No. 08-1332

In the Supreme Court of the United States

CITY OF ONTARIO, CALIFORNIA, ET AL., PETITIONERS

v.

JEFF QUON, ET AL.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF FOR THE UNITED STATES AS AMICUS CURIAE SUPPORTING REVERSAL

ELENA KAGAN
Solicitor General
Counsel of Record
LANNY A. BREUER
Assistant Attorney General
NEAL KUMAR KATYAL
Deputy Solicitor General
WILLIAM M. JAY
Assistant to the Solicitor General
JOSH GOLDFOOT
VIJAY SHANKER
Attorneys
Department of Justice
Washington, D.C. 20530-0001
(202) 514-2217

QUESTIONS PRESENTED

The United States will address the following questions:

1. Whether a government employee has a reasonable expectation of privacy in messages sent through government-issued communications equipment when his employer has notified him that his use of the equipment is subject to monitoring without notice.

2. Whether, if those messages are deemed private, a government employer's noninvestigative review is unreasonable under the Fourth Amendment because the employer reviewed the messages' content.

3. Whether the sender of a message has a reasonable expectation that the message will remain private once the message is delivered to the recipient.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases: Page

Cases—Continued: Page

Cases—Continued: Page

Constitution and statutes:

Miscellaneous:

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 08-1332

CITY OF ONTARIO, CALIFORNIA, ET AL., PETITIONERS

v.

JEFF QUON, ET AL.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

BRIEF FOR THE UNITED STATES AS AMICUS CURIAE SUPPORTING REVERSAL

INTEREST OF THE UNITED STATES

As the Nation's largest employer, the United States owns or leases hundreds of thousands of wireless communications devices, computers, and similar equipment for the official use of its employees. Federal agencies adopt and enforce policies regulating employees' expectation of privacy in using those resources. Furthermore, in its law-enforcement capacity, the United States investigates state and local government officials for criminal offenses such as public-integrity and civil-rights crimes; those investigations often involve evidence obtained from government-owned computers, communications equipment, and similar devices. In addition, the United States regulates the protection of individual privacy in electronic data and communications under various regu-

latory schemes. The United States accordingly has a strong interest in the resolution of the questions presented by this case. The United States filed a brief as amicus curiae in the court of appeals supporting rehearing en banc.

STATEMENT

1. This case involves messages sent between two-way, alphanumeric text-messaging pagers. In late 2001, the City of Ontario, California obtained 20 of the two-way pagers for use by its employees, including police officers. The City contracted with Arch Wireless Operating Co. for a text-messaging service involving multiple destination points: a message would go from the sender's pager to an Arch receiving station, then to Arch's computer server (where it would be archived), then to an Arch transmitting station, and ultimately to the recipient's pager. Pet. App. 3-4.

The City distributed several of the pagers to members of its SWAT team to assist in instant communication in urgent situations. Respondents Jeff Quon and Steve Trujillo, both SWAT sergeants, received pagers.

Before the City obtained the pagers, it promulgated a Computer Usage, Internet and E-Mail Policy (Policy), which applied to all City employees using the City's electronic resources. Pet. App. 151-155. The Policy contained a number of provisions specifying that the City could monitor its employees' use of electronic resources and that records of that use could be made public. For example, the Policy stated that the City "reserve[d] the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." *Id.* at 152. Sim-

ilarly, the Policy cautioned that "[a]ccess to * * * 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." *Id.* at 153. Finally, the City specified that personal, nonbusiness use of the e-mail system was limited to "'light' personal communications," *i.e.*, "personal greetings or personal meeting arrangements," subject to review for content by a department head. *Ibid.* Personal messages would also be treated as City records "subject to 'access and disclosure' in the legal system and the media." *Ibid.*

Both Quon[1] and Trujillo signed acknowledgments that they were aware of the Policy. Pet. App. 156-157. Each of the acknowledgments reiterated that the City "reserve[d] the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." *Ibid.*

After the City obtained the pagers, it decided to extend the e-mail policy to cover text messages sent through the pager network. In April 2002, Chief of Police Lloyd Scharf convened a meeting of his supervisory staff, at which an administrative officer, Lt. Steven Duke, gave a "[r]eminder that two-way pagers are considered e-mail messages. This means that messages would fall under the City's policy as public information and eligible for auditing." J.A. 30; see Pet. App. 48. Quon attended the meeting and subsequently received a memo from Chief Scharf, see J.A. 28, 30, memorializ-

[1] Unless otherwise specified, "Quon" refers to Jeff Quon rather than his co-plaintiff and ex-wife Jerilyn Quon.

ing Lieutenant Duke's reminder that text messages were treated like e-mail under the Policy. Pet. App. 48.

2. The City's contract with Arch allowed each user 25,000 characters per month; any overage imposed additional costs. Pet. App. 45. Almost immediately, Quon exceeded his monthly character allotment. Lieutenant Duke directed Quon to pay for the overage for which he was responsible, a practice that Lieutenant Duke followed with other pager users as well. *Id.* at 7-8, 50. Although the parties' evidence differs on precisely what Lieutenant Duke said to Quon, Lieutenant Duke apparently did not want to spend his time auditing officers' text messages to determine whether the overage was work-related, and so told Quon that he would not audit the messages if Quon admitted responsibility and paid for the overages. *Id.* at 7-8, 49-51.

Quon repeatedly exceeded the monthly limit and was dunned for the overages. Pet. App. 8. In August 2002, Lieutenant Duke complained about having to collect the overage fees. Chief Scharf asked him if the monthly limit was too low to accommodate work-related messages, or if instead the overages were attributable to personal messages. He directed Lieutenant Duke to request the transcripts of the messages sent from the two pagers with the highest overage for that billing period, one of which turned out to be Quon's. *Id.* at 8, 52-54. The jury subsequently found that the purpose of the audit was indeed to verify the efficacy of the 25,000-character limit, not to view the content of anyone's messages. *Id.* at 12.

Arch provided the transcripts. It agreed to do so because the City was the account holder for the two pagers in question and authorized to obtain that information. Pet. App. 54.

"Many of the text messages sent and/or received by Quon's pager while he was on-duty were, to say the least, sexually explicit in nature." Pet. App. 54. Quon's interlocutors included his wife, Jerilyn Quon; a police dispatcher, April Florio, with whom he was having an affair; and Trujillo. *Id.* at 2, 55. Quon and Florio have alleged that they were disciplined based on the content of the text messages. C.A. E.R. 20-21.

3. Respondents—Jeff and Jerilyn Quon, Florio, and Trujillo—brought Fourth Amendment claims against the City, the Ontario Police Department, and Chief Scharf, as well as other claims not at issue here. The parties cross-moved for summary judgment.

Examining whether Quon had a reasonable expectation of privacy in the text messages sent through his City-issued pager, the district court first looked to the Policy. The court agreed that "Quon had been informed in writing and in person that the City considered the use of the pagers to fall within its e-mail policy, and that the City would monitor the use of its pagers." Pet. App. 89. The court further agreed that the Policy "would have put any employee on fair notice that the [text messages] were, in essence, open to the public for view." *Ibid.* And the court confirmed that, if the Policy were "all that was before it," it "would agree with [petitioners'] position that Quon would have no * * * reasonable expectation of privacy." *Id.* at 88-89.

The court concluded, however, that Lieutenant Duke had "in effect turned a blind eye to whatever purpose an employee used the pager [for], thereby vitiating the department's policy." Pet. App. 90. As a result, "Lieutenant Duke effectively provided [Quon] a reasonable basis to expect privacy in the contents of the text messages," so long as Quon paid for his overages. *Id.* at 90-91.

The district court next concluded that the reasonableness of the search presented a fact question. If Chief Scharf had ordered the audit as a way of testing the efficacy of the 25,000-character limit, then the search was reasonable, the court held. The court therefore set the case for trial on the question of Chief Scharf's intent. Pet. App. 103. The jury found that Chief Scharf had intended to examine the 25,000-character limit, and the district court therefore entered judgment for petitioners on the Fourth Amendment claims. *Id.* at 12, 119.

4. The court of appeals reversed in relevant part. Pet. App. 21-36, 39-40. It concluded that the examination of respondents' text messages had been a search that was "unreasonable as a matter of law" in violation of the Fourth Amendment. *Id.* at 21.

a. The court first held that Quon had a reasonable expectation of privacy in his text messages. Like the district court, the court of appeals observed that the Policy, taken alone, would defeat any reasonable expectation of privacy. See Pet. App. 29. But the court of appeals thought that Lieutenant Duke's actions amounted to an "informal policy" that negated the effect of the official one. *Id.* at 31. Petitioners had objected that Lieutenant Duke had no authority to negate the Policy; the panel rejected that argument, stating: "That Lieutenant Duke was not the official policymaker, or even the final policymaker, does not diminish the chain of command. He was in charge of the pagers, and it was reasonable for Quon to rely on the policy—formal or informal—that Lieutenant Duke established and enforced." *Ibid.*

The court of appeals also held that Quon's expectation of privacy was reasonable even if, as petitioners

contended, Quon's text messages were subject to disclosure on demand by any member of the public under the California Public Records Act, Cal. Gov't Code § 6253 (West 2008). The court of appeals held that the public-records law would only "slightly diminish" Quon's reasonable expectation of privacy, because disclosure requests were not "so widespread or frequent as to [create] an open atmosphere." Pet. App. 32 (citations omitted).

b. Next, the court held that the review of Quon's text messages had unconstitutionally infringed Quon's reasonable expectation of privacy. The court acknowledged that government employers may conduct some work-related searches, and that the City's purpose—evaluating the 25,000-character limit—was reasonable. Pet. App. 34. The court thought, however, that the search was not reasonable in scope, because "[t]here were a host of simple ways" to achieve that purpose without reviewing the content of any messages. *Id.* at 35.

c. Separately, the court of appeals held that, "[a]s a matter of law," the other respondents—Jerilyn Quon, Florio, and Trujillo—had a reasonable expectation of privacy in the text messages they had sent to Jeff Quon, and that petitioners had infringed that privacy right by obtaining the transcripts. Pet. App. 28; see *id.* at 27-29 & n.6. The court acknowledged that those three respondents "had no reasonable expectation that Jeff Quon would maintain the private nature of their text messages, or vice versa." *Id.* at 28. Accordingly, the court wrote, "[h]ad Jeff Quon voluntarily permitted the Department to review his text messages, [those three respondents] would have no claims." *Ibid.* But the court held that the Fourth Amendment precluded "third-party

review" except with "consent from either a sender or recipient of the text messages." *Id.* at 28-29.

The court of appeals thus concluded that all four respondents "prevail[ed] as a matter of law" on their claims against the City and Department. Pet. App. 40. The court held, however, that Chief Scharf was entitled to qualified immunity. *Id.* at 37-38.

4. The court of appeals denied rehearing en banc.

Judge Ikuta, joined by six other circuit judges, dissented from the denial of rehearing. Pet. App. 136-150. In Judge Ikuta's view, Quon's expectation of privacy "was either significantly diminished or non-existent" in light of the City's policy "that even personal messages are subject to 'access and disclosure'" and the possibility that all of Quon's text messages could be made public under the California Public Records Act. *Id.* at 141-142; see *id.* at 142-143. And, she noted, "Quon could have avoided exposure of his sexually explicit text messages simply by using his own cell phone or pager." *Id.* at 143. Judge Ikuta concluded that the panel had erred by dismissing these important considerations based solely on "the informal statement of Lieutenant Duke that he personally would not audit the pagers if the SWAT team members agreed to pay for any overages." *Ibid.*

Judge Ikuta also disagreed with the panel's conclusion that the scope of the search had been unreasonable. In her view, the panel should simply have asked whether the City's audit of the text messages was "reasonably related to the objectives of the search and not excessively intrusive in light of [its purpose]." Pet. App. 145 (brackets in original) (quoting *O'Connor* v. *Ortega*, 480 U.S. 709, 726 (1987) (plurality opinion)). She concluded that the panel erred in looking instead at whether the City could have conducted a less intrusive search, be-

cause this Court has repeatedly specified that a search need not be the "least intrusive means" to be valid under the "special needs" doctrine. *Id.* at 144-149.

Judge Wardlaw, author of the panel opinion, filed a concurrence responding to Judge Ikuta's dissent. Pet. App. 125-136. She contended that Lieutenant Duke's practice of not auditing text messages when officers paid for their own overages was an "express and specific," albeit "informal," City policy that gave Quon an expectation of privacy in his pager and "offset" the California Public Records Act in the analysis. *Id.* at 127, 132. Judge Wardlaw also stated that the panel's opinion "did not adopt a 'less intrusive means' test." *Id.* at 133.

SUMMARY OF ARGUMENT

A. The City provided Quon with a pager for official business and set the ground rules for its use. That policy was entirely legitimate, and nothing in the Fourth Amendment prevents it from having full effect. As the parties and the court of appeals all recognize, an employee has no reasonable ground to expect privacy in his employer-provided equipment when the employer has warned him not to have that expectation.

There are numerous valid reasons—indeed, compelling reasons—why most public and private employers adopt comparable policies, monitoring their computers and networked equipment and warning their employees that they will do so. A single employee's imprudent or malicious use of such devices, including a computer, pager, or "smart phone," can threaten the security of the employer's entire computer network, breach the confidentiality of sensitive data, or expose the employer to liability.

Without disputing these important interests, the court of appeals wrongly concluded that the City was liable here. The court reasoned that a lone lieutenant, who decided not to audit the use of a pager when the officer paid the full overage charge, overrode the City's official policy reserving the right to monitor and disclose employees' electronic communications. But this Court has often concluded that the acts of a subordinate officer do not bind an entire city. That is particularly so here, because the authority Lieutenant Duke exercised related only to overage collection. By contrast, the Policy was not limited to situations when an overage appeared: it told Quon he had no expectation of privacy in his text messages whatsoever.

B. The court of appeals also erred in holding that the City's audit violated the Fourth Amendment. The court did not dispute that the City could validly review the extent to which Quon used his pager for personal rather than official purposes. But the court appears to have held that if the City had any way to perform such an audit without looking at the content of the personal messages, the City was obliged to use that method. That analysis is inconsistent with *O'Connor* v. *Ortega*, 480 U.S. 709 (1987), and other special-needs cases. The proper analysis asks not what methods the City could have chosen, but whether the methods the City in fact chose were appropriate to effectuate its purpose. The City met that standard.

C. Because the City obtained all of the messages at issue through a valid search of the pager account assigned to Quon, the senders of those messages— Jerilyn Quon, Florio, and Trujillo—have no valid Fourth Amendment claim. Once their messages to Quon were delivered to his City-issued pager, they had no further

cognizable interest under the Fourth Amendment in what happened to those messages. A valid search of a person's papers frequently extends to papers sent by another person, such as an already-delivered letter. The original letter-writer has no right to object. So too here: the City had a constitutionally valid basis for searching Quon's text messages, and that basis extends to all of the messages, irrespective of who sent them.

ARGUMENT

THE CITY'S REVIEW OF TEXT MESSAGES FROM A CITY-ISSUED PAGER DID NOT VIOLATE THE FOURTH AMENDMENT

A. Quon Could Not Expect To Keep His Use Of The City's Paging System Private Because The City Policy Dispelled Any Expectation of Privacy

Quon did not own the pager or subscribe to the wireless communications service that he used to send text messages. To facilitate Quon's police work, the City provided him with both the device and the subscription, and the City also set the terms of their use. To establish that the Fourth Amendment precludes the City from inspecting the messages sent to or from the pager issued to him, Quon must prove "that he personally ha[d] an expectation of privacy in the place searched, and that his expectation [was] reasonable." *Minnesota* v. *Carter*, 525 U.S. 83, 88 (1998). Because the City specified that communications using the pager were public records, subject to monitoring and auditing, Quon cannot show that he expected his messages to be private or that society would treat as reasonable any such expectation.

1. Employers specify the terms upon which they provide communications, data, or storage facilities

An individual cannot have an expectation of privacy in property owned or lent by his employer unless "society is prepared to recognize [that sort of privacy interest] as 'reasonable.'" *E.g.*, *Oliver* v. *United States*, 466 U.S. 170, 177 (1984) (quoting *Katz* v. *United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). Ascertaining whether society recognizes a protected zone of privacy in a particular context may at times be difficult. See, *e.g.*, *Carter*, 525 U.S. at 91 (Scalia, J., concurring) (describing the test as "fuzzy"). But that is not the case when an official policy squarely answers the question. When a government employer gives its employee access to a device or facility, but explicitly reserves its own right of access, the employee has no reasonable expectation of a right to exclude the employer.

"[T]he government as employer * * * has far broader powers than does the government as sovereign." *Engquist* v. *Oregon Dep't of Agric.*, 128 S. Ct. 2146, 2151 (2008) (citation omitted). As part of its role as employer, the government has broad authority to set rules, and corresponding expectations, in the workplace. That authority was recognized in this Court's leading case involving privacy in the government workplace, *O'Connor* v. *Ortega*, 480 U.S. 709 (1987). Justice O'Connor's opinion for four Justices observed that "[t]he employee's expectation of privacy must be assessed in the context of the employment relation." *Id.* at 717. The opinion further confirmed that in that context, the reasonableness of a claim of privacy "may be reduced by virtue of actual office practices and procedures, or by

legitimate regulation." *Ibid.*;[2] see *id.* at 739 n.5 (Blackmun, J., dissenting) (acknowledging that "[i]n some cases, courts have decided that an employee had no [reasonable] expectation [of privacy] with respect to a workplace search because an established regulation permitted the search," and noting that "[t]he question of such a search * * * is not now before this Court"). These opinions in *O'Connor* correctly recognize the significant role that an employer's policy plays under the Fourth Amendment in two distinct but complementary respects.

First, by establishing and communicating the terms of access, the government employer eliminates any subjective expectation of privacy that conflicts with those terms. Without "an actual expectation of privacy; that is, [a purpose] 'to preserve [something] as private,'" the employee has no Fourth Amendment claim. *E.g.*, *Bond* v. *United States*, 529 U.S. 334, 338 (2000) (second brackets in original) (quoting *Smith* v. *Maryland*, 442 U.S. 735, 740 (1979)). And the employee can hardly be said to have sought "to preserve [something] as private," *ibid.* (brackets in original) (quoting *Smith*, 442 U.S. at 740), when he places it within a zone of the government workplace where, according to express policy, the employer may look. An employee who ignores this policy and brings private material into such a sphere may have a desire for privacy, but cannot show an expectation of privacy.

Second, even if an employee did develop a subjective expectation of privacy under those circumstances, no such expectation would be reasonable. The core of the Fourth Amendment right is the protection of *one's own*

[2] Justice O'Connor also noted that "the absence of * * * a policy does not create an expectation of privacy where it would not otherwise exist." *O'Connor*, 480 U.S. at 719.

"persons, houses, papers, and effects." Although this Court has recognized that the Fourth Amendment sometimes protects a privacy interest in a space formally owned or controlled by someone else, see, *e.g.*, *Minnesota* v. *Olson*, 495 U.S. 91, 98 (1990) (overnight guest at friend's home), not every invitation to enter such a space confers an accompanying privacy right. See, *e.g.*, *Carter*, 525 U.S. at 90 (defendants had no Fourth Amendment protection in an apartment they visited for a few hours to bag cocaine); *Rakas* v. *Illinois*, 439 U.S. 128, 148 (1978) (merely being "in [a] car with the permission of [the] owner" does not entitle the invited guest to borrow Fourth Amendment protections along with the car).

When an individual is claiming a privacy right based on an invitation from someone else—*e.g.*, to visit a place or use a communications device—the terms of the invitation naturally affect whether the individual can reasonably expect privacy if he accepts. For instance, an overnight guest "seeks shelter in another's home precisely because it provides him with privacy"—the host's privacy. *Olson*, 495 U.S. at 99. "The houseguest is there with the permission of his host, *who is willing to share his house and his privacy* with his guest." *Ibid.* (emphasis added). By contrast, someone who enters a residence only for a short business transaction receives no such "acceptance into the household" and no expectation of shared privacy. *Carter*, 525 U.S. at 90. Thus, while both *Olson* and *Carter* involved "a 'home' in which [the defendants] were present," *ibid.*, Olson and Carter entered those homes on different terms, and those terms conferred different expectations of privacy.

This focus on the terms of an invitation, and their consequence for any expectation of privacy, has particu-

lar force in the government-employment context. This Court's cases involving privacy in someone else's home, car, or property take as a given that the claimant does not expect privacy as against the property owner; rather, he hopes to share the property owner's own privacy from government intrusion. *Olson*, 495 U.S. at 99; accord *Mancusi* v. *DeForte*, 392 U.S. 364, 369 (1968); *O'Connor*, 480 U.S. at 730 (Scalia, J., concurring in the judgment). But in cases like this one, the claimant is demanding something still more. He is contending that when the government has permitted him to use a space or device, the government has also forfeited its own authority to intrude on his private use of that property. That contention is not reasonable when the government employer has told its employee at the outset that it is reserving all of its rights.

2. Employer-provided communications equipment is not subject to a different rule

Employers commonly, and validly, reserve the right to monitor electronic communications equipment, as the courts of appeals have recognized and as respondents do not dispute. Accordingly, the City's policy rests comfortably within any bounds that the Fourth Amendment might place on a government employer's formulation of policy to monitor the workplace.[3] A government employee can claim no expectation of privacy in electronic

[3] For instance, this case does not present the sort of questions that would be raised by searches of employees' *own* accouterments in the physical workplace, such as "closed luggage," a "handbag," or a "briefcase"—three examples that Justice O'Connor suggested might fall outside the scope of a permissible policy on workplace searches, see *O'Connor*, 480 U.S. at 716.

equipment when the employer providing the equipment expressly rules out any such expectation.

a. As the court of appeals recognized, Pet. App. 29-30, federal courts broadly agree that employers may provide that the computers and other electronic equipment their employees use at work are not private. Courts have given effect to monitoring policies implemented in various ways. In some cases, the employers adopted a single written policy governing all computer use. See, *e.g.*, *United States* v. *Thorn*, 375 F.3d 679, 682 (8th Cir. 2004) (state agency's policy warned that "[e]mployees *do not* have any personal privacy rights regarding their use of [agency] information systems and technology"), vacated on other grounds, 543 U.S. 1112 (2005); *United States* v. *Angevine*, 281 F.3d 1130, 1132-1133, 1134 (10th Cir.) (state university's policy "reserved the right to randomly audit Internet use" or to investigate possible misuse and "explicitly caution[ed] computer users that information flowing through the University network is not confidential either in transit or in storage on a University computer"), cert. denied, 537 U.S. 845 (2002); *United States* v. *Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (federal agency's policy "clearly stated that [the agency or its contractor] would 'audit, inspect, and/or monitor' employees' use of the Internet, * * * 'as deemed appropriate'"); accord *Bohach* v. *City of Reno*, 932 F. Supp. 1232, 1234-1235 (D. Nev. 1996) (similar policy as to city-issued pagers); see also *Leventhal* v. *Knapek*, 266 F.3d 64, 74, 75-77 (2d Cir. 2001) (Sotomayor, J.) (finding a factual dispute over whether the state employer "had placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer," but upholding the search as reasonable in any event). In other cases, government em-

ployers maintained an electronic "banner" or "splash screen" that warned the user each time he logged on to the computer system that his computer use was subject to monitoring. *Angevine*, 281 F.3d at 1133, 1134; *United States* v. *Monroe*, 52 M.J. 326, 330 (C.A.A.F. 2000).

Those decisions complement a line of cases similarly upholding government employers' authority to set the terms under which they will monitor other facilities that they make available to employees. For example, the courts have upheld a United States Postal Service (USPS) policy permitting searches of the lockers the USPS provides to its employees. See *American Postal Workers Union* v. *USPS*, 871 F.2d 556, 560-561 (6th Cir. 1989); *United States* v. *Broadus*, 7 F.3d 460, 463-464 (6th Cir. 1993); accord *United States* v. *Bunkers*, 521 F.2d 1217, 1219, 1220 (9th Cir.), cert. denied, 423 U.S. 989 (1975). Regardless whether an employee would have an expectation of privacy in an employer-provided locker in the absence of a policy, see note 2, *supra*, the employee can have no such expectation when the employer makes clear from the outset that it can inspect the locker.

b. Respondents have not argued that the Fourth Amendment forbids or renders ineffective an employer's clearly articulated policy of workplace monitoring. To the contrary, they have conceded that a government employer may specify that it reserves all rights to audit text messages (or similar communications) that employees send through an employer-provided system. See Pls.' Resp. to Pet. for Reh'g En Banc 12 n.3 (government policies, if adhered to in practice, "would negate or diminish an expectation of privacy"). That recognition of an employer's ability to monitor electronic communications under an established policy is appropriate. For at

least three reasons, employer-provided devices such as computers, pagers, and "smart" phones are precisely the type of workplace aid that employers have an important interest in regulating.

First, employers face unique risks from the use of networked devices, which require careful attention. Networked devices are frequently the targets of electronic attacks, designed to steal confidential information, seize control of a network, or distribute malicious software. See generally, *e.g.*, United States Computer Emergency Readiness Team, Dep't of Homeland Sec., *Cyber Threat Source Descriptions* (last visited Feb. 10, 2010) <http://www.us-cert.gov/control_systems/csthreats.html>. Employers may need to monitor the entire network to guard against such threats, because carving out "personal" information (even if practicable) creates too grave a vulnerability. When employees are using an employer's networked device for personal purposes, they pose a potential threat, intentionally or not, to the employer's entire network. Malicious software is just as likely—if not more likely—to be introduced to a network through a personal e-mail as a work-related one. And mobile devices can present the same dangers as traditional desktop computers. See, *e.g.*, United States Computer Emergency Readiness Team, Dep't of Homeland Sec., *Cyber Security Tip ST06-007: Defending Cell Phones and PDAs Against Attack* (2006) <http://www.us-cert.gov/cas/tips/ST06-007.html>; accord, *e.g.*, Yuki Noguchi, *Cell Phones Increasingly Attractive to Hackers*, Wash. Post, Nov. 26, 2004, at A1 <http://www.washingtonpost.com/wp-dyn/articles/A13361-2004Nov25.html>.

Second, and relatedly, the nature of electronic media (whether networked or not) makes it difficult to sepa-

rate work-related matters, over which the employer plainly has policymaking authority, from employees' personal matters. A single sector of a flash drive, a single "packet" of information arriving from the Internet, or even a single text or e-mail message may contain both. The reasons employers adopt auditing policies (such as to protect against malicious software that may be introduced via a flash drive, network, or some other means) thus may extend to all uses of a government-owned device, not just those identifiably related to work. See generally Office of Legal Counsel, United States Dep't of Justice, *Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection System (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Executive Branch* (Jan. 9, 2009) <http://www.justice.gov/olc/2009/e2-issues.pdf> (*OLC Memorandum*).

Third, employees' personal use of a governmental employer's facilities may have legal effects upon the employer itself. Documents created by a public employee for his own use may nonetheless constitute public records that the employer is obliged by state or local open-records laws to preserve and disclose, as the City argues is true here. See Pet. Br. 35-40.[4] Conversely,

[4] See, *e.g.*, *Flagg* v. *City of Detroit*, 252 F.R.D. 346, 355-356 (E.D. Mich. 2008) (text messages sent from city-owned device were public records under Michigan open-records law). Compare, *e.g.*, *Cowles Publ'g Co.* v. *Kootenai County Bd. of County Comm'rs*, 159 P.3d 896, 899-901 (Idaho 2007) (holding that e-mails between county employees, including personal e-mails, are "public records" under state open-records law if they relate to the public interest), with, *e.g.*, *Associated Press* v. *Canterbury*, No. 34768, 2009 WL 3805646 (W. Va. Nov. 12, 2009) (e-mails whose content is entirely personal are not public records). The federal Freedom of Information Act, 5 U.S.C. 552, generally does not require disclosure of purely personal e-mails.

employees' personal communications may reveal sensitive work-related information that the employer validly wishes to keep confidential. Employees' personal documents may also be relevant to the employer's ability to defend itself in litigation. See, *e.g.*, *O'Connor*, 480 U.S. at 713 (plurality opinion) (Dr. Ortega's employer seized his personal greeting card, book, and photograph, all later used as impeachment material); *Biby* v. *Board of Regents*, 419 F.3d 845, 850-851 (8th Cir. 2005) (employer successfully invoked policy specifically reserving the right to search employees' work computers to respond to discovery requests in litigation). For instance, to avoid liability for a hostile work environment created by its employees, an employer must promptly and effectively investigate complaints of harassment. See *Faragher* v. *City of Boca Raton*, 524 U.S. 775, 806-807 (1998). Such an investigation may well require review of employees' personal messages (including e-mail) sent using the company facilities. See, *e.g.*, *EEOC* v. *PVNF, L.L.C.*, 487 F.3d 790, 795, 798 (10th Cir. 2007) (e-mail between co-workers was evidence of hostile work environment). The employer therefore may have valid interests in monitoring the content of communications sent by its employees using facilities the employer provides.

For those compelling reasons, the overwhelming majority of the Nation's employers—including the United States and other public employers—have adopted policies to monitor activities on their electronic communications equipment. See *OLC Memorandum* 4-5; American Mgmt. Ass'n, *2007 Electronic Monitoring & Surveillance Survey* (Feb. 28, 2008) <http://www.amanet.org/

news/177.aspx>.[5] Consistent with these policies, many employers, including the City here, permit their employees to make modest personal use of office equipment. Pet. App. 153. Were this Court to hold that an employer could not monitor personal communications of employees pursuant to a clearly articulated policy, public employers would be left with only two options: either to bar *all* personal use of government-owned communications equipment, or to give over to employees a portion of the government's electronic resources and risk the damage to government networks that such loss of control might cause.

3. The City clearly and validly informed Quon that he would have no expectation of privacy in his text messages

Because the City clearly informed Quon, in advance, that it reserved the right to monitor the text messages sent through his City-issued pager, Quon had no reasonable expectation of privacy in those messages under the Fourth Amendment. The Policy, which by its terms governed e-mails, specified that such messages were "not confidential" or private; were City property; could be "monitor[ed] and log[ged]"; were "subject to 'access and disclosure' in the legal system and the media"; and, therefore, "should not be used for personal or confidential communications." Pet. App. 152-153. And after the City obtained the pagers, it informed Quon, both orally and in writing, that text messages sent through the pag-

[5] Numerous federal agencies notify employees, each time they log onto a government computer or network, that "[y]ou have no reasonable expectation of privacy regarding any communications transmitted through or data stored on this information system." *OLC Memorandum* 6 n.5; see *id.* at 5.

ers "[we]re considered e-mail" and "would fall under the [Policy] as public information and eligible for auditing." J.A. 28, 30 (memorandum addressed to Quon, among others); see Pet. App. 48.[6]

The panel opinion in the court of appeals substantially agreed that the Policy applied to pagers. See Pet. App. 29. To be sure, Judge Wardlaw later suggested that "[t]he record [was] clear that the City had no official policy governing the use of the pagers." *Id.* at 127 (opinion concurring in denial of rehearing en banc). But as both the panel opinion and the district court recognized, Chief Scharf's memorandum, as well as statements made at the meeting he previously convened (see *id.* at 48; J.A. 30), informed Quon and other officers that text messages sent through the City-provided pagers were to be considered e-mail subject to the Policy. See Pet. App. 29, 88-89. Judge Wardlaw noted Quon's testimony that he did not recall learning at the meeting that text messages would be considered e-mail. *Id.* at 127. But the advice given there is memorialized in Chief Scharf's memorandum, J.A. 30, which is apparently uncontroverted. And in any event, the panel did not identify a factual dispute about whether Quon was aware of the Department's policy; it instead held Quon entitled to judgment as a matter of law. Pet. App. 28-29, 40.

In ruling for Quon, the panel relied in part on past practice: the panel noted that Quon's messages had never been reviewed before and that the Department had not received many requests for records under the California Public Records Act. Pet. App. 31, 32. But the extent to which the City had previously exercised its

[6] Indeed, it appears that the pagers received e-mail; the record contains a number of messages from Trujillo's OntarioPolice.org e-mail address to Quon's pager. See, *e.g.*, C.A. Supp. E.R. 514-515.

authority to read officers' text messages, or the public its right to demand city records, is not relevant to the question. So long as the City and public possessed such authority, Quon could not have an expectation of privacy in his text messages that would render ineffective the City's enforcement of its Policy.

This Court held in *Smith, supra*, that a practice of forbearance does not create a reasonable expectation of privacy where none otherwise would exist. In *Smith*, the defendant conceded that a telephone number he dialed would not be private if the telephone company automatically recorded the dialed-number information. 442 U.S. at 744. He argued, however, that he had a reasonable expectation of privacy in the local phone number he dialed, because "telephone companies, in view of their present billing practices, usually do not record local calls." *Id.* at 745. The Court rejected that argument, holding that "[t]he fortuity of whether or not the phone company in fact elects" to record a number dialed "does not, in our view, make any constitutional difference." *Ibid.* What mattered was that Smith "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record," whether or not the company elected to record it for any particular call. *Ibid.* Similarly, a criminal who entrusts information to another person cannot claim an invasion of privacy if that person is or becomes a police informant—whether or not the informant has ever turned state's evidence before. See *United States* v. *White*, 401 U.S. 745, 752 (1971) (plurality opinion). Thus, the City's track record of conducting audits is irrelevant to the question whether Quon could reasonably consider private the messages sent through his City-issued pager. The Policy made clear that he could not.

4. A nonpolicymaking individual such as Lieutenant Duke could not vitiate the City's official policy or give Quon a reasonable expectation of privacy in his text messages

In sustaining Quon's Fourth Amendment claim, the panel relied primarily on Lieutenant Duke's purported informal amendment of the City's monitoring policy. See also Pet. App. 127 (Wardlaw, J., concurring in denial of rehearing en banc) (opining that Lieutenant Duke's policy was "express and specific"). That conclusion is legally and factually flawed.

a. Lieutenant Duke had no authority to set City policy. Indeed, the panel acknowledged as much. Pet. App. 31 (agreeing that "Lieutenant Duke was not the official policymaker, or even the final policymaker"). The panel erred by treating him as having the power to revoke or nullify the Policy for Fourth Amendment purposes.[7]

This Court has often had occasion to determine whether an official makes policy for the municipality that employs him, such that the employer is vicariously liable for his actions. Under none of those cases would Lieutenant Duke be thought capable of reversing the City's policy and announcing his own in its place. "When an official's discretionary decisions are constrained by policies not of that official's making, *those policies*, rather than the subordinate's departures from them, *are the act of the municipality*." *City of St. Louis* v. *Praprotnik*, 485 U.S. 112, 127 (1988) (plurality opinion)

---

[7] To be sure, Lieutenant Duke voiced the initial admonition that text messages sent through the City-provided pagers would be considered e-mail for purposes of the Policy. But Lieutenant Duke did not *set* that policy, and it was the Chief of Police who memorialized the advice in minutes of the meeting, issued under the Chief's signature. J.A. 28, 30.

(emphasis added); see also, *e.g.*, *Jett* v. *Dallas Indep. Sch. Dist.*, 491 U.S. 701, 738 (1989) (treating the *Praprotnik* plurality opinion's analysis of "final policy-making authority" as controlling). "[T]he authority to make municipal policy is necessarily the authority to make *final* policy," and Lieutenant Duke lacked any authority to make final policy. *Praprotnik*, 485 U.S. at 127 (plurality opinion). At most, Lieutenant Duke had some discretion in how he implemented the Policy with respect to pagers. Such interstitial discretion does not transform an employee into a policymaker. See, *e.g.*, *id.* at 130; *id.* at 139-140 (Brennan, J., concurring in the judgment).

b. Even if the Ninth Circuit were right to treat Lieutenant Duke's practice (rather than the written policies of duly authorized policymakers) as the controlling "operational reality," Pet. App. 30, petitioners should still prevail. Lieutenant Duke's actions did not alter the entirety of the Policy; he specified only how he would choose to handle an officer's overage charges (*i.e.*, he would accept an officer's personal check without conducting an audit when the officer admitted personal responsibility for the full amount of the overage). But the police department's interest in monitoring pager use extends far beyond allocating overage charges—as the Policy made clear. See *id.* at 153. There is no evidence that Lieutenant Duke stated or implied that paying the overage charges would confer an absolute immunity from the Policy.

Moreover, only a few months passed between the City's acquisition of the pagers (when Lieutenant Duke developed his practice of collecting for overages) and the Chief's directive to conduct an audit of the two pagers with the greatest overages (when Lieutenant Duke

stopped his practice). See pp. 3-4, *supra*. A brief period of underenforcement by a single subordinate officer does not detract from the force of a policy. Cf. *Monell* v. *Department of Soc. Servs.*, 436 U.S. 658, 691 (1978) (to "constitute a 'custom or usage' with the force of law," a practice must be "permanent and well settled") (quoting *Adickes* v. *S.H. Kress & Co.*, 398 U.S. 144, 168 (1970)).

c. Tying Fourth Amendment protection to representations made, expressly or implicitly, by lower-level employees would severely compromise a government employer's ability to safeguard its network or investigate its employees' on-the-job activities. Because auditors often will not know about these representations, they will not be able to assess whether their behavior comports with the Fourth Amendment. To take an obvious and likely example, investigators might rely on a monitoring policy in requesting an audit, only to learn later that a help-desk staffer had nullified that policy orally. The uncertainty that the court of appeals' unprecedented rule would yield may create a powerful disincentive to conduct searches even when clearly authorized by official workplace policy. And under that rule, any search authorized by an official policy may well become the subject of lengthy, fact-intensive litigation. If any non-policymaking employee can negate an official policy by the kinds of actions that Lieutenant Duke took here, then a government's compliance with such an official policy will not suffice to support a search.

B. The Search Was Not Rendered Unreasonable Merely Because It Examined Content

After holding that Quon had a reasonable expectation of privacy in his text messages, the court of appeals concluded that the search was unreasonable in scope be-

cause there were "less intrusive methods" available. Pet. App. 35 (citation omitted). Whether or not the panel (as Judge Ikuta contended and Judge Wardlaw denied) required the use of the *least* intrusive means,[8] the panel clearly held that if the City could achieve its desired goal without looking at Quon's private messages, the City was required to do so. See *id.* at 35-36. That analysis is inconsistent with *O'Connor* and with this Court's other cases.

The Fourth Amendment's "special needs" doctrine does not impose a rigid distinction between "private material" and "other material."[9] As Justice O'Connor explained in *O'Connor*, the scope of a search is to be assessed by looking at the government's legitimate need, 480 U.S. at 726 (plurality opinion); accord *id.* at 732 (Scalia, J., concurring in the judgment), not just at the "private" nature of the material uncovered. The court of appeals' decision is in tension with this approach; indeed, under the court of appeals' reasoning, the *O'Connor* Court would not have needed to remand to the Ninth Circuit, because the search at issue in that case indisputably encompassed several of Dr. Ortega's personal items. See *id.* at 713-714 (plurality opinion).

Properly understood, the Fourth Amendment's special-needs doctrine requires only that the purpose of the search be legitimate and that the scope be reasonably related to its object. *O'Connor*, 480 U.S. at 726

---

[8] Judge Ikuta was correct in pointing out that this Court has definitively ruled out the notion that a "special needs" search requires use of the least restrictive means. Pet. App. 145 (citing, inter alia, *Board of Educ.* v. *Earls,* 536 U.S. 822, 837 (2002)).

[9] To be sure, if an inspection does not trench on a reasonable expectation of privacy at all, then the Fourth Amendment is not implicated.

(plurality opinion) (citing *New Jersey* v. *T.L.O.*, 469 U.S. 325, 342 (1985)); accord, *e.g.*, *Michigan Dep't of State Police* v. *Sitz*, 496 U.S. 444, 455 (1990). That standard is amply met in this case. As this Court has recognized, "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* v. *Railway Labor Executives Ass'n*, 489 U.S. 602, 629 n.9 (1989) (brackets in original) (quoting *United States* v. *Montoya de Hernandez*, 473 U.S. 531, 542 (1985)). But here, the imagined means that the panel offered all depended on Quon's accurate and timely cooperation, see Pet. App. 35-36, which the City could reasonably think would not be forthcoming. And the actual means that the City used was appropriately limited in scope in view of its object; indeed, it involved review limited to a single billing period. *Id.* at 54.

C. Because The City Validly Obtained Messages Delivered To Quon, The Authors Of Those Messages Suffered No Constitutional Injury

Because the City did not violate Quon's Fourth Amendment rights in obtaining the text messages from the Arch account for Quon's City-issued pager, individuals who sent those text messages to Quon likewise have no claim. The panel erred by concluding that senders retained a privacy interest in those text messages once delivered. Like a letter-writer or a gift-giver, a text-message-sender loses a cognizable privacy interest once the message reaches the recipient, because other people can lawfully obtain the message from the recipient. The question with respect to Trujillo, Florio, and Jerilyn Quon therefore is not whether "users of text messaging

services * * * have a reasonable expectation of privacy in their text messages stored on the service provider's network," Pet. App. 24. Rather, it is whether *senders* of text messages have a reasonable expectation of privacy in their text messages once they arrive at their destination. They do not.[10]

1. The City did not request the transcript of Quon's text messages until a few days after the relevant billing period had ended. Accordingly, it did not intercept real-time messages queued for delivery to Quon; it received transcripts only of messages that Quon had already sent or received. Although both the panel and respondents emphasize that the City obtained the messages from Arch rather than from Quon, the difference is immaterial: once each message was delivered, the City could have gained access to it by requiring Quon to hand over his City-issued pager and reading that message in the pager's memory.[11] Any distinction between those two methods of retrieving the identical information is constitutionally irrelevant. Cf. *Smith*, 442 U.S. at 744-745 (caller had no expectation of privacy in phone number dialed, regardless whether that information was remem-

---

[10] Senders who retain a copy of each message they send may have an expectation of privacy in those copies, depending on where and how the copies are stored. Quon's copies of messages he sent were stored on the City's paging system, and he therefore had no expectation of privacy in his sent messages, for the reasons discussed above.

[11] The record does not disclose whether Quon deleted any of the relevant text messages from his handheld pager. But the Policy warned him that "[d]eletion of * * * electronic information may not fully delete the information from the system." Pet. App. 153. And in any event, the length of time that Quon chose to store a particular message on his handheld pager is irrelevant to whether Jerilyn Quon, Florio, or Trujillo had a reasonable expectation of privacy in the message once transmitted.

bered by a human operator, recorded in the phone company's billing records, or captured by a pen register).

Moreover, the City could retrieve messages from Arch only to the extent they were sent through a City-issued pager. See Pet. App. 8-9. Florio and Jerilyn Quon, for instance, had pagers that were *not* paid for by the City, C.A. Supp. E.R. 303, 307, and the City could not have obtained (and did not try to obtain) the transcripts of messages between them alone. Thus, the City obtained messages from Jerilyn Quon, Florio, and Trujillo only because those messages were in Quon's possession, through his City-issued pager.[12]

2. Because the City obtained the messages from the Arch account for Quon's pager, and did so in a manner consistent with the Fourth Amendment (see Parts A and B, *supra*), it did not invade any cognizable Fourth Amendment right of the three other respondents. Once a message is received—whether via paper or electronically—the sender no longer has a reasonable expectation under the Fourth Amendment that it will be kept confidential.[13] Although other sources of law (such as evidentiary privileges) may protect a message even once it reaches the hands of the recipient, the sender no longer has a constitutional right to insist that the message remain private.

---

[12] The City could separately have obtained messages sent through Trujillo's City-issued pager, but did not.

[13] Indeed, the court of appeals recognized that "[a]bsent an agreement to the contrary, Trujillo, Florio, and Jerilyn Quon had no reasonable expectation that Jeff Quon would maintain the private nature of their text messages." Pet. App. 28.

This Court has long held that when one person voluntarily discloses information to another,[14] the first person loses any cognizable interest under the Fourth Amendment in what the second person does with the information. See *United States* v. *Miller*, 425 U.S. 435, 443 (1976); *Couch* v. *United States*, 409 U.S. 322, 325 (1973); *White*, 401 U.S. at 752 (plurality opinion); *Hoffa* v. *United States*, 385 U.S. 293, 302-303 (1966). For Fourth Amendment purposes, the same principle applies whether the recipient intentionally makes the information public or hands it over as part of a constitutionally reasonable search. Thus, when Quon received text messages from the other three respondents addressed to his government pager, these three senders assumed the risk that Quon would give those messages to the police; leave them somewhere freely accessible to the police; or place them somewhere subject to a constitutionally valid search. If the City could constitutionally obtain messages from Quon (or from the Arch account of Quon's pager), that ends the analysis: the Fourth Amendment does not give greater protection to messages Quon received from the respondents than it does to Quon's retained copies of messages he sent himself.

In these respects, text messages are no different from letters or e-mails. (The panel recognized this similarity but not the consequences of it.) Although the Fourth Amendment protects sealed letters in transit, "if a letter is sent to another, the sender's expectation of

---

[14] "Another" refers to an ultimate recipient, not (for example) a commercial carrier. See *United States* v. *Jacobsen*, 466 U.S. 109, 114 (1984). Thus, for instance, no party has argued in this case that respondents lost all expectation of privacy the moment their messages were passed to Arch for delivery—only that they had no expectation of privacy once Quon received the messages.

privacy ordinarily terminates upon delivery." *United States* v. *King*, 55 F.3d 1193, 1196 (6th Cir. 1995) (citations omitted). The same rule applies to e-mail users, who lack "a legitimate expectation of privacy in an e-mail that had already reached its recipient." *Guest* v. *Leis*, 255 F.3d 325, 333 (6th Cir. 2001). See also *SEC* v. *Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."); *United States* v. *Heckencamp*, 482 F.3d 1142, 1146 (9th Cir.) (an "expectation of privacy may be diminished" for "transmissions over the Internet or e-mail that have already arrived at the recipient") (citation omitted), cert. denied, 552 U.S. 1023 (2007).

The panel erred in holding that the government cannot obtain a text message without the consent of either the sender or the recipient. Consent is not the only way the City could validly obtain the messages involved in this case, just as consent is not the only way police officers may enter a home or search a container. In this case, because the messages were sent to Quon's City-provided pager, the City validly obtained these messages pursuant to a workplace search. The other respondents had no further rights in those messages.

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

ELENA KAGAN
Solicitor General
LANNY A. BREUER
Assistant Attorney General
NEAL KUMAR KATYAL
Deputy Solicitor General
WILLIAM M. JAY
Assistant to the Solicitor General
JOSH GOLDFOOT
VIJAY SHANKER
Attorneys

FEBRUARY 2010