

Update to Work Law: Cases and Materials, 2d Ed., (Crain, Kim & Selmi)

Replace note 5. on page 395-96 with the following:

5. Constitutional Protection for Confidential Information and Personal Autonomy. In addition to the privacy protections against unreasonable searches and seizures afforded by the Fourth Amendment, the Fourteenth Amendment’s “concept of ordered liberty” has been interpreted to protect two types of privacy interests: “One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions.” *Whalen v. Roe*, 429 U.S. 589, 599 (1977).

Public employees have raised constitutional challenges when a government employer seeks access to sensitive personal information—such as medical or financial records. *See, e.g., Denius v. Dunlap*, 209 F.3d 944 (7th Cir. 2000) (finding infringement of a public employee’s right of privacy where the employer required employee to sign a release permitting it to review personal medical records and confidential financial information without any justification for seeking the information and in the absence of safeguards against misuse). The right of confidentiality, however, is not absolute, but must be balanced against the government’s interest in disclosure. *See Fraternal Order of Police v. Philadelphia*, 812 F.2d 105 (3d Cir. 1987) (holding that a flexible balancing test should be applied to public employees’ claims that required disclosures violated their privacy interest in avoiding disclosure of confidential information).

The U.S. Supreme Court recently decided a case involving a claim by employees of a government contractor that parts of a government required background investigation violated their constitutional right to avoid disclosure of personal matters. *Nat’l Aeronautics and Space Admin. v. Nelson*, 562 U.S. --- (2011). A Ninth Circuit panel had granted a preliminary injunction against the background investigations, finding that there were serious questions as to whether a broad, open-ended inquiry seeking “any adverse information” from third parties violated the employees’ informational privacy rights. *Nelson v. Nat’l Aeronautics and Space Admin.*, 530 F.3d 865, 881 (9th Cir. 2008). The panel also found that the balance of hardships tipped sharply in favor of the plaintiffs “who face a stark choice—either violation of their constitutional rights or loss of their jobs.” *Id.*

Noting that only two cases, decided more than 30 years earlier, had “referred broadly” to such a constitutional privacy interest, the Supreme Court “assume[d], without deciding” that the Constitution protects informational privacy. Even assuming that such a right exists, the Court held that the challenged background checks would not violate that right because “the Government’s interests as employer and proprietor in managing its internal operations” combined with existing statutory protections against dissemination of the information satisfied any such constitutional right. Justice Scalia and Thomas concurred in the judgment, but wrote separately to emphasize that in their view “[a] federal constitutional right to ‘informational privacy’ does not exist.”

The *Nelson* decision raises some uncertainty about the status of a constitutionally protected right of informational privacy in general. But even if such a right exists, the Court’s opinion makes clear that the employment context is highly relevant to evaluating any such claim, noting

that “the Government has a much freer hand in dealing ‘with citizen employees than it does when it brings its sovereign power to bear on citizens at large.” (Slip Op. at 12, *citing Enquist v. Oregon Dept. of Agriculture*, 55 U.S. 591, 598 (2008)).

Public employees have also asserted constitutional privacy claims under the “autonomy” prong—with mixed success—to challenge decisions by their employers based on their off-duty relationships. *Compare Thorne v. City of El Segundo*, 726 F.2d 459 (9th Cir. 1983) (holding that police department’s refusal to hire plaintiff based in part on a past, private sexual relationship violated her constitutional rights of privacy and free association), *with Mercure v. Van Buren*, 81 F. Supp. 2d 814 (E.D. Mich. 2000) (rejecting constitutional privacy claim by police officer fired for having an affair with the estranged wife of a fellow officer on the grounds that adultery is not constitutionally protected).

Update to Work Law: Cases and Materials, 2d Ed., (Crain, Kim & Selmi)

Replace pages 423-33 in the text with the following:

STENGART v. LOVING CARE AGENCY, INC.

Supreme Court of New Jersey

990 A.2d 650 (2010)

Chief Justice RABNER delivered of the opinion of the Court.

In the past twenty years, businesses and private citizens alike have embraced the use of computers, electronic communication devices, the Internet, and e-mail. As those and other forms of technology evolve, the line separating business from personal activities can easily blur.

In the modern workplace, for example, occasional, personal use of the Internet is commonplace. Yet that simple act can raise complex issues about an employer's monitoring of the workplace and an employee's reasonable expectation of privacy. . . .

Loving Care provides home-care nursing and health services. Stengart began working for Loving Care in 1994 and, over time, was promoted to Executive Director of Nursing. The company provided her with a laptop computer to conduct company business. From that laptop, Stengart could send e-mails using her company e-mail address; she could also access the Internet and visit websites through Loving Care's server. Unbeknownst to Stengart, certain browser software in place automatically made a copy of each web page she viewed, which was then saved on the computer's hard drive in a "cache" folder of temporary Internet files. Unless deleted and overwritten with new data, those temporary Internet files remained on the hard drive.

On several days in December 2007, Stengart used her laptop to access a personal, password-protected e-mail account on Yahoo's website, through which she communicated with her attorney about her situation at work. She never saved her Yahoo ID or password on the company laptop.

Not long after, Stengart left her employment with Loving Care and returned the laptop. On February 7, 2008, she filed the pending complaint [alleging employment discrimination].

In an effort to preserve electronic evidence for discovery, in or around April 2008, Loving Care hired experts to create a forensic image of the laptop's hard drive. Among the items retrieved were temporary Internet files containing the contents of seven or eight e-mails Stengart had exchanged with her lawyer via her Yahoo account.¹ . . . [Loving Care's attorneys reviewed the e-mails and used information culled from them in the course of discovery. When Stengart's lawyers learned that defense counsel had copies of their e-mail communications with plaintiff, they sought the

¹ [n.1]The record does not specify how many of the e-mails were sent or received during work hours. Loving Care asserts that the e-mails in question were exchanged during work hours through the company's server. However, counsel for Stengart represented at oral argument that four of the e-mails were transmitted or accessed during non-work hours—three on a weekend and one on a holiday. It is unclear, and ultimately not relevant, whether Stengart was at the office when she sent or reviewed them.

return of the originals and all copies of the e-mails and moved to disqualify defense counsel as a sanction for violating the attorney-client privilege.]

A legend appears at the bottom of the e-mails that Stengart's lawyer sent [warning readers that the e-mail was confidential and might contain a privileged attorney-client communication.]

. . . Loving Care and its counsel relied on an Administrative and Office Staff Employee Handbook that they maintain contains the company's Electronic Communication policy (Policy) [to argue that its employees have no expectation of privacy in their use of company computers.]

The proffered Policy states, in relevant part:

The company reserves and will exercise the right to review, audit, intercept, access, and disclose all matters on the company's media systems and services at any time, with or without notice. . . .

E-mail and voice mail messages, internet use and communication and computer files are considered part of the company's business and client records. Such communications are not to be considered private or personal to any individual employee.

The principal purpose of electronic mail (*e-mail*) is for company business communications. Occasional personal use is permitted; however, the system should not be used to solicit for outside business ventures, charitable organizations, or for any political or religious purpose, unless authorized by the Director of Human Resources.

The Policy also specifically prohibits "[c]ertain uses of the e-mail system" including sending inappropriate sexual, discriminatory, or harassing messages, chain letters, "[m]essages in violation of government laws," or messages relating to job searches, business activities unrelated to Loving Care, or political activities. The Policy concludes with the following warning: "Abuse of the electronic communications system may result in disciplinary action up to and including separation of employment." . . .

It is not clear from [the Policy's] language whether the use of personal, password-protected, web-based e-mail accounts via company equipment is covered. The Policy uses general language to refer to its "media systems and services" but does not define those terms. Elsewhere, the Policy prohibits certain uses of "the e-mail system," which appears to be a reference to company e-mail accounts. The Policy does not address personal accounts at all. In other words, employees do not have express notice that messages sent or received on a personal, web-based e-mail account are subject to monitoring if company equipment is used to access the account.

The Policy also does not warn employees that the contents of such e-mails are stored on a hard drive and can be forensically retrieved and read by Loving Care.

The Policy goes on to declare that e-mails “are not to be considered private or personal to any individual employee.” In the very next point, the Policy acknowledges that “[o]ccasional personal use [of e-mail] is permitted.” As written, the Policy creates ambiguity about whether personal e-mail use is company or private property. . . .

According to some courts, employees appear to have a lesser expectation of privacy when they communicate with an attorney using a company e-mail system as compared to a personal, web-based account like the one used here. *See, e.g., Smyth v. Pillsbury Co.*, 914 *F.Supp.* 97, 100-01 (E.D.Pa.1996) (finding no reasonable expectation of privacy in unprofessional e-mails sent to supervisor through internal corporate e-mail system); *Scott v. Beth Israel Med. Ctr., Inc.*, 17 *Misc.3d* 934, 847 *N.Y.S.2d* 436, 441-43 (N.Y.Sup.Ct.2007) (finding no expectation of confidentiality when company e-mail used to send attorney-client messages). *But see Convertino v. U.S. Dep’t of Justice*, 674 *F.Supp.2d* 97, 110 (D.D.C.2009) (finding reasonable expectation of privacy in attorney-client e-mails sent via employer’s e-mail system). As a result, courts might treat e-mails transmitted via an employer’s e-mail account differently than they would web-based e-mails sent on the same company computer.

Courts have also found that the existence of a clear company policy banning personal e-mails can also diminish the reasonableness of an employee’s claim to privacy in e-mail messages with his or her attorney. We recognize that a zero-tolerance policy can be unworkable and unwelcome in today’s dynamic and mobile workforce and do not seek to encourage that approach in any way.

The location of the company’s computer may also be a relevant consideration. In *Curto v. Medical World Communications, Inc.*, 99 *Fair Empl. Prac. Cas.* (BNA) 298, 2006 WL 1318387 (E.D.N.Y. May 15, 2006), for example, an employee working from a home office sent e-mails to her attorney on a company laptop via her personal AOL account. *Id.* at 301. Those messages did not go through the company’s servers but were nonetheless retrievable. *Ibid.* Notwithstanding a company policy banning personal use, the trial court found that the e-mails were privileged. *Id.* at 305. . . .

Applying the above considerations to the facts before us, we find that Stengart had a reasonable expectation of privacy in the e-mails she exchanged with her attorney on Loving Care’s laptop.

Stengart plainly took steps to protect the privacy of those e-mails and shield them from her employer. She used a personal, password-protected e-mail account instead of her company e-mail address and did not save the account’s password on her computer. In other words, she had a subjective expectation of privacy in messages to and from her lawyer discussing the subject of a future lawsuit.

In light of the language of the Policy and the attorney-client nature of the communications, her expectation of privacy was also objectively reasonable. As noted earlier, the Policy does not address the use of personal, web-based e-mail accounts accessed through company equipment. It does not address personal accounts at all. Nor does it warn employees that the contents of e-mails sent via personal accounts can be forensically retrieved and read by the company. Indeed, in ac-

knowledging that occasional personal use of e-mail is permitted, the Policy created doubt about whether those e-mails are company or private property.

Moreover, the e-mails are not illegal or inappropriate material stored on Loving Care's equipment, which might harm the company in some way. They are conversations between a lawyer and client about confidential legal matters, which are historically cloaked in privacy. Our system strives to keep private the very type of conversations that took place here in order to foster probing and honest exchanges.

In addition, the e-mails bear a standard hallmark of attorney-client messages. They warn the reader directly that the e-mails are personal, confidential, and may be attorney-client communications. While a pro forma warning at the end of an e-mail might not, on its own, protect a communication, other facts present here raise additional privacy concerns.

Under all of the circumstances, we find that Stengart could reasonably expect that e-mails she exchanged with her attorney on her personal, password-protected, web-based e-mail account, accessed on a company laptop, would remain private.

It follows that the attorney-client privilege protects those e-mails. In reaching that conclusion, we necessarily reject Loving Care's claim that the attorney-client privilege either did not attach or was waived. . . . Specifically, Loving Care contends that Stengart effectively brought a third person into the conversation from the start—watching over her shoulder—and thereby forfeited any claim to confidentiality in her communications. We disagree.

. . . The Policy did not give Stengart, or a reasonable person in her position, cause to anticipate that Loving Care would be peering over her shoulder as she opened e-mails from her lawyer on her personal, password-protected Yahoo account. The language of the Policy, the method of transmittal that Stengart selected, and the warning on the e-mails themselves all support that conclusion. . . . Stengart took reasonable steps to keep discussions with her attorney confidential: she elected not to use the company e-mail system and relied on a personal, password-protected, web-based account instead. She also did not save the password on her laptop or share it in some other way with Loving Care.

As to whether Stengart knowingly disclosed the e-mails, she certified that she is unsophisticated in the use of computers and did not know that Loving Care could read communications sent on her Yahoo account. Use of a company laptop alone does not establish that knowledge. Nor does the Policy fill in that gap. Under the circumstances, we do not find either a knowing or reckless waiver.

Our conclusion that Stengart had an expectation of privacy in e-mails with her lawyer does not mean that employers cannot monitor or regulate the use of workplace computers. Companies can adopt lawful policies relating to computer use to protect the assets, reputation, and productivity of a business and to ensure compliance with legitimate corporate policies. And employers can enforce such policies. They may discipline employees and, when appropriate, terminate them, for violating proper workplace rules that are not inconsistent with a clear mandate of public policy. For example, an employee who spends long stretches of the workday getting personal, confidential

legal advice from a private lawyer may be disciplined for violating a policy permitting only occasional personal use of the Internet. But employers have no need or basis to read the specific *contents* of personal, privileged, attorney-client communications in order to enforce corporate policy. Because of the important public policy concerns underlying the attorney-client privilege, even a more clearly written company manual—that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee’s attorney-client communications, if accessed on a personal, password-protected e-mail account using the company’s computer system—would not be enforceable.

[The Court then decided that the defendant violated a New Jersey rule of professional conduct by failing to immediately notify plaintiff’s counsel or seek court permission to read the e-mails once it realized that they were attorney-client communications. The Court remanded the case to determine what sanctions were appropriate]

NOTES

1. **Divergent Outcomes.** In both *Smyth* and *Stengart*, an employee challenged as violations of privacy an employer’s actions accessing and reading email messages sent using a company owned computer. Why does *Smyth*’s claim fail and *Stengart*’s succeed? Are there factual differences between the two cases that explain the differing outcomes? Or do the two courts simply have fundamentally different attitudes towards the privacy of email communications?

One critical difference between *Smyth* and *Stengart* are the legal contexts in which the privacy claims arise. *Smyth* alleged invasion of privacy in order to challenge his termination, while *Stengart*’s privacy claim arose as part of a claim of attorney-client privilege. Do you think these differing contexts influenced the divergent outcomes? Should the different contexts make a difference in whether or not a privacy interest is recognized?

2. **Content of Communications.** The court in *Smyth* repeatedly refers to his email comments as “inappropriate and unprofessional.” The content of his comments may be relevant to whether his discharge was justified, but are they relevant to the question of whether his privacy was invaded? Conversely, the court in *Stengart* put significant emphasis on the importance of the attorney-client privilege. What if the emails recovered by *Stengart*’s former employer were not privileged communications, but emails to her boyfriend complaining about her supervisors? Would her privacy have been invaded in that case? Should the employer be permitted to use those emails to impeach her testimony in subsequent litigation? In other words, is it the sensitive content of the communications that gives rise to privacy concerns, or are there other privacy interests at stake?

3. **Expectations of Privacy.** In *Smyth*, the court finds that the plaintiff had no reasonable expectation of privacy in the e-mails that led to his discharge. It does not provide much explanation for this conclusion, but its very brief discussion mentions the following factors: (1) the communication was voluntarily made (2) to *Smyth*’s supervisor (3) over the company e-mail system. Are these facts relevant to the issue whether *Smyth* had a legitimate interest in the privacy of his e-mails? How does the court in *Stengart* analyze whether the plaintiff had a reasonable expectation of privacy? What facts *should* be relevant to this inquiry?

In determining whether an individual has a “reasonable expectation of privacy” in other contexts, courts have looked at historical values, societal understandings, established practices and whether the individual has manifested an expectation of privacy through her behavior. Most of these factors, however, are not of much assistance when dealing with new technologies such as e-mail. Because of its newness, the norms surrounding an emerging technology are unsettled and contested. In such a situation, trying to determine legitimate expectations of privacy by referring to societal expectations is wholly circular, for societal expectations will be shaped by whether the law legitimates an individual’s claims of privacy.

Like *Smyth*, cases raising privacy claims in an employee’s work email generally have not succeeded. *See, e.g., Garrity v. John Hancock Mutual Life Ins. Co.*, 18 IER Cases 981 (D. Mass. 2002) (holding that plaintiff employees had no reasonable expectation of privacy in their work email); *McLaren v. Microsoft Corp.*, 1999 Texas App. LEXIS 4103 (Tx. Ct. App. 1999) (same), while claims of invasion of privacy when an employer reads emails on an employee’s personal email account, even when accessed at work or through employer provided computers, have been more successful. *See, e.g., Fischer v. Mt. Olive Lutheran Church*, 207 F. Supp.2d 914 (W.D. Wisc. 2002) (denying defendants’ summary judgment motion on a common law invasion of privacy claim because it was disputed whether the employers’ accessing of plaintiff’s email account is highly offensive to a reasonable person and whether plaintiff’s email account would be considered private by a reasonable person); *Van Alstyne v. Elec. Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009) (reporting jury verdict in favor of former employee on her claim that employer’s accessing of her personal email account violated federal statutory law).

Does it matter what norms ultimately emerge? If a general consensus emerges that e-mail messages—at least in the workplace setting—are not protected communications, then employees will adjust their expectations and behavior accordingly. From this perspective, the choice of a legal rule need not have any long-term impact on privacy interests. Once the rule is clear, employees can protect confidential communications simply by not using e-mail to transmit sensitive information. *See* Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035 (2006) (arguing that employees should avoid using employer equipment for personal use during work, but that their activities off-duty should be protected from employer scrutiny). Are there any costs of failing to protect the privacy of employees’ e-mail communications at work? Can employees neatly segregate work and personal aspects of their communications and their lives?

4. **Employer Policies.** In *Smyth* the employer had assured its employees that it would not intercept their email communications or use them to discipline or discharge. In contrast, the employer in *Stengart* had a policy reserving the right to review all electronic communications. Why did these express employer policies not determine the outcome in each case? *Should* an employer’s policies be decisive? Are there any problems with relying solely on an employer’s formal policies to determine whether an employee has a reasonable expectation of privacy?

5. **Employer Interests.** Employers assert a number of interests in accessing and monitoring their employees’ electronic communications. Among other things, employers worry about lost productivity, the disclosure of trade secrets, liability for sexual or racial harassment and unautho-

rized use of property. These concerns led one federal court of appeals to comment that “the abuse of access to workplace computers 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.” *Muick v. Glenayre Elec.*, 280 F.3d 741, 743 (7th Cir. 2002). Do you agree?

Employers may have legitimate business reasons for engaging in electronic monitoring and surveillance, but the law also affects their incentives for doing so. To the extent that employers fear liability for sexual or racial harassment based on electronic communications, they have an incentive to monitor their employees. The legal standard for liability, however, requires that the conduct must be “severe or pervasive”; isolated or sporadic incidents will not give rise to liability. Although purportedly intended to avoid liability for harassment, employer monitoring practices may go far beyond what the law requires. Professor Dennis Nolan explains how this happens:

Why do employers do more than the minimum required to avoid legal liability, even when that “more” involves spying on all employees or restricting otherwise lawful activities? The answer lies in the relative exposure to liability. The chance of losing a hostile work environment suit, or even of having to defend against a meritless suit, is more than minimal. . . . [T]he law does not protect employees’ interests in the privacy of their electronic communications at work, so there is almost no risk of paying damages to the employees subject to strict employer monitoring and control. Absent a legal counterweight to sexual or racial harassment suits, it is safer for employers to err on the side of intrusion and restriction than on the side of toleration; to do the former is almost costless; to do the latter could be expensive.

Dennis R. Nolan, *Privacy and Profitability in the Technological Workplace*, 24 J. LAB. RES. 209 (2003).

6. Collective Interests in Electronic Privacy. Whether or not the privacy of email and other forms of electronic communication is protected also has implications for the ability of employees to act collectively. One of the challenges facing employees who wish to raise workplace concerns is finding effective means of communicating with others who might share similar concerns. We address the topic of employee voice later in Chapter 8, *infra*, but it is important to note that employees’ interests in speaking collectively is closely linked to concerns about the privacy of their communications.

As discussed above, the labor laws have been held to prohibit certain intrusive employer monitoring practices that might interfere with the right to organize, and these protections apply to electronic forms of monitoring as well. See Richard A. Paul & Lisa Hird Chung, *Brave New Cyberworld: The Employer’s Legal Guide to the Interactive Internet*, 24 LAB. LAW. 109, 137-39 (2008) (employees’ discussions of wages, hours, or working conditions on social networking sites would likely be protected activity under § 7); Jeffrey M. Hirsch & Barry T. Hirsch, *The Rise and Fall of Private Sector Unionism: What Next for the NLRA?*, 34 FLA. ST. U. L. REV. 1133, 1177-79 (2007) (monitoring of e-mails may constitute unlawful surveillance if employees’ communications involve wages, hours and working conditions). The risk is particularly acute in the context of employer-sponsored work groups established to encourage exchange among workers about their

views on workplace issues—including exchanges over e-mail. *Id.* Moreover, some social networking sites and blogs are explicitly designed to serve as sites for building a collective identity that can serve as a basis for union organizing efforts. *See, e.g.,* Wakeup Wal-Mart, <http://www.wakeupwalmart.com> (last visited Jan. 3, 2009) (providing information on Wal-Mart’s “Anti-Union” policy and wages, and inviting workers to share their stories about their employment experiences with Wal-Mart); Starbucks Union, <http://www.starbucksunion.org> (last visited Jan. 3, 2009) (website maintained by Industrial Workers of the World Starbucks Workers Union to provide Starbucks employees with information on joining the union and up-to-date news information on organizing efforts across the country). The labor laws also prohibit discipline or discharge based on employees’ electronic communications if they related to organizing activities. *See Guard Publ’g Co. v. NLRB*, 571 F.3d 53 (D.C. Cir. 2009) (finding that discipline applied to an employee who sent union-related e-mails to coworkers violated 8(a)(3) where the employer’s neutral no-solicitation policy banning non-work-related solicitation of all kinds was selectively enforced).

Surveillance law under the NLRA does allow employer monitoring where the employer has a sufficient business justification. Much of this law was developed, however, in the context of older surveillance technology, such as videotaping employee activities. Consider which of the following would constitute a sufficient business justification for surveillance of electronic communication: monitoring employees’ use of the internet to view pornography; monitoring employees’ use of e-mail to send messages with sexual content; monitoring e-mail for critical or negative comments about supervisors or managers; monitoring e-mail for messages that divulge trade secrets; monitoring e-mail for expressions of poor morale or concern about workplace rules. What employee rights is section 7 aimed at protecting? What employer interests justify intrusion on those rights?

7. Statutory Regulation of E-mail Interception. The Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510 *et seq.*, which amended the Omnibus Crime Control and Safe Streets Act, would appear to provide some privacy protections for e-mail communications. Title I of that statute prohibits the interception of “electronic communications.” Most circuit courts, however, have concluded that an “intercept” for purposes of the ECPA only occurs contemporaneously with transmission, and that, therefore, the retrieval of stored e-mail messages does not violate this provision of the ECPA. *See, e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 (3d Cir. 2004) (holding that an insurance agent had no claim under the ECPA when the insurance company searched its file server on which all of his e-mail messages were stored because there was no “intercept”); *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868 (9th Cir. 2002) (concluding that employer’s unauthorized access of employee’s secure website did not violate Title I because the communication must be acquired during transmission, not while in electronic storage, to be an unlawful “intercept”).

The Stored Communications Act (SCA), found in Title II of the ECPA, does not require an “intercept,” but creates civil liability for one who “(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility,” 18 U.S.C. § 2701(a). However, the statute exempts the seizure of electronic communications by the person or entity providing the electronic communications service. To the extent that an employer accesses employee email on an electronic

communications service it provides, its actions are likely exempted from the prohibitions of the SCA. See, e.g., *Fraser*, 352 F.3d at 115 (holding that because insurance agent’s email was stored on insurance company’s email system, the search of his email falls within exception for provider of service).

On the other hand, employer attempts to access password protected email or web pages maintained by third party service providers are more likely to run afoul of the SCA. For example, in *Pietrylo v. Hillstone Rest. Group*, 2008 U.S. Dist. LEXIS 108834 (D.N.J. 2008), two employees who worked as servers at the employer’s restaurant were fired after managers read their postings on a private MySpace group. The two employees had created the private group for the restaurant’s employees for the purpose of “vent[ing] about any BS we deal with out [sic] work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation.” Postings on the site included sexual remarks about management and customers, jokes about the specifications established for customer service and quality, and references to violence and illegal drug use. A factual dispute over whether the employee who had provided the password had done so voluntarily raised the question of whether the managers had accessed the postings “with authorization”, and therefore the court denied summary judgment for the employer on the SCA claim. A jury ultimately found a violation of the SCA and awarded damages. *Pietrylo v. Hillstone Rest. Group*, 2009 U.S. Dist. LEXIS (D.N.J. 2009). See also *Konop*, 302 F.3d at 880 (reversing summary judgment on SCA claim for employer who accessed employee’s password protected website where parties disputed whether it had gained access through an authorized user); *Fischer*, 207 F. Supp.2d at 926 (denying summary judgment on SCA claim to employer who accessed plaintiff’s web-based Hotmail account).

The Supreme Court recently considered a case involving a public employee’s claim of privacy in electronic communications in the workplace. As you will see, the Court ducked the issue of whether public employees have a reasonable expectation of privacy in their electronic communications in the workplace. Should it have? Instead the Court focused on the reasonableness of the employer’s search. What are the implications of its decision for privacy in the public sector workplace?

CITY OF ONTARIO v. QUON

United States Supreme Court
130 S.Ct. 2619 (2010)

JUSTICE KENNEDY delivered the opinion of the Court.

.....

I A

The City of Ontario (City) is a political subdivision of the State of California. The case arose out of incidents in 2001 and 2002 when respondent Jeff Quon was employed by the Ontario Police

Department (OPD). He was a police sergeant and member of OPD's Special Weapons and Tactics (SWAT) Team. The City, OPD, and OPD's Chief, Lloyd Scharf, are petitioners here. . . .

In October 2001, the City acquired 20 alphanumeric pagers capable of sending and receiving text messages. Arch Wireless Operating Company provided wireless service for the pagers. Under the City's service contract with Arch Wireless, each pager was allotted a limited number of characters sent or received each month. Usage in excess of that amount would result in an additional fee. The City issued pagers to Quon and other SWAT Team members in order to help the SWAT Team mobilize and respond to emergency situations.

Before acquiring the pagers, the City announced a "Computer Usage, Internet and E-Mail Policy" (Computer Policy) that applied to all employees. Among other provisions, it specified that the City "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." In March 2000, Quon signed a statement acknowledging that he had read and understood the Computer Policy.

The Computer Policy did not apply, on its face, to text messaging. Text messages share similarities with e-mails, but the two differ in an important way. In this case, for instance, an e-mail sent on a City computer was transmitted through the City's own data servers, but a text message sent on one of the City's pagers was transmitted using wireless radio frequencies from an individual pager to a receiving station owned by Arch Wireless. It was routed through Arch Wireless' computer network, where it remained until the recipient's pager or cellular telephone was ready to receive the message, at which point Arch Wireless transmitted the message from the transmitting station nearest to the recipient. After delivery, Arch Wireless retained a copy on its computer servers. The message did not pass through computers owned by the City.

Although the Computer Policy did not cover text messages by its explicit terms, the City made clear to employees, including Quon, that the City would treat text messages the same way as it treated e-mails. At an April 18, 2002, staff meeting at which Quon was present, Lieutenant Steven Duke, the OPD officer responsible for the City's contract with Arch Wireless, told officers that messages sent on the pagers "are considered e-mail messages. This means that [text] messages would fall under the City's policy as public information and [would be] eligible for auditing." Duke's comments were put in writing in a memorandum sent on April 29, 2002, by Chief Scharf to Quon and other City personnel.

Within the first or second billing cycle after the pagers were distributed, Quon exceeded his monthly text message character allotment. Duke told Quon about the overage, and reminded him that messages sent on the pagers were "considered e-mail and could be audited." *Id.*, at 40. Duke said, however, that "it was not his intent to audit [an] employee's text messages to see if the overage [was] due to work related transmissions." *Ibid.* Duke suggested that Quon could reimburse the City for the overage fee rather than have Duke audit the messages. Quon wrote a check to the City for the overage. Duke offered the same arrangement to other employees who incurred overage fees.

Over the next few months, Quon exceeded his character limit three or four times. Each time he reimbursed the City. Quon and another officer again incurred overage fees for their pager usage in August 2002. At a meeting in October, Duke told Scharf that he had become “tired of being a bill collector.” Scharf decided to determine whether the existing character limit was too low—that is, whether officers such as Quon were having to pay fees for sending work-related messages—or if the overages were for personal messages. Scharf told Duke to request transcripts of text messages sent in August and September by Quon and the other employee who had exceeded the character allowance.

. . . Arch Wireless provided the desired transcripts. Duke reviewed the transcripts and discovered that many of the messages sent and received on Quon’s pager were not work related, and some were sexually explicit. Duke reported his findings to Scharf, who, along with Quon’s immediate supervisor, reviewed the transcripts himself. After his review, Scharf referred the matter to OPD’s internal affairs division for an investigation into whether Quon was violating OPD rules by pursuing personal matters while on duty.

The officer in charge of the internal affairs review was Sergeant Patrick McMahon. Before conducting a review, McMahon used Quon’s work schedule to redact the transcripts in order to eliminate any messages Quon sent while off duty. He then reviewed the content of the messages Quon sent during work hours. McMahon’s report noted that Quon sent or received 456 messages during work hours in the month of August 2002, of which no more than 57 were work related; he sent as many as 80 messages during a single day at work; and on an average workday, Quon sent or received 28 messages, of which only 3 were related to police business. The report concluded that Quon had violated OPD rules. Quon was allegedly disciplined.

B

. . . . [Quon filed suit alleging] that petitioners violated [his] fourth Amendment rights and the [Stored Communications Act, 18 U.S.C. §2701 *et seq.* (SCA)] by obtaining and reviewing the transcript of Jeff Quon’s pager messages and that Arch Wireless had violated the SCA by turning over the transcript to the City. . . .Relying on the plurality opinion in *O’Connor v. Ortega*, 480 U.S. 709, 711 (1987), the District Court determined that Quon had a reasonable expectation of privacy in the content of his text messages. Whether the audit of the text messages was nonetheless reasonable, the District Court concluded, turned on Chief Scharf’s intent: “[I]f the purpose for the audit was to determine if Quon was using his pager to ‘play games’ and ‘waste time,’ then the audit was not constitutionally reasonable”; but if the audit’s purpose “was to determine the efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs. . . . no constitutional violation occurred.” 445 F.Supp.2d, at 1146. [After a jury concluded that Scharf ordered the audit to determine the efficacy of the character limits, the District Court held that petitioners did not violate the Fourth Amendment.]

The United States Court of Appeals for the Ninth Circuit reversed in part. 529 F.3d 892 (2008). The panel agreed with the District Court that Jeff Quon had a reasonable expectation of privacy in his text messages but disagreed with the District Court about whether the search was reasonable. Even though the search was conducted for “a legitimate work-related rationale,” the Court of Appeals concluded, it “was not reasonable in scope.” *Id.*, at 908. . . . The Court of Appeals further

concluded that Arch Wireless had violated the SCA by turning over the transcript to the City. [The Supreme Court granted the petition for certiorari to consider the Fourth Amendment claim, but declined to review the ruling on the SCA claim.] . . .

III A

[The parties disagree] over whether Quon had a reasonable expectation of privacy. The record does establish that OPD, at the outset, made it clear that pager messages were not considered private. The City's Computer Policy stated that "[u]sers should have no expectation of privacy or confidentiality when using" City computers. Chief Scharf's memo and Duke's statements made clear that this official policy extended to text messaging. The disagreement, at least as respondents see the case, is over whether Duke's later statements overrode the official policy. Respondents contend that because Duke told Quon that an audit would be unnecessary if Quon paid for the overage, Quon reasonably could expect that the contents of his messages would remain private. . . .

The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. See, e.g., *Olmstead v. United States*, 277 U.S. 438 (1928), overruled by *Katz v. United States*, 389 U.S. 347, 353 (1967). In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. See *id.*, at 360-361 (Harlan, J., concurring). It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.

Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve.

[Even if the Court follows the *O'Connor* plurality's approach,] the Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.

A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds. For present purposes we assume several propositions *arguendo*: First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City; second, petitioners' review of the transcript constituted a search within the meaning of the Fourth Amendment; and third, the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere.

B

Even if Quon had a reasonable expectation of privacy in his text messages, petitioners did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcripts. . . .

Under the approach of the *O'Connor* plurality, when conducted for a "noninvestigatory, work-related purpos[e]" or for the "investigatio[n] of work-related misconduct," a government employer's warrantless search is reasonable if it is "justified at its inception" and if "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of" the circumstances giving rise to the search. 480 U.S., at 725-726. The search here satisfied the standard of the *O'Connor* plurality and was reasonable under that approach.

The search was justified at its inception because there were "reasonable grounds for suspecting that the search [was] necessary for a noninvestigatory work-related purpose." *Id.*, at 726. As a jury found, Chief Scharf ordered the search in order to determine whether the character limit on the City's contract with Arch Wireless was sufficient to meet the City's needs. . . . The City and OPD had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand that the City was not paying for extensive personal communications.

As for the scope of the search, reviewing the transcripts was reasonable because it was an efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use. The review was also not "excessively intrusive." *O'Connor, supra*, at 726 (plurality opinion). Although Quon had gone over his monthly allotment a number of times, OPD requested transcripts for only the months of August and September 2002. While it may have been reasonable as well for OPD to review transcripts of all the months in which Quon exceeded his allowance, it was certainly reasonable for OPD to review messages for just two months in order to obtain a large enough sample to decide whether the character limits were efficacious. And it is worth noting that during his internal affairs investigation, McMahon redacted all messages Quon sent while off duty, a measure which reduced the intrusiveness of any further review of the transcripts.

Furthermore, and again on the assumption that Quon had a reasonable expectation of privacy in the contents of his messages, the extent of an expectation is relevant to assessing whether the search was too intrusive. Even if he could assume some level of privacy would inhere in his messages, it would not have been reasonable for Quon to conclude that his messages were in all circumstances immune from scrutiny. Quon was told that his messages were subject to auditing.

As a law enforcement officer, he would or should have known that his actions were likely to come under legal scrutiny, and that this might entail an analysis of his on-the-job communications. Under the circumstances, a reasonable employee would be aware that sound management principles might require the audit of messages to determine whether the pager was being appropriately used. Given that the City issued the pagers to Quon and other SWAT Team members in order to help them more quickly respond to crises—and given that Quon had received no assurances of privacy—Quon could have anticipated that it might be necessary for the City to audit pager messages to assess the SWAT Team’s performance in particular emergency situations.

From OPD’s perspective, the fact that Quon likely had only a limited privacy expectation, with boundaries that we need not here explore, lessened the risk that the review would intrude on highly private details of Quon’s life. OPD’s audit of messages on Quon’s employer-provided pager was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been. That the search did reveal intimate details of Quon’s life does not make it unreasonable, for under the circumstances a reasonable employer would not expect that such a review would intrude on such matters. The search was permissible in its scope.

The Court of Appeals erred in finding the search unreasonable. It pointed to a “host of simple ways to verify the efficacy of the 25,000 character limit . . . without intruding on [respondents’] Fourth Amendment rights.” 529 F.3d, at 909. The panel suggested that Scharf “could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if [OPD] wanted to review past usage, it could have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to [OPD] to review the redacted transcript.” *Ibid.*

This approach was inconsistent with controlling precedents. This Court has “repeatedly refused to declare that only the ‘least intrusive’ search practicable can be reasonable under the Fourth Amendment.” *Vernonia, supra*, at 663. That rationale “could raise insuperable barriers to the exercise of virtually all search-and-seizure powers,” *United States v. Martinez-Fuerte*, 428 U.S. 543, 557, n. 12 (1976), because “judges engaged in *post hoc* evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished,” *Skinner*, 489 U.S., at 629, n. 9. . . . Even assuming there were ways that OPD could have performed the search that would have been less intrusive, it does not follow that the search as conducted was unreasonable. . . .

Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable . . . and the Court of Appeals erred by holding to the contrary. Petitioners did not violate Quon’s Fourth Amendment rights. . . .

[The opinion of JUSTICE STEVENS, concurring on this judgment, is omitted]

[The opinion of JUSTICE SCALIA, concurring in part and concurring in the judgment, is omitted]

NOTES

1. **Reasonable in Scope?** The Ninth Circuit had a different view of the reasonableness of the scope of the search in *Quon*. It wrote:

A search is reasonable “at its inception” if there are “reasonable grounds for suspecting . . . that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file.” *O’Connor*, 480 U.S. at 726. Here, the purpose was to ensure that officers were not being required to pay for work-related expenses. This is a legitimate work-related rationale, as the district court acknowledged.

However, the search was not reasonable in scope. As *O’Connor* makes clear, a search is reasonable in scope “when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct].” *Id.* Thus, “if less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government’s legitimate purposes . . . the search would be unreasonable . . .” *Schwenkerdt v. General Dynamics Corp.*, 823 F.2d [1328,] 1336 [(9th Cir. 1987)] There were a host of simple ways to verify the efficacy of the 25,000 character limit (if that, indeed, was the intended purpose) without intruding on Appellants’ Fourth Amendment rights. For example, the Department could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all of his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if the Department wanted to review past usage, it could have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to the Department to review the redacted transcript. . . . Instead, the Department opted to review the contents of all the messages, work-related and personal, without the consent of Quon or the remaining Appellants. This was excessively intrusive in light of the noninvestigatory object of the search, and because Appellants had a reasonable expectation of privacy in those messages, the search violated their Fourth Amendment rights.

Quon, 529 F.3d at 908-09. How did the Supreme Court respond to this reasoning? Which approach do think is most consistent with the Supreme Court’s precedent in *O’Connor v. Ortega*?