. The court stated that unless there is regular monitoring and access, people retain a legitimate expectation of privacy in their messages. Applying this rule of law to the facts in Quon, the court’s ruling hinged upon the police department’s informal monitoring policy. Despite the police department holding a meeting to explicitly inform employees that the text messages were subject to the department’s general e-mail and Internet use policy, the court ruled that Officer Quon had a reasonable expectation of privacy in his text messages—absent the consent of a sender or recipient—because the operational reality revealed that text messages were not monitored in most cases. The court specifically noted that personal text messages were not monitored if employees paid for the messages and that many of the employees were aware of this fact. Thus, the court determined that Quon retained a reasonable expectation of privacy. This privacy expectation is not boundless, however, because the court explained that one of the recipients could have permitted the department to review their messages.

IV. THE LEGAL QUONUNDRUM: HOW QUON CONFLICTS WITH E-MAIL PRIVACY RULINGS

“The Internet is just a world passing around notes in a classroom.”
—Jon Stewart

Although the Ninth Circuit concluded in Quon that the privacy interest in letters, e-mails, and text messages are identical, the court’s holding conflicts with the general principle that employees have no reasonable expectation of privacy in the presence of an employer monitoring policy.

104. For a discussion of the increase in text message as a form of electronic communication, see supra note 11 and accompanying text.
105. See Quon, 529 F.3d at 896, 906-07 (highlighting department’s lack of formal written policy regarding text messaging and presence of formal written policy regarding computer, Internet, and e-mail usage).
106. See id.
107. See id. at 905 n.6 (recognizing importance of informal monitoring policy to disposition of case).
108. See id. (addressing reasonable expectation of privacy due to informal usage policy).
109. See id. at 907 (same).
110. See id. at 906-07.
111. See id. at 906.
113. See Quon, 529 F.3d at 905 (reasoning employer policy renders employees’ expectations of privacy unreasonable). For a discussion of why employees have no
In particular, courts have ruled that employees have no reasonable expectation of privacy in the contents of e-mail messages sent and received over their employers’ e-mail systems and stored on the employees’ office computers. 114 The Ninth Circuit should have adhered to the law concerning e-mail and computer privacy in the workplace and applied this principle of law to text messaging.115

Because text messages are similar to e-mails, an employee’s expectation of privacy may be overcome by a formal usage policy.116 Courts have found no expectation of privacy in computer files or e-mails for an employee where: (1) the employer owns the computer; (2) the employee uses that computer to obtain access to the Internet and e-mail through the employer’s network; and (3) the employer explicitly cautions the employee that information flowing through or stored on computers within the network cannot be considered confidential.117 In particular, where a government employer has adopted and enforced an express e-mail usage policy, an employee’s expectation of privacy will not be reasonable.118 Yet even when there is no formal usage policy, an employee may lack a reasonable expectation of privacy: in one case, a court determined that a private employee had no reasonable expectation of privacy even when the employer repeatedly assured employees that the company “would not intercept e-mail communications and reprimand or terminate them based on the contents thereof.”119

At least one court has also looked to ownership of e-mail accounts and computers to determine reasonable expectations of privacy.120 In McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *5 (Tex. App. May 28, 1999) (not designated for publication) (allowing no reasonable expectation of privacy on employer-owned computer).


115. For a discussion of e-mail privacy, see supra notes 54-68 and accompanying text.

116. See, e.g., Smyth, 914 F. Supp. at 101 (finding no reasonable expectation of privacy in tort action concerning e-mails voluntarily made from employee to employer using company email system).

117. See Wasson v. Sonoma County Junior Coll., 4 F. Supp. 2d 893, 905-06 (N.D. Cal. 1997) (noting that employer’s computer policy, which provides "the right to access all information stored on [the employer's] computers," defeats employee’s reasonable expectation of privacy in files stored on employer’s computers). For further discussion of privacy cases in the workplace see supra note 56.


119. See Smyth, 914 F. Supp. at 100 n.2 (discussing employer assurances not to monitor e-mails).

Laren v. Microsoft Corporation,\textsuperscript{121} the Court of Appeals of Texas concluded that an employee had no reasonable expectation of privacy in the contents of e-mail messages sent and received over his employer’s e-mail system and stored on the employee’s office computer.\textsuperscript{122} Following the termination of his employment, the employee filed suit against his employer, bringing a claim for invasion of privacy based on allegations that his employer broke into some of the personal folders maintained on his office computer.\textsuperscript{123} The employee asserted that because he stored e-mail messages under a private password with the employer’s consent, he had a legitimate expectation of privacy in the contents of the folders.\textsuperscript{124}

In ruling that there was no legitimate expectation of privacy, the court considered the specific work-related purpose of the computer.\textsuperscript{125} In that case, the employee was provided with an employer-owned workstation to perform the functions of his job.\textsuperscript{126} The court held that “the e-mail messages contained on the company computer were not [the employee’s] personal property, but were merely an inherent part of the office environment.”\textsuperscript{127}

Despite precedent that employees lack an expectation of privacy in e-mail and computer files, the Ninth Circuit instead relied on the informal monitoring policy to decide that Officer Quon had a reasonable expectation of privacy in his text messages.\textsuperscript{128} Like computers, cellular phones are also an inherent part of the office environment.\textsuperscript{129} Further, the monitoring of e-mail and Internet usage was specifically covered in a formal policy, which was later extended to include text messages.\textsuperscript{130} In fact, Officer Quon even attended the meeting during which the police department announced that the “general” monitoring policy specifically covered texting.\textsuperscript{131} Nevertheless, as one scholar summarized, the court held that

\textsuperscript{121} No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999) (not designated for publication).
\textsuperscript{122} See id. at *4 (distinguishing locked lockers from computers and finding no expectation of privacy in email on company-owned email system and stored in file folder on company-owned computer).
\textsuperscript{123} See id. at *1 (discussing allegations of disclosure of e-mails to third parties).
\textsuperscript{124} See id. at *4 (recapitulating plaintiff’s argument, which analogized password protected e-mails to locked lockers to establish reasonable expectation of privacy).
\textsuperscript{125} See id. (considering work-related activities conducted on computer and ownership of computer and email system).
\textsuperscript{126} See id. (same).
\textsuperscript{127} Id. (holding that e-mails are work items).
\textsuperscript{128} See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 905 (9th Cir. 2008), reh’g en banc denied, 554 F.3d 769 (9th Cir. 2009). For further discussion on the Ninth Circuit’s ruling, see supra notes 101-103 and accompanying text.
\textsuperscript{129} For further discussion of the integration of text messaging and cell phones into the workplace, see supra notes 28-30 and accompanying text.
\textsuperscript{130} See Quon, 529 F.3d at 906. For further discussion of the employer’s formal policy in Quon, see supra note 92.
\textsuperscript{131} See Quon, 529 F.3d at 896.
"[t]he operational reality of the Department was that text messages were not monitored in most cases, particularly if personal use was paid for, and that many of the employees were aware of this fact. Thus, despite having a policy, the employer's failure to consistently implement it proved fatal."\(^{132}\)

V. QUONING AROUND: HOW TO AVOID GIVING EMPLOYEES A REASONABLE EXPECTATION OF PRIVACY

"The fault lies not with our technologies but with our systems."

—Roger Levian\(^{133}\)

Due to the Ninth Circuit's divergence from traditional employee privacy law, \textit{Quon} received significant attention from employment and privacy law lawyers.\(^{134}\) Many privacy advocates and media outlets hailed \textit{Quon} as a victory for employee privacy.\(^{135}\) Meanwhile, employment lawyers speculated about whether employers would need to make substantial changes to their technology usage policies.\(^{136}\)

Employers may still protect their interests while showing deference to the \textit{Quon} decision.\(^{137}\) Drawing from the court's analogy of text messages to letters, it appears likely that an employer could still receive "address information" for text messages and the number of text characters without


\(^{134}\) See, e.g., Philip Gordon, \textit{Quon} Ruling Not a Significant Obstacle to Employers' Accessing Text Messages (June 20, 2008), http://privacyblog.littler.com/tags/fourth-amendment/ (noting various media attention regarding ruling).


\(^{137}\) See Wendy M. Lazerson & Kristen M. Pezone, \textit{Text Messages Off Limits to Employer Inspection} (June 24, 2008), http://www.bingham.com/Media.aspx?MediaID=7175 ("In the new frontier of electronic workplace communications, . . . employers [may] not [ ] read the content of text messages sent by employees through a third-party service provider without the consent of [ ] the employee . . . .")
obtaining consent.\textsuperscript{138} Moreover, there are straightforward and legal ways for employers to navigate the court’s ruling.\textsuperscript{139} For example, employers may create and enforce policies requiring employees to conduct company business on company networks and configure electronic devices to ensure that all related communication is routed over those networks.\textsuperscript{140}

Pedagogically, \textit{Quon} instructs employers to have specific formal policies, to enforce such policies, and to inform employees of any limits on their rights of privacy.\textsuperscript{141} A company should develop a comprehensive Internet and electronic usage policy.\textsuperscript{142} Specifically, employers should (1) review their electronic communication policies to ensure that the policies extend to all forms of workplace electronic communication and put employees on notice that they should have no expectation of privacy in any of these communications, and (2) ensure that there are no informal policies in place that are consistent with their state policies.\textsuperscript{143}

When crafting a policy, an employer should adhere to the following key principles: (1) have a formal written policy and distribute it to all employees; (2) use the policy to inform employees that e-mail and other employer provided hardware are for business use only; (3) enforce the policy to avoid creating an informal expectation of privacy through lack of enforcement; (4) prohibit offensive or sexually explicit material; and (5) include all forms of electronic communications in the policy.\textsuperscript{144}

\begin{itemize}
  \item \textsuperscript{138} See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906 (9th Cir. 2008) (examining possibility of extracting address information from text messages), reh'g en banc denied, 554 F.3d 769 (9th Cir. 2009).
  \item \textsuperscript{139} See Philip Gordon, \textit{supra} note 134 ("Employers can \textit{easily and lawfully} circumvent the Court's ruling.").
  \item \textsuperscript{140} See id. (discussing strategies to navigate \textit{Quon} ruling).
  \item \textsuperscript{141} See Stewart, \textit{supra} note 136 ("The lesson to be learned [from \textit{Quon}] is that an employer should have a specific written policy, that is enforced, informing employees of any limits on their rights of privacy.").
  \item \textsuperscript{142} See generally Todd J. Shill, Kevin M. Gold & John R. Martin, \textit{Still Don't Get IT?}, in \textit{Employment Law Institute WEST 2007, V-9 to V-10} (2007), available at http://www.pacemarl.org/still%20dont%20get%20IT.htm (noting effective e-mail/Internet policy should address following areas: (1) expectation of privacy; (2) code of conduct; (3) e-mail retention; (4) monitoring, and (5) employee training and awareness). Further,
    The policy should include a clear and concise statement informing employees that: (1) they shall have no expectation of privacy with regard to anything that is placed on the employer's computer network; (2) the computer network is owned by the employer; and (3) a password is no indication of personal privacy.
  \item \textsuperscript{143} Lazerson & Pezone, \textit{supra} note 137.
  \item \textsuperscript{144} See Bruce R. Alper, \textit{Managing the Electronic Workplace}, in 2 \textit{36TH ANNUAL INSTITUTE ON EMPLOYMENT LAW 2007}, 1157, 1179-80 (2007) (outlining essential elements of policy); Shill et al., \textit{supra} note 142, at V-9 to V-10 (same).
\end{itemize}
Importantly, an employer should consistently enforce all policies.\textsuperscript{145} The Ninth’s Circuit’s reliance on the employer’s operational reality could “open the door for employee claims against employers or third-parties based on discrepancies between the day-to-day realities and written policies of a workplace.”\textsuperscript{146} Beyond initial training and distribution of policy manuals, employers may take other actions to reduce employee misconduct.\textsuperscript{147} Frequently redisseminating policies on employees’ permitted use and actual monitoring, and reminding employees of the policies as part of the start-up procedure for their office computers are two such actions.\textsuperscript{148} To illustrate the importance of adhering to the policies, employers should also remind employees of the penalties for violating such restrictions and publicize violations and punishments as they arise.\textsuperscript{149}

Currently, many employers lack adequate Internet or electronic communications monitoring policies.\textsuperscript{150} According to a recent survey by the American Management Association, only 66\% of American corporations monitor employee use of computers and Internet.\textsuperscript{151} Less than half monitor employee e-mail usage.\textsuperscript{152} Overall, employer storage and review of e-mail has increased dramatically.\textsuperscript{153}

In addition to monitoring policies, employer behavior also can greatly impact privacy expectations.\textsuperscript{154} Although employers should proactively try to articulate any employee privacy issues, employees can avoid employers’ access to certain communications by refraining from using their employer-owned devices for any such communication.\textsuperscript{155} Further, employers should ensure that employees closely follow company policies regarding electronic communications.\textsuperscript{156} In fact, given such policies, most employ-

\textsuperscript{145} See Shill et al., supra note 142, at V-10 (discussing importance of dissemination, enforcement, and periodic reminders of policies).


\textsuperscript{148} See id.

\textsuperscript{149} See id.

\textsuperscript{150} See AM. MGMT. ASS’N & EPOL’Y INST., supra note 70, at 1.

\textsuperscript{151} See id. (reporting survey statistics).

\textsuperscript{152} See id. (noting 43\% of companies monitor e-mail use).

\textsuperscript{153} See id. (noting increase in monitoring policies).

\textsuperscript{154} See Brown, supra note 19, at 66 (noting employees should not expect privacy for electronic communications).

\textsuperscript{155} See Stewart, supra note 136 (discussing implications of Quon).

\textsuperscript{156} For further discussion on electronic communication monitoring policies, see supra note 142.
ees acknowledge that they have no reasonable expectation of privacy in electronic communications.  

Technology in the workplace is a new and dynamic source of potential liability and litigation for employers. Some organizations, however, also receive substantial benefits from the use of mobile forms of electronic communication such as text messaging. Thus, to balance the possible harms and benefits of emerging technology and electronic communication, employers should carefully “enact appropriate and effective policies for employee use of company provided technology.”

VI. CONCLUSION: ADDRESSING THE QUONUNDRUM

"Now this is not the end. It is not even the beginning of the end."

—Winston Churchill

157. See Philip Gordon, supra note 134 (analyzing survey results). Littler Mendelson, P.C. and the Ponemon Institute LLC recently surveyed employee’s expectations of privacy. The survey found that:

[E]mployees exhibited a very low expectation of privacy in their electronic mail over the corporate intranet. Only 38% of both [young adults] and [older adults] responded that their privacy would be violated if their employer viewed their e-mail and Internet access over the corporate intranet. This response rate was far lower than the sense of privacy violation created by an employer’s monitoring of any other activity examined, including location tracking, off-duty blogging, and iPod use. The percentages did not change significantly even when respondents were asked whether their privacy would be violated if their employer required them to permit access to Web-based e-mail accounts used for business purposes (including the respondent’s home computer), with only 52% of [young adults] and only 42% of [older adults] responding that they would consider such conduct to be a privacy violation. Ironically and in somewhat of a contradiction, 68% of [young adults] responded that their employer should not use their e-mails and instant messages without their consent.


158. For further discussion of liability arising out of electronic communication, see supra note 79 and accompanying text.

159. For further discussion of the role of text messaging in the corporate world, see supra notes 13, 69, and accompanying text. One company has even implemented the policy of terminating employees via a text message rather than confronting the employee in a phone call. See Katie Freeland, U.K. Store Worker Fired by Text Message, USA TODAY, Aug. 7, 2006, http://www.usatoday.com/tech/news/2006-08-07-text-message-fired_x.htm (describing employer’s defense of firing one employee via text message is attempt to “keep modern”).


Quon provides little guidance to the specifics of employee privacy rights in regards to text messaging on an employer's phone. Indeed, by creating a conflict between e-mail and text messaging case law, Quon raises new questions but does not provide answers.\textsuperscript{162} Although Quon may be limited, employers should still be cognizant of the importance of employee privacy rights with employer owned devices.\textsuperscript{163}

Quon highlights five important issues that employers should consider. First, it highlights the importance of having clear and precise monitoring policies that adapt to rapidly expanding forms of mobile communication.\textsuperscript{164} Second, the Ninth Circuit demonstrated that it would look beyond formal monitoring policies to the operational realities of the workplace; therefore, consistent monitoring is critical.\textsuperscript{165} Third, even though an employer may own the device, have a monitoring policy, and pay for the service, monitoring the content of the communications may not be permissible.\textsuperscript{166} Fourth, usage policies should account for text messaging and other technological developments in communications.\textsuperscript{167} Fifth, employers—at least in the Ninth Circuit—should review current usage policies and monitoring standards to make sure both adhere to Quon. Through careful adherence to these key issues, employers may avoid the legal conundrum presented by Quon's ruling.\textsuperscript{168}

\textit{Amanda J. Lavis}

\textsuperscript{162} See Sylvia Hsieh, \textit{supra} note 88 (discussing unanswered questions raised by ruling).

\textsuperscript{163} For a further discussion of employee privacy rights in the context of employer owned devices, see \textit{supra} notes 125-60 and accompanying text.

\textsuperscript{164} For a further discussion on monitoring policies, see \textit{supra} notes 142-53 and accompanying text.

\textsuperscript{165} For a further discussion of the operational realities test, see \textit{supra} note 46-50 and accompanying text.

\textsuperscript{166} For a further discussion of the monitoring of the contents of electronic communication, see \textit{supra} note 142 and accompanying text.

\textsuperscript{167} For a further discussion of the importance of text messaging in corporate America, see \textit{supra} notes 13-14 and 26-30 and accompanying text.

\textsuperscript{168} For further discussion of the importance of a usage policy, see \textit{supra} notes 56-68 and accompanying text.