#### No. 08-1332

# In the Supreme Court of the United States

CITY OF ONTARIO, CALIFORNIA, ET AL.,

Petitioners,

v.

JEFF QUON, ET AL.,

Respondents.

On Writ Of Certiorari To The United States Court Of Appeals For The Ninth Circuit

BRIEF OF ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, AMERICAN CIVIL LIBERTIES UNION, AND PUBLIC CITIZEN AS *AMICI CURIAE* IN SUPPORT OF RESPONDENTS

DAN M. KAHAN SCOTT L. SHUCHART Yale Law School Supreme Court Clinic 127 Wall Street New Haven, CT 06511 (203) 432-4992 ANDREW J. PINCUS Counsel of Record CHARLES ROTHFELD Mayer Brown LLP 1999 K Street, NW Washington, DC 20006 (202) 263-3000 apincus@mayerbrown.com

Counsel for Electronic Frontier Foundation and Center for Democracy & Technology [Additional Counsel Listed on Inside Cover] STEVEN R. SHAPIRO American Civil Liberties Union Foundation 125 Broad Street New York, NY 10004 (212) 549-2500

Counsel for American Civil Liberties Union GREGORY A. BECK Public Citizen 1600 20th Street, NW Washington, DC 20009 (202) 588-7713

Counsel for Public Citizen

## TABLE OF CONTENTS

Pag	e
TABLE OF AUTHORITIESii	ii
SUMMARY OF ARGUMENT	2
ARGUMENT	5
I. THE COURT SHOULD TREAD CAUTIOUSLY IN ADDRESSING THE APPLICATION OF THE FOURTH	
AMENDMENT TO NEW	_
COMMUNICATION TECHNOLOGIES	5
A. Text Messaging and Email Are Rapidly Replacing Traditional Forms of Communication	6
B. The Technology Used To Transmit Text Messages And Email Creates An Expectation Of Privacy As Reasonable As That Associated With Older Forms of Communication	0
C. Employers Typically Permit—And Often Encourage—Employees To Use Employer-Provided Equipment To Transmit Personal Emails And Text Messages	6
D. The Court Should Not Address In This Case The Impact of Employers' Monitoring Policies On Fourth Amendment Protection Against Law Enforcement Access to Private Sector Or Government Employees' Electronic Communications	0
II. THE SEARCH HERE VIOLATED THE FOURTH AMENDMENT STANDARD APPLICABLE TO SEARCHES OF GOVERNMENT WORKPLACES	4

i

# TABLE OF CONTENTS—continued

# Page

A. The <i>O'Connor</i> Plurality Opinion Supplies The Governing Standard	25
B. The Government Employee Respondents Had A Reasonable Expectation Of Privacy In Their Text Messages	27
<ol> <li>Lieutenant Duke's Interpretation Of The Department's Policy, Together With His Settled Practice, Supported A Reasonable Expectation Of Privacy</li></ol>	28
2. The California Public Records Act Does Not Undermine The Employees' Reasonable Expectation Of Privacy	32
C. The Search Of The Text Messages Was Unreasonable In Its Scope	35
D. Because The Search Of The Officers' Text Messages Was Unreasonable, Petitioners Also Violated The Fourth Amendment Rights Of The Private Individuals Who Sent Messages To The	-
Officers	

ii

# TABLE OF AUTHORITIES

Page(s)

## CASES

American Postal Workers Union v.	
U.S. Postal Service,	
871 F.2d 556 (6th Cir. 1989)26	3
Biby v. Board of Regents,	
419 F.3d 845 (8th Cir. 2005)26	3
California State University v. Superior Court,	
108 Cal. Rptr. 2d 870 (2001)33-34	ł
Camara v. Municipal Court,	
387 U.S. 523 (1967)25	5
Chandler v. Miller, 520 U.S. 305 (1997)	2
City of Indianapolis v. Edmond,	
531 U.S. 32 (2000)	3
Denver Publishing Co. v. Board of County	
Commissioners, 121 P.3d 190 (Colo. 2005) 34	ł
Garcetti v. Ceballos, 547 U.S. 410 (2006)	2
Griffis v. Pinal County,	
156 P.3d 418 (Ariz. 2007)	ł
Guest v. Leis, 255 F.3d 325 (6th Cir. 2001)16	
International Federation of Professional &	
Technical Engineers, Local 21, AFL-CIO v.	
Superior Court, 165 P.3d 488 (Cal. 2007)	1
Katz v. United States,	
389 U.S. 347 (1967)6, 36	3
Kyllo v. United States, 533 U.S. 27 (2001)	3
Leventhal v. Knapek,	
266 F.3d 64 (2d Cir. 2001)	)
Mancusi v. DeForte, 392 U.S. 364 (1968)	L

iii

Marshall v. Barlow's, Inc.,
436 U.S. 307 (1978)
Michigan Dep't of State Police v. Sitz,
496 U.S. 444 (1990)22
Narducci v. Moore,
572 F.3d 313 (7th Cir. 2009)26
New Jersey v. T.L.O., 469 U.S. 325 (1985)25
O'Connor v. Ortega, 480 U.S. 709 (1987) passim
Rehberg v. Paulk, No. 09-11897,
2010  WL  816832
(11th Cir. Mar. 11, 2010)16
<i>Reno</i> v. <i>ACLU</i> , 521 U.S. 844 (1997)2
Rogers v. Lodge, 458 U.S. 613 (1982)
Rumsfeld v. Forum for Academic and
Institutional Rights, Inc.,
547 U.S. 47 (2006)
Smith v. Maryland, 442 U.S. 735 (1979)36
Stewart v. Evans,
351 F.3d 1239 (D.C. Cir. 2003)27
Tiberino v. Spokane County,
13 P.3d 1104 (Wash. Ct. App. 2000)
Tiffany Fine Arts, Inc. v. United States,
469 U.S. 310 (1985)
United States v. Angevine,
281 F.3d 1130 (10th Cir. 2002)26-27
United States v. Esser,
284 Fed. Appx. 757 (11th Cir. 2008)27
United States v. Jacobsen, 466 U.S. 109 (1984) 11

United States v. Johnson,	
16 F.3d 69 (5th Cir. 1994)	
United States v. Lifshitz,	
369 F.3d 173 (2d Cir. 2004)	16
United States v. Mancini,	
8 F.3d 104 (1st Cir. 1993)	
United States v. Simons,	
206 F.3d 392 (4th Cir. 2000)	
United States v. Taketa,	
923 F.2d 665 (9th Cir. 1991)	
STATUTES	
5 U.S.C. § 552	
18 U.S.C.	
§ 2510	
§ 2702	
§ 2703	· · ·
44 U.S.C. § 2201	
Quifernia Querrante Qui	

California Government Code	
§ 6250	
§ 6254	

## **OTHER AUTHORITIES**

Jay Akasie, 'Addiction' to BlackBerries May	
Bring on Lawsuits, The Sun (N.Y.),	
Sept. 7, 2006	17-18
American Management Association, The	
Latest on Workplace Monitoring and	
Surveillance, Mar. 13, 2008,	
http://tinyurl.com/yjb4q4a	23

v

# Page(s)

Associated Press, Obama Wants Company Cell
Phone Tax Repealed, MSNBC News, Jan.
31, 2010, http://www.msnbc.msn.com/id/
35169772/ns/business-personal_finance/18, 19
Bender's Payroll Tax Guide (2010)19
Stephen J. Blumberg & Julian Luke, Wireless
Substitution: Early Release of Estimates
From the National Health Interview
Survey, CDC National Center for Health
Statistics, July-December 2008,
http://tiny.cc/cdcnihstats7
Press Release, CTIA, The Wireless Association
Announces Semi-Annual Wireless Industry
Survey Results (Oct. 7, 2009),
http://www.ctia.org/media/press/body.cfm/
prid/1870
•
Editorial, The IRS Phones Home, Wall St. J.,
June 16, 200917
Jennifer Stisa Granick & Kurt Opsahl,
Taking Reality Into Account,
N.Y. Times, Dec. 21, 2009,
http://roomfordebate.blogs.nytimes.com/
2009/12/21/your-boss-and-your-
blackberry/17, 18
Harris Interactive, Harris Poll #36, Cell Phone
Usage Continues to Increase (Apr. 4, 2008),
http://www.harrisinteractive.com/vault/Har
ris-Interactive-Poll-Research-Cell-Phone-
Usage-Continues-to-Increase-2008-04.pdf
Kim Hart, IRS Asked to Repeal Cell Phone
<i>Tax</i> , The Hill, Sept. 6, 2009
- and - in Septi 0, =0000 minimum 10

# Page(s)

Internal Revenue Service, Notice 2009-46, Substantiating Business Use of Employer- Provided Cell Phones (June 8, 2009), available at http://www.irs.gov/irb/2009- 23_IRB/ar07.html
Internal Revenue Service, Statement of IRS
Commissioner Doug Shulman, June 16, 2009, http://tinyurl.com/IRSstatement20
Tom Kaneshige, <i>Haiti Donations: A Turning</i> <i>Point in Mobile Commerce</i> ?, CIO (Feb. 10, 2010), http://www.cio.com/article/
538513/Haiti_Donations_A_Turning_Point _in_Mobile_Commerce9
Timothy B. Lee, <i>Snooping Isn't the Answer</i> , N.Y. Times, Dec. 21, 2009, http://roomfordebate.blogs.nytimes.com/ 2009/12/21/your-boss-and-your- blackberry/
Helen Leggatt, U.S. Teens Texting Ten Times Per Hour, Bizreport, Feb. 9 2010, http://www.bizreport.com/2010/02 /us_teens_texting_ten_times_per_
hour.html
Over the Past Five Years: Pew Internet
Looks Back (Aug. 19, 2009),
http://www.pewinternet.org/Reports/2009/1 4Teens-and-Mobile-Phones-Data-
Memo.aspx7

# Page(s)

National Federation of Independent Business, 411 Small Business Facts: Telecommunica-
tions, http://www.411sbfacts.com/sbpoll- about.php?POLLID=002216-17
Osterman Research, Inc., <i>Mobile Messaging</i> <i>Market Trend, 2008-2011</i> , Oct. 2008, <i>available at</i> http://tinyurl.com/ markettrends2008-2011
Pew Research Center, Internet, Broadband, and Cell Phone Statistics, http://www.pewinternet.org/Reports/2010/I nternet-broadband-and-cell-phone- statistics.aspx
Press Release, The Radicati Group, Inc., Email Statistics Report, 2009-2013 (May 6, 2009), <i>available at</i> http://tinyurl.com/emailstatistics10
Marguerite Reardon, Americans Text More Than They Talk, CNET, Sept. 22, 2008, http://tiny.cc/CNET
S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555
John Schulze, Jr., <i>Technology Has Created the</i> <i>Perpetual Workplace</i> , 34, For the Defense, Oct. 2009, http://www.dri.org/(S(r4hiuj45mjaudwyvspj
tsx3q))/articles/CommercialLitigation/FTD- 0910-Schulze.pdf17
Gemma Simpson, <i>Study: BlackBerry Users</i> <i>More Productive</i> , Silicon.com, July 5, 2007, http://tinyurl/blackberrystudy

# Page(s)

SMS & MMS Outlook Strong; Text Message
Revenues Reaching \$223B by 2014, Qwasi
(Feb. 3, 2010),
http://www.qwasi.com/news/blog/sms-text-
message-revenues-reaching-233b-by-
2014.htm9
Teens Point the Way to Texting Trends
(averaging 2900 txt per month), Qwasi, Oct.
1, 2009, http://www.qwasi.com/news/blog/
teens-point-the-way-to-texting-trends-
averaging-2900-txt-per-month.htm9
Press Release, United States Postal Service,
Postal Service Begins 2010 with First-
Quarter Loss (Feb. 9, 2010),
http://www.usps.com/communications/news
room/2010/pr10_014.htm10
United States Postal Service, Operating
Statistics, http://www.usps.com/
cpim/ftp/ar09html/ar_2_115.htm10
William Webb, Wireless Communications:
<i>The Future</i> (2007)18
Workplace 2.0: The Modern Electronic
Workplace and Issues Faced by Employers,
HR Roundtable (The TemPositions Group
of Companies), May 7, 2009
http://www.tempositions.com/site/hrnews/H
R_Roundtable_May_2009.pdf17

ix

#### INTEREST OF THE AMICI CURIAE1

This case brings before the Court important issues regarding the application of the Fourth Amendment's protection of personal privacy in the context of new communications technologies. *Amici* consist of the following nationwide organizations that seek to preserve individuals' privacy rights, including the protection afforded by the Fourth Amendment:

The Electronic Frontier Foundation (EFF) is a member-supported, non-profit legal foundation that litigates to protect free speech and privacy rights in the digital world. As part of its mission, EFF has often served as counsel or *amicus* in key cases addressing constitutional and statutory rights of privacy in electronic communications.

The Center for Democracy & Technology (CDT) is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the internet and other communications networks. CDT represents the public's interest in an open, decentralized Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty.

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization with over 500,000 members dedicated to the principles of

<sup>&</sup>lt;sup>1</sup> Pursuant to Rule 37.6, *amici* affirm that no counsel for a party authored this brief in whole or in part and that no person other than *amici* or their counsel made a monetary contribution to its preparation or submission. The parties' letters consenting to the filing of this brief have been filed with the Clerk.

liberty and equality embodied in the Constitution and this nation's civil rights laws. Since its founding in 1920, the ACLU has appeared before this Court in numerous cases involving the interpretation of the Fourth Amendment and, more generally, the application of the Constitution to new technologies. See, *e.g.*, *Reno* v. *ACLU*, 521 U.S. 844 (1997).

Public Citizen is a national consumer-advocacy and watchdog organization based in Washington, D.C. Since its founding in 1971, Public Citizen has argued as counsel and as *amicus curiae* for the privacy rights of consumers. Public Citizen has also represented government employees in cases involving the intersection of the Constitution and the government's authority as an employer, including *Garcetti* v. *Ceballos*, 547 U.S. 410 (2006).

#### **SUMMARY OF ARGUMENT**

1. Communication in America is in the midst of a technological revolution. Information that individuals formerly conveyed in oral conversations (either face-to-face or over the telephone) or in letters or other physical correspondence is now routinely transmitted using text messages or emails.

This case presents the Court with one of its first opportunities to address the application of the Fourth Amendment to private information conveyed via these new mediums of communications. Given the technological complexity of the context, and the extremely significant implications for continued protection under the Fourth Amendment of Americans' most private communications, the Court should proceed cautiously and limit its decision to the specific factual circumstances presented here. To begin with, the technology used to transmit text messages and email creates an expectation of privacy that is just as reasonable as that associated with the more traditional modes of communication that are being replaced. The processes of sending the communications are similar, and the actual chances that a message will be read by someone other than the sender and recipient are infinitesimal in each situation. Moreover, Congress enacted the Stored Communications Act to reinforce the privacy of the content of electronic written communications—a factor that plainly supports the reasonableness of users' privacy expectations.

The factual circumstances of this case—in which an employee used an employer-provided communications device to send electronic written communications—are not at all unique. Many employers, both governmental and private, provide communications devices to their employees. And they permit, and often encourage, employees to use those devices for personal as well as business communications. That is because the more the employee uses the device away from the office, the more accessible the employee is for after-hours work assignments—and the greater the benefit to the employer. The mixed personal and professional use of company-provided devices is an essential tool for transacting business in the information age.

Petitioners argue that the Police Department's policy applicable to employees' internet use vitiates any reasonable expectation of privacy on the part of respondents. That argument is wrong on the merits. But to the extent the Court addresses the argument, it should make clear that its analysis applies only in the context of government workplace searches. A private employer's policy permitting the employer to access messages transmitted on company-provided devices does not affect in any way the employee's reasonable expectation that the messages will remain inaccessible to the government. And whatever authority the government may have to monitor employee communications in its role as employer is limited to that context, and does not apply to law enforcement searches.

2. The legal framework for deciding this case is provided by the plurality opinion in *O'Connor* v. *Ortega*, 480 U.S. 709 (1987). The threshold question is whether both courts below correctly determined that Officer Quon had a reasonable expectation of privacy in the content of the text messages. Those holdings are correct.

Both lower courts found as a fact that petitioners' written internet use policy did not encompass text messaging. Petitioners' sole support for their contention that the policy did apply to text messaging is Lieutenant Duke's testimony that he informed members of the Police Department that pager messages would fall within the policy. But the very same Lieutenant Duke established the informal policy and practice that text messages would not be reviewed as long as employees paid any overage charges-the policy and practice that support Officer Quon's reasonable expectation of privacy. Because petitioners themselves rely on the authoritative nature of some of Lieutenant Duke's statements, they cannot dispute the authoritative status of the statements and actions of the same individual relied upon by respondents.

The search here did not comply with O'Connor's requirement that a government workplace search

must be reasonably related to the goals of the search and not "excessively intrusive." 480 U.S. at 726. The reason for the search was to determine whether police officers were being required to pay for workrelated messages. Several obvious alternative approaches—for example, asking officers to identify work-related text messages in excess of the existing monthly character allotment—would have enabled petitioners to fulfill their purpose without intruding on the sensitive privacy interests protected by the Fourth Amendment.

#### ARGUMENT

#### I. THE COURT SHOULD TREAD CAU-TIOUSLY IN ADDRESSING THE APPLICA-TION OF THE FOURTH AMENDMENT TO NEW COMMUNICATION TECHNOLOGIES.

Mobile communications devices—including cellular phones, pagers, and combination devices known as smartphones—have rapidly become ubiquitous. Unlike traditional ("landline") telephones, these new devices are not limited to transmitting oral conversations; they also enable users to exchange written communications through the extremely popular medium of text messages.

Increased access to the internet in homes and offices, as well as through mobile devices such as the Blackberry and iPhone, is also producing an explosion in electronic written communication via email. These new technologies are combining to displace landline telephones, letters, and even face-to-face interaction as dominant means of communication.

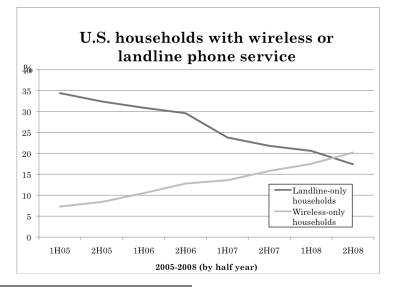
Although these new media are now a part of everyday life for most Americans, the courts have had few opportunities to address the extent to which the Fourth Amendment limits governments' ability to access citizens' private communications effected via these new technologies. These questions are complex, turning on the application of settled legal principles in new and technologically complex contexts. *Cf. Kyllo* v. *United States*, 533 U.S. 27, 34 (2001) (refusing to "permit police technology to erode the privacy guaranteed by the Fourth Amendment").

This Court accordingly should proceed with caution, and take care to limit its decision here to the specific factual situation before it. The Court's ruling otherwise could have unjustified and unintended, but extremely significant, implications for the continued protection under the Fourth Amendment of Americans' most private communications, which increasingly are conducted using these new technologies. Compare Katz v. United States, 389 U.S. 347, 355 (1967) (overturning prior holding in Olmstead v. United States, 277 U.S. 438 (1928), regarding application of Fourth Amendment to telephone conversations); id. at 362 (Harlan, J., concurring) (observing that the Court's prior requirement of physical penetration of a premises to establish a Fourth Amendment violation "is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion").

#### A. Text Messaging and Email Are Rapidly Replacing Traditional Forms of Communication.

Cell phones and similar mobile communication devices have become omnipresent. A 2009 survey

found that 85% of adults owned a mobile phone.<sup>2</sup> Approximately nine out of ten adults use a mobile phone and one in seven adults owns *only* a mobile phone.<sup>3</sup> Furthermore, 14.5% of American homes received "all or almost all" calls on wireless telephones, even if there also was a landline telephone in the house. Stephen J. Blumberg & Julian Luke, *Wireless Substitution: Early Release of Estimates From the National Health Interview Survey*, CDC National Center for Health Statistics, July-December 2008, http://tiny.cc/cdcnihstats. The chart below demonstrates the extent to which wireless-only homes are surpassing landline-only households. *Ibid*.



<sup>2</sup> See Amanda Lenhart, *Teens and Mobile Phones Over the Past Five Years: Pew Internet Looks Back* (Aug. 19, 2009), http://www.pewinternet.org/Reports/2009/14--Teens-and-Mobile-Phones-Data-Memo.aspx.

<sup>3</sup> See Harris Interactive, Harris Poll #36, Cell Phone Usage Continues to Increase (Apr. 4, 2008), http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Cell-Phone-Usage-Continues-to-Increase-2008-04.pdf. Landline telephones are limited to voice communication, but mobile phones offer opportunities for written communication and sharing of photo and video messages. Text messaging, also known as "SMS" (short message service) or "texting," uses cell phones or pagers to send and receive electronic written messages.

Texting, along with the related services for transmitting photos and videos between phones, has become an extremely popular form of communication, with an average of 4.1 billion text messages sent and received in the nation *each day*. See Press Release, CTIA, The Wireless Association Announces Semi-Annual Wireless Industry Survey Results (Oct. 7, 2009), http://www.ctia.org/media/press/body.cfm/ prid/1870.

Many Americans today use text messages to convey information that formerly would have been the subject of an oral telephone conversation. According to a 2008 Nielson Mobile survey, U.S. mobile subscribers "sent and received on average 357 text messages per month [in the second quarter of 2008], compared with making and receiving 204 phone calls a month \*\*\*. The new statistic clearly indicates that Americans have jumped onto the SMS text bandwagon." Marguerite Reardon, *Americans Text More Than They Talk*, CNET, Sept. 22, 2008, http://tiny.cc/CNET.

Indeed, political and humanitarian campaigns now utilize text-messaging as a preferred method for reaching supporters. After the devastating earthquake in Haiti in January 2010, the American Red Cross raised \$7 million in two days from individuals donating \$10 each through text-messaged donations over wireless networks. The "magic," as media analyst Jeff Roster termed it, was the ease of being able to support a distant place in need through a simple and quick text message. "People are comfortable with text messaging," he says. "Texting is the form of communication for the next generation."<sup>4</sup>

Text-message use is expected to continue to surge. One study estimated that there were 5 trillion SMS texts sent worldwide in 2009 and that there will be more than 10 trillion SMS texts sent worldwide in 2013. SMS & MMS Outlook Strong; Text Message Revenues Reaching \$223B by 2014, Qwasi (Feb. 3, 2010), http://www.qwasi.com/news/blog/smstext-message-revenues-reaching-233b-by-2014.htm.<sup>5</sup>

The data regarding use of email is similarly dramatic. An estimated 74% of adults use the internet. Pew Research Center, *Internet, Broadband, and Cell Phone Statistics,* http://www.pewinternet.org/ Reports/2010/Internet-broadband-and-cell-phonestatistics.aspx. The number of non-spam emails sent

<sup>&</sup>lt;sup>4</sup> Tom Kaneshige, *Haiti Donations: A Turning Point in Mobile Commerce?*, CIO (Feb. 10, 2010), http://www.cio.com/article/538513/Haiti\_Donations\_A\_Turning\_Point\_in\_Mobile\_Commerce\_.

<sup>&</sup>lt;sup>5</sup> Text messaging is a particularly prevalent form of communication among young people. One study found that American teenagers sent, on average, "10 texts per hour that they're awake and not in school. That's an average of 3,146 per month." Helen Leggatt. U.S. Teens Texting Ten Times Per Hour. Bizreport. 2010,http://www.bizreport.com/2010/02 Feb. 9 /us\_teens\_texting\_ten\_times\_per\_hour.html. While the number of calls sent and received by mobile-phone using teenagers is remaining constant (and relatively low) the number of text messages is sky-rocketing. See Teens Point the Way to Texting Trends (averaging 2900 txt per month), Qwasi, Oct. 1, 2009, http://www.gwasi.com/news/blog/teens-point-the-way-totexting-trends-averaging-2900-txt-per-month.htm.

worldwide per day reached an estimated 47 billion in 2009. Press Release, The Radicati Group, Inc., Email Statistics Report, 2009-2013, at 1 (May 6, 2009), *available at* http://tinyurl.com/emailstatistics.

Text messaging and email are not substituting only for oral telephone conversations. The increase in the use of these new technologies has been accompanied by a corresponding decline in the use of traditional mail. The number of pieces of first-class mail handled by the Postal Service has declined on an accelerating basis over the past four years—the reduction was 1.8% from 2006 to 2007; 4.8% from 2007 to 2008; and 8.6% from 2008 to 2009. United States Postal Operating Service. Statistics. http://www.usps.com/cpim/ftp/ar09html/ar 2 115.htm. For the first quarter of 2010, the decline in total mail volume amounted to an additional 9.0% compared to the first quarter of 2009. Press Release, United States Postal Service, Postal Service Begins 2010 with First-Quarter Loss (Feb. 9. 2010). http://www.usps.com/communications/newsroom/201 0/pr10\_014.htm.

The data thus establish a clear shift in Americans' private communications from traditional media—physical mail and oral telephone conversations—to text messages and email messages.

B. The Technology Used To Transmit Text Messages And Email Creates An Expectation Of Privacy As Reasonable As That Associated With Older Forms of Communication.

Text messaging and email utilize new forms of technology to transmit written communications from one individual to another, but the characteristics of those technologies give rise to expectations of privacy in the senders and recipients of such messages that are virtually identical to, and just as reasonable as, the privacy expectations associated with messages transmitted via more traditional communications media.

*First*, the sending of electronic written communications from one device to another—whether text messages via phones or email messages via computers or smartphones—resembles the process for sending physical letters. The sender composes a message and transmits it to the recipient, retaining a copy for himself. The recipient receives an electronic copy of the message, which he may retain or (at least for email) transform into a physical document by printing out the message.

Senders and recipients of physical written communications have reasonable expectations of privacy in information contained in those documents. United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Illetters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy"). That is true notwithstanding the fact that letters and packages may be opened by persons other than the recipient either intentionally or unintentionally—including for legitimate reasons (e.g., because they are misdelivered or damaged in transit or because the address becomes illegible) or for illegitimate reasons (e.g., malfeasance by postal employees or by neighbors or others interfering with the proper delivery of those messages).6

<sup>&</sup>lt;sup>6</sup> The same is true of oral telephone conversations, which may be accessed by employees of communications carriers as well as

The senders and recipients of electronic written communications have a similar expectation of privacy. Although it is technically possible for the electronic written communication to be viewed by a person other than the recipient—such as an employee of one of the entities providing transmission or delivery services—the actual chances are infinitesimal that such an interception will occur with respect to any of the billions of emails or text messages sent each day.

In the electronic context, the process of transmission may create copies of the message on the servers operated by one or more providers of services enabling the transmission and delivery of the electronic written communication. And those copies are accessible by the entities supplying the transmission services. But Congress has specifically reinforced users' reasonable expectations of privacy by strictly regulating—through the use of criminal sanctions access to and distribution of the contents of electronic written communications.

The Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, bars anyone providing an "electronic communication service"—which is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications," *id.* § 2510(15)—from divulging the contents of communications in electronic storage to anyone other than the "addressee or intended recipient of such communication," *id.* § 2702(a)(1) & (b)(1), with very limited specified exceptions. Significantly, government entities may compel disclosure of the content of

by other persons—from family members or co-workers listening on other extensions, to those using more surreptitious means.

a communication only through a warrant, court order, or subpoena. Id. § 2703(a) & (b).

Congress enacted this statute to "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555. It pointed out that

[w]hen the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the fourth amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions.

*Id.* at 1-2. Existing law, Congress found, was "'hopelessly out of date.' It has not kept pace with the development of communications and computer technology. Nor has it kept pace with changes in the structure of the telecommunications industry." *Id.* at 2 (citation omitted). The Stored Communications Act fills this gap by ensuring protection of Americans' privacy in the context of these new communications technologies.

Indeed, the court below relied on this statute in holding that the company providing text messaging services to the Department violated the Act by turning over the text message transcripts to the City. Pet. App. 20-21. That holding—which this Court declined to review—makes clear the strong support for Officer Quon's reasonable expectation of privacy that results from the congressional enactment.

For all of these reasons, senders and recipients of electronic written communications have a reasonable expectation of privacy—grounded in the nature of the technology and in statutes enacted by Congress—with respect to the contents of those messages.

Second, the sending of a written communication—whether physical or electronic—does not eliminate the sender's reasonable expectation of privacy in any copy of the communication that he retains. To be sure, once a communication is sent, the sender no longer exercises exclusive control over the message's contents: The recipient may choose voluntarily to disclose the copy of the letter that he received. Or the government may compel the recipient to disclose the delivered copy of the communication through means that comply with the Fourth Amendment's reasonableness requirement (which would apply because a recipient of a written electronic communication who did not disclose the message's contents would have a reasonable expectation of privacy in those contents).

But the government cannot without a showing of probable cause—or satisfying any other applicable Fourth Amendment reasonableness standard compel an individual (or a business) to disclose retained copies of sent correspondence. If sending a communication completely vitiated the sender's reasonable expectation of privacy, then the Fourth Amendment would not preclude the government from demanding such documents routinely from anyone without *any* particularized suspicion whatever. And it cannot be argued that a different rule should apply with respect to the sender or recipient's retained copies of electronic communications because the transmission and delivery process creates additional copies of the message—Congress in the Stored Communications Act has tightly regulated disclosure by persons possessing such copies in a manner that enhances the reasonableness of the sender's and recipient's expectations of privacy in any copies of the email or text messages that they retain. Just as the sender of a physical letter has a reasonable expectation of privacy in his retained copy of that letter, senders of electronic communications have an expectation of privacy in retained email and text messages.

*Third*, to the extent an electronic written communication is not disclosed voluntarily by either the sender or recipient, the Stored Communications Act confers on both parties to the communication a reasonable expectation of privacy with respect to copies of the message retained by entities providing services related to the sending, transmission, or receipt of the message. After all, that statute's very purpose is to prevent (with extremely limited exceptions) the disclosure of the contents of electronic communications in the absence of the consent of the parties to the communication. Its effect is to give those individuals a reasonable expectation that their communication will remain private unless one of them decides to reveal it.<sup>7</sup>

<sup>&</sup>lt;sup>7</sup> One lower court recently espoused the expansive, and in our view erroneous, principle that the sender of an electronic written communication can have no reasonable expectation of privacy with respect to the copy of the communication that is in

#### C. Employers Typically Permit—And Often Encourage—Employees To Use Employer-Provided Equipment To Transmit Personal Emails And Text Messages.

Text messaging and email are not only staple tools of personal communication, but of business communication as well.

Nearly a quarter of the private workforce uses employer-provided mobile devices. See Osterman Research, Inc., Mobile Messaging Market Trends, 2008-2011. Oct. 2008.available athttp://tinyurl.com/markettrends2008-2011. That figure continues to grow. By the middle of 2010, almost 40% of corporate employees are expected to use mobile devices provided by their employers. See *ibid*. And the use of such devices is no longer confined to major companies. As the price of mobile devices plummeted, the use of such devices in smaller entities has skyrocketed. Mobile devices now play a vitally important role in American small businesses. Indeed, "seventy-eight percent of small business owners use a cell-phone for business purposes." Nat'l

the hands of the service provider. *Rehberg* v. *Paulk*, No. 09-11897, 2010 WL 816832 (11th Cir. Mar. 11, 2010). This mistaken conclusion is based on a misreading of two much more limited decisions—*United States* v. *Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) ("special needs" of the probation system may render a computer monitoring condition reasonable), and *Guest* v. *Leis*, 255 F.3d 325, 333 (6th Cir. 2001) (no expectation of privacy in messages sent to a public bulletin board system visited by FBI agent). As discussed in the text, it is true that the sender cannot prevent the recipient from voluntarily disclosing the contents; but in the absence of such a voluntary disclosure, the sender retains an expectation of privacy in the copies of the communications retained by the sender and by a service provider.

Fed. of Indep. Bus., 411 Small Business Facts: Telecommunications, http://www.411sbfacts.com/sbpollabout.php?POLLID=0022.

The proliferation of mobile devices has produced a significant benefit for businesses, "mak[ing] sure that employees are only a click or a call away from work at all times." John Schulze, Jr., *Technology Has Created the Perpetual Workplace*, 34, For the Defense, Oct. 2009, http://www.dri.org/ (S(r4hiuj45mjaudwyvspjtsx3q))/articles/Commercial Litigation/FTD-0910-Schulze.pdf. Employees with employer-provided devices "are expected to remain tethered to the office 24-7." Editorial, *The IRS Phones Home*, Wall St. J., June 16, 2009.<sup>8</sup>

A corporate executive can now be just as engaged in work-related activity while standing in line at the grocery store or attending a baseball game as she is when sitting at her office desk. Surveys showcase this new reality. For instance, some "37% of mobile users check their mobile email [on their handheld device] more than 10 times each day. Even on the weekend, 47% of mobile users check their mobile email more than 10 times per day." See Osterman Research, *supra*, at 2. And 76% of employees with a mobile device "always" bring it with them on vacations. *Ibid.*; see also Jay Akasie, 'Addiction' to Black-Berries May Bring on Lawsuits, The Sun (N.Y.),

<sup>&</sup>lt;sup>8</sup> See also Jennifer Stisa Granick & Kurt Opsahl, Op-ed, *Taking Reality Into Account*, N.Y. Times, Dec. 21, 2009, http://roomfordebate.blogs.nytimes.com/2009/12/21/your-boss-and-your-blackberry/; *Workplace 2.0: The Modern Electronic Workplace and Issues Faced by Employers*, HR Roundtable (The TemPositions Group of Companies), May 7, 2009, at 3, http://www.tempositions.com/site/hrnews/HR\_Roundtable\_May \_2009.pdf.

(N.Y.), Sept. 7, 2006. Smartphone users accordingly "tend to put in more hours than [the] average employee" without such a device. See Gemma Simpson, *Study: BlackBerry Users More Productive*, Silicon.com, July 5, 2007, http://tinyurl/blackberrystudy.

Given that employees carry their employerprovided devices with them at all times, it is only natural that they use them to facilitate both personal and business communications. "[W]orkers increasingly use company-issued mobile devices for texting, e-mailing and browsing the Internet—sometimes for work, sometimes for personal use." Associated Press, Obama Wants Company Cell Phone Tax Repealed. **MSNBC** News. Jan. 31.2010.http://www.msnbc.msn.com/id/35169772/ns/businesspersonal\_finance/. Employees rely on their employerprovided devices to manage their personal lives as well as their professional ones. See, e.g., Granick & Opsahl, supra note 8; William Webb, Wireless Com*munications: The Future* 15:13 (2007). Even employers whose policies nominally prohibit the personal use of company devices "frequently turn a blind eye to employees engaging in personal activities 'on the clock" because of the substantial economic benefits they gain from personal use of these employerprovided facilities. See Timothy B. Lee, Snooping Isn't the Answer, N.Y. Times, Dec. 21, 2009, http://roomfordebate.blogs.nytimes.com/2009/12/21/y our-boss-and-your-blackberry/.

The practice of managing personal activities on one's "work" phone has thus become routine for millions of employees. It represents "one side of a *quid pro quo*: the same employee who spends an afternoon ordering Christmas presents on Amazon.com may be expected to take time away from his family to deal with a weekend emergency at work." *Ibid*. Encouraging or allowing the personal use of company-provided communications devices produces significant business advantages, incentivizing employees to employ their devices ever more *frequently*, and thus to be ever more available—and willing—to attend to business tasks, in addition to personal ones.

A recent controversy involving the taxation of personal use of employer-provided devices demonstrates the degree to which employers accept, and even encourage, the personal use of companyprovided mobile devices. Under a provision of the Internal Revenue Code enacted in 1989, the value of personal use of employer-provided cell phones must be included in an employee's taxable income unless the employer or employee maintains detailed records distinguishing between personal and business calls. Internal Revenue Service, Notice 2009-46, Substantiating Business Use of Employer-Provided Cell 2009). Phones (June 8. available athttp://www.irs.gov/irb/2009-23 IRB/ar07.html. The IRS issued a notice in 2009 requesting comments on several proposed reforms to the law's reporting requirements. Ibid.

This request for comment generated uniform opposition to the reporting requirement. See, *e.g.*, 1-4 Bender's Payroll Tax Guide § 4.340 (2010); Associate Press, *Obama Wants, supra*. The clear message: "[C]ell phones are so ubiquitous and have become such an essential business tool that it's nearly impossible to keep track of the line between professional and personal use." Kim Hart, *IRS Asked to Repeal Cell Phone Tax*, The Hill, Sept. 6, 2009.

Only days after requesting public comment on the regulatory proposal, IRS Commissioner Doug Shulman and Treasury Secretary Timothy Geithner called on Congress to repeal the law outright. See Internal Revenue Service, Statement of IRS Commissioner Doug Shulman. June 16. 2009.http://tinyurl.com/IRSstatement. According to Commissioner Schulman, "The passage of time, advances in technology, and the nature of communication in the modern workplace have rendered this law obsolete." *Ibid.* He urged Congress to "make clear that there will be no tax consequences to employers or employees for personal use of work-related devices such as cell phones provided by employers." Ibid.

The reaction to the IRS's proposal makes clear that the personal use of employer-provided devices represents the prevailing business norm. See Osterman Research, *supra*; Lee, *supra*.

D. The Court Should Not Address In This Case The Impact of Employers' Monitoring Policies On Fourth Amendment Protection Against Law Enforcement Access to Private Sector Or Government Employees' Electronic Communications.

This case involves the extent to which government employees have a reasonable expectation of privacy protected by the Fourth Amendment with respect to their use of an electronic communication system provided by their employer. One of the principal arguments advanced by petitioners is that the Police Department's internet use policy undermines all reasonable expectation of privacy in this case. See, *e.g.*, Pet. Br. 31. *Amici* do not share that view for the reasons stated below.

To the extent the Court chooses to discuss the effect of such a government policy on the reasonableness of Officer Quon's expectation of privacy, it should make clear that its analysis in this case relates solely to the government workplace context and not to the very different questions (1) whether a private employer's internal policy regarding monitoring of electronic communications affects its employees' reasonable expectation, protected by the Fourth Amendment, with respect to the privacy of those electronic communications vis-à-vis government law enforcement officers; and (2) whether a government workplace monitoring policy may affect a government employee's reasonable expectation of privacy with respect to government law enforcement access to emails and text messages.

The fact that a private employee may agree as a condition of his use of the employer's electronic communication system to permit the employer access to the content of his communications no more undermines the legitimacy of the employee's expectation of privacy vis-à-vis the government than the private employer's right to search the employee's office vitiates the employee's protection under the Fourth Amendment against an unreasonable government search of that office. See, *e.g., Mancusi* v. *DeForte*, 392 U.S. 364, 369 (1968) (employer's reasonable expectation of privacy vis-à-vis the government).

That distinction is simply a specific recognition of the general Fourth Amendment principle that permitting other private parties to access protected spaces or materials does not diminish privacy expectations as against the government or other entities to whom the private parties have not granted consent. Admitting a guest to one's home or allowing an accountant to visit an office and review private papers does not mean government actors may enter the home or seize the papers from the individual without a warrant. So too here. Permitting a private employer to access messages transmitted on companyprovided devices does not vitiate the employee's reasonable expectation that the messages will remain inaccessible to the government.<sup>9</sup>

When an individual's employer is the government, the inquiry is a bit more complex. To the extent a government employer has established a legitimate policy providing for access to otherwise private places or communications,<sup>10</sup> a government employee cannot make the argument-available to private sector employees—that the policy has no relevance to the individual's expectation of privacy vis-à-vis the government as employer. But whatever authority the government may have to monitor employee communications in its role as employer is limited to that context, and does not apply to law enforcement searches. O'Connor, 480 U.S. at 717 (plurality opinion) ("The operational realities of the workplace, however, may make some employees' expectations of privacy unreasonable when an intrusion is by a supervisor rather than a law enforcement official.").<sup>11</sup> Conclusions regarding the effect on the

<sup>&</sup>lt;sup>9</sup> The Solicitor General explicitly limits her argument regarding the impact of an employer's policy to the government employee context. *E.g.*, U.S. Br. 12 (referring to "government employer['s]" reservation of a right of access) & 16 (citing decisions regarding government policies).

<sup>&</sup>lt;sup>10</sup> As we discuss below, the government's authority to establish such policies is constrained by the unconstitutional conditions doctrine. See note 13, *infra*.

<sup>&</sup>lt;sup>11</sup> Compare *Michigan Dep't of State Police* v. *Sitz*, 496 U.S. 444 (1990) (allowing highway stops for safety purposes without in-

legitimacy of an expectation of privacy of a policy adopted by a government employer are not at all transferable to law enforcement access in either the public or the private employment situation.

Prudential reasons also counsel against allowing employment policies to trump employees' expectations of privacy in electronic written communications.

Many private employers have policies permitting them to access employees' emails and other communications for specified purposes. American Management Association, The Latest on Workplace Monitorand Surveillance, Mar. 13. ing 2008.http://tinyurl.com/yjb4q4a (43% of employees surveyed review computer files whereas 70% filter messages). Employers desire such access in order to prevent use of their communications system for illegal purposes, to obtain information relevant to employee performance, and for other legitimate business reasons. If the unavoidable consequence of agreeing to employer access on these grounds were unfettered government access to all of an employee's emails without any judicial oversight-many employees might be reluctant to use their employer's systems for personal messages.

Permitting such automatic government access would undermine the incentive structure at the heart of private-sector privacy policies. As we have discussed, many employers benefit significantly from their employees' personal use of employer-provided communications systems. But surrendering a slight

dividualized suspicion), with *City of Indianapolis* v. *Edmond*, 531 U.S. 32 (2000) (prohibiting highway stops for law enforcement purposes without individualized suspicion).

amount of privacy to an employer is one thing; surrendering a broad swath of privacy to the government is quite another. Employees might hesitate, under this system, to use the employer's communications devices at all. Or they might use them more sparingly, thus eliminating the business advantage derived from employees' constant use of mobile devices. See pages 17-18, *supra*.

In addition, holding that an employer's monitoring policy suffices to eliminate any reasonable expectation of privacy would dramatically restrict the Fourth Amendment protection accorded individuals' most private communications. Nothing in this Court's jurisprudence supports that result.

For these reasons, the Court should limit its ruling in this case to the government employer context and make clear that it is not addressing the effect of employers' electronic communications system use policies upon the Fourth Amendment protection against warrantless law enforcement surveillance of employees' written electronic communications.

#### II. THE SEARCH HERE VIOLATED THE FOURTH AMENDMENT STANDARD AP-PLICABLE TO SEARCHES OF GOVERN-MENT WORKPLACES.

All agree that the issue presented here is governed by the standard set forth in the plurality opinion in *O'Connor* v. *Ortega*, 480 U.S. 709 (1987). The parties' disagreement before this Court involves two case-specific, and entirely record-dependent, issues: first, whether on the particular facts here Officer Quon had a reasonable expectation of privacy in the content of the text messages; and second, whether the Department's search was reasonably related to its goals and not excessively intrusive. There is no basis for reversing the court of appeals' determinations regarding these issues, which are fully supported by the record in this case.

# A. The O'Connor Plurality Opinion Supplies The Governing Standard.

This Court in O'Connor addressed public employees' Fourth Amendment rights against unreasonable searches by their employer. The O'Connor plurality recognized that the Fourth Amendment provides protection against unreasonable searches conducted by government officials in other noncriminal contexts and extended that rationale to the public workplace. See New Jersey v. T.L.O., 469 U.S. 325 (1985) (school officials); Camara v. Municipal Court, 387 U.S. 523 (1967) (building inspectors); Marshall v. Barlow's, Inc., 436 U.S. 307 (1978) (OSHA inspectors). See also O'Connor, 480 U.S. at 714-15 (citing these cases).<sup>12</sup>

The O'Connor inquiry is context-specific, examining the "operational realities of the workplace" to determine whether a public employee has a reasonable expectation of privacy vis-à-vis her employer. *Id.* at 717. There is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable." *Id.* at 715; see also *id.* at 718 ("the question whether an employee has a

<sup>&</sup>lt;sup>12</sup> O'Connor applies only to "noninvestigatory work-related intrusion[s] or an investigatory search for evidence of suspected work-related employee misfeasance." O'Connor, 480 U.S. at 723. Because the jury in this case found that "Chief Scharf's intent was to 'determine the efficacy of the character limit," Pet. App. 34, the text message audit falls under O'Connor's noninvestigatory, work-related intrusion prong.

reasonable expectation of privacy must be addressed on a case-by-case basis"); *id.* at 717 ("[t]he employee's expectation of privacy must be assessed in the context of the employment relation"). *O'Connor* therefore mandates a case-by-case approach that takes into account the diversity of workplace environments and of policies promulgated by government employers.

If the public employee has a reasonable expectation of privacy in the workplace, O'Connor adopts a familiar two-pronged inquiry to ascertain whether a workplace search was reasonable. First, the search must be justified at its inception. See *id.* at 726. A workplace search is justified at its inception if "necessary for a noninvestigatory work-related purpose such as to retrieve a needed file" or necessary for an investigation of workplace-related misconduct. *Ibid.* 

Second, the search must be "reasonably related in scope to the circumstances which justified the interference in the first place" and "not excessively intrusive." *Ibid.* (quoting *T.L.O.*, 469 U.S. at 341, 342). Once again, *O'Connor* requires a fact-bound inquiry into the government employer's actions.

The O'Connor plurality standard has been applied consistently by the lower courts. See United States v. Mancini, 8 F.3d 104, 108 (1st Cir. 1993); Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (Sotomayor, J.); United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000); United States v. Johnson, 16 F.3d 69, 73-74 (5th Cir. 1994); Am. Postal Workers Union v. U.S. Postal Serv., 871 F.2d 556, 560 (6th Cir. 1989); Narducci v. Moore, 572 F.3d 313 (7th Cir. 2009); Biby v. Bd. of Regents, 419 F.3d 845, 850-851 (8th Cir. 2005); United States v. Taketa, 923 F.2d 665, 673-674 (9th Cir. 1991); United States v. Ange-

Angevine, 281 F.3d 1130, 1134 (10th Cir. 2002); United States v. Esser, 284 Fed. Appx. 757, 758-759 (11th Cir. 2008); Stewart v. Evans, 351 F.3d 1239, 1243 (D.C. Cir. 2003) (Roberts, J.). The standard strikes a manageable and appropriate Fourth Amendment balance between the government's interest in running an efficient workplace and public employees' rights to privacy.

Indeed, petitioners and the Solicitor General agree that the *O'Connor* plurality opinion supplies the appropriate test. Pet. Br. 22-28; U.S. Br. 12-13 & 27-28.

## B. The Government Employee Respondents Had A Reasonable Expectation Of Privacy In Their Text Messages.

Under O'Connor, all of the "operational realities of the workplace," 480 U.S. at 717, must be considered in determining whether there is a reasonable expectation of privacy. Both courts below correctly held that the officers had a reasonable expectation of privacy in the content of the text messages sent and received via the government-provided pagers.

Petitioners do not argue that the sender and recipient of a text message may never have a reasonable expectation of privacy in the message's contents. See Pet. Br. 63 ("But whether users of text mesaging generally have a reasonable expectation of privacy in the content of text messages is not the issue here."); U.S. Br. 31 n.14 ("[N]o party has argued in this case that respondents lost all expectation of privacy the moment their messages were passed to [the wireless provider] for delivery \* \* \*."). Rather, the arguments advanced by petitioners and their *amici* turn on the particular facts of this case. When those facts are examined, however, they plainly support the lower courts' determination.

# 1. Lieutenant Duke's Interpretation Of The Department's Policy, Together With His Settled Practice, Supported A Reasonable Expectation Of Privacy.

Both courts below concluded (a) that the City did not have a written policy that expressly governed the use of the pagers, Pet. App. 6, 29-31, 47-48, 49-51, 88-89, 90-91; see also *id*. at 127; and (b) that the Department had "informal-but express and specificpolicy and practices that did govern use of the pagers" id. at 127 (Wardlaw, J.) (concurring in the denial of rehearing en banc); see also *id.* at 30, 98. "[T]his Court has frequently noted its reluctance to disturb findings of fact concurred in by two lower courts." Rogers v. Lodge, 458 U.S. 613, 623 (1982); see also Tiffany Fine Arts, Inc. v. United States, 469 U.S. 310, 317 n.5 (1985). And the two factual findings concurred in by the lower courts here compel the conclusion that Officer Quon had a reasonable expectation in the privacy of his email messages.

First, the position of petitioners and their amici is premised almost exclusively on the contention that the Department's written "no privacy" policy encompassed text messages. E.g., Pet. Br. 31-35. But that written policy did not expressly include pagers or text messaging; indeed, the policy had been issued to, and acknowledged by, Officer Quon before the Department even acquired the pagers. Pet. App. 5. That is why both lower courts found as a factual matter that the written policy was inapplicable. Second, petitioners' sole support for their contention that the policy encompassed text messages is Lieutenant Duke's testimony that he informed members of the Police Department that pager messages would fall within the policy. Pet. Br. 33-34. But this is the very same Lieutenant Duke who established the informal policy and practice that text messages would not be reviewed as long as employees paid any overage charges.

Lieutenant Duke explained that the "practice was, if there was overage, that the employee would pay for the overage that the City had." Pet. App. 6 (internal quotation marks omitted). He testified that Officer Quon "needed to pay for his personal messages so we didn't—pay for the overage so we didn't do the audit." Pet. App. 51; see also *id.* at 8 (Officer Quon testified that he was told by Lieutenant Duke that "if you don't want us to read [your messages] pay the overage fee").

Moreover, the Department's actual practice was consistent with this informal policy established by Lieutenant Duke. Each time Office Quon exceeded the monthly allotment, Lieutenant Duke would tell him how much he owed and Officer Quon would pay that amount; the Department did not review Officer Quon's messages. Pet. App. 7-8. This practice was maintained for several months until Lieutenant Duke precipitated the review of text messages that gave rise to this action. *Ibid*. The district court found:

Lieutenant Duke made it clear to the staff, and to Quon in particular, that he would *not* audit their pagers so long as they agreed to pay for any overages. Given that Lieutenant Duke was the one in charge of administering the use of the city-owned pagers, his statements carry a great deal of weight. Indeed, before the events that transpired in this case the department did not audit any employee's use of the pager for the eight months the pagers had been in use. \*\*\* Lieutenant Duke in effect turned a blind eye to whatever purpose an employee used the pager, thereby vitiating the department's policy of any force or substance.

*Id.* at 90.

In light of these facts, both courts below concluded that "it was reasonable for Quon to rely on the policy-formal or informal-that Lieutenant Duke established and enforced." Pet. App. 31: see also id. at 90-91 ("Lieutenant Duke effectively provided employees a reasonable basis to expect privacy in the contents of the text messages they received or sent over their pagers; the only qualifier to guaranteeing that the messages remain private was that they pay for any overages"). Lieutenant Duke's informal, permissive policy contrasts sharply with an environment in which "searches were frequent, widespread, or extensive enough to constitute an atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable." Leventhal, 266 F.3d at 74 (internal quotation marks omitted) (Sotomayor, J.).

*Third*, petitioners and the Solicitor General argue that Lieutenant Duke did not occupy a policymaking position in the Department and therefore could not alter the written policy. But the written policy did not by its terms apply to text messaging the only basis for extending it to include text messaging is the statement to that effect by Lieutenant Duke. And if (as petitioners and the Solicitor General assume) Lieutenant Duke had sufficient authority to make that statement, he necessarily had sufficient authority to enunciate and implement the policy and practice against reviewing the content of text messages.

For that reason, the nature of Lieutenant Duke's authority is beside the point on the facts here. Because petitioners themselves rely on the authoritative nature of some of Lieutenant Duke's statements, petitioners cannot dispute the authoritative status of the statements and actions of the same individual relied upon by respondents.

Fourth, petitioners point to O'Connor in asserting that a Department "no privacy" policy would vitiate any reasonable expectation of privacy in text messages sent over government-provided pagers. Pet. Br. 31-35. But petitioners overstate O'Connor, which merely observed that there was no applicable government access policy-and therefore could not, and did not, hold that an access policy is dispositive in every case. O'Connor, 480 U.S. at 719 (noting that there was no evidence of any established "reasonable \* \* \* regulation or policy discouraging employees from storing personal papers and effects in their desks"). Moreover, the O'Connor inquiry is contextspecific and looks to "actual office practices and procedures" and "legitimate regulation." Id. at 717 (emphasis added). Thus, even if the Department's written policy addressed the issue of pager usage, it would not be dispositive.<sup>13</sup>

<sup>&</sup>lt;sup>13</sup> For example, a government agency engaged in routine administrative functions surely could not require as a condition of employment that employees waive all Fourth Amendment rights with respect to searches of the employee's person and of-

*Fifth*, petitioners, but not the Solicitor General, argue that a special standard should apply to text messages of police SWAT teams because there may be a need to review such messages in connection with after-action analyses of SWAT team activity. See Pet. Br. 29-31.

There is no basis in *O'Connor* for such an approach. The fact that the government may at some point have a legitimate basis to review employee text messages, or emails, or physical documents, does not mean that the employee lacks any reasonable expectation of privacy. Indeed, under this theory no government employee would ever have any Fourth Amendment protection with respect to the workplace because some set of facts could be hypothesized that could justify review of his emails or documents. This Court should reject petitioners' attempt to reduce the *O'Connor* standard to a dead letter.

# 2. The California Public Records Act Does Not Undermine The Employees' Reasonable Expectation Of Privacy.

Petitioners also point to the California Public Records Act (CPRA), Cal. Gov't Code § 6250, in asserting that respondents had no reasonable expectation of privacy. Pet. Br. 35-40.

The fact that an electronic record may be reviewed in response to a CPRA request does not un-

fice. That is because the government may not impose "unconstitutional conditions" in an attempt to circumvent the Fourth Amendment. See *Chandler* v. *Miller*, 520 U.S. 305 (1997) (holding that candidates for public office cannot be required to submit to a suspicion-less drug test); *cf. Rumsfeld* v. *Forum for Academic and Institutional Rights, Inc.*, 547 U.S. 47. 59-60 (2006) (discussing unconstitutional conditions doctrine).

dermine an employee's reasonable expectation of privacy in that record any more than such a review would vitiate the employee's expectation of privacy with respect to personal paper files kept in a government employee's office.<sup>14</sup> An individual's reasonable expectation of privacy is not binary: The fact that someone might review records pursuant to the CPRA does not open the door to review by the government for any purpose whatever. Under petitioner's theory, any document potentially subject to mere review-not even disclosure-whether under the CPRA, the Freedom of Information Act (FOIA), 5 U.S.C. § 552, or the Presidential Records Act (PRA), 44 U.S.C. § 2201, would be stripped of any protection under the Fourth Amendment. That expansive contention would deprive the private papers of numerous public employees of all protection simply because they are located in those employees' government offices.

Finally, it is unlikely that the CPRA would require disclosure of the text messages—even if the messages were subject to the CPRA in the first place. The California courts have construed the CPRA to exempt from disclosure as a general matter purely personal information. *California State University* v. *Superior Court*, 108 Cal. Rptr. 2d 870, 879-880 (2001) ("The mere custody of a writing by a public agency does not make it a public record \*\*\*. [P]urely personal information unrelated to 'the con-

<sup>&</sup>lt;sup>14</sup> That is especially true when, as here, the lower courts found that there is "no evidence \* \* \* suggesting CPRA requests to the department are so widespread or frequent as to constitute 'an open atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable." Pet. App. 94 (quoting *Leventhal*, 266 F.3d at 74).

duct of the public's business' could be considered exempt from this definition, i.e., the shopping list phoned from home, the letter to a public officer from a friend which is totally void of reference to governmental activities.") (citations omitted); see also Cal. Gov't Code § 6254(c) (exempting from CPRA documents whose disclosure "would constitute an unwarranted invasion of personal privacy"). Other states have reached similar conclusions in the context of electronic communications. See, *e.g., Griffis* v. *Pinal County*, 156 P.3d 418 (Ariz. 2007); *Denver Pub. Co.* v. *Board of County Comm'rs*, 121 P.3d 190 (Colo. 2005).

Amici media and publishing organizations correctly point out that even private communications may be subject to disclosure under certain circumstances where those communications relate to the public interest—for example, where communications reflect a dereliction of official duties or a bias that renders the person unfit for his or her position. Am. Br. 24-25. But disclosure under such circumstances, where personal privacy is implicated, is the result of a case-by-case balancing of "the public's interest in disclosure and the individual's interest in personal privacy." International Federation of Professional and Technical Engineers, Local 21, AFL-CIO v. Superior Court, 165 P.3d 488, 493 (Cal. 2007). This balancing might well justify disclosure of only some portions of a document—for example, the time at which a personal text was sent and the recipient, but not the contents. Cf. Tiberino v. Spokane County, 13 P.3d 1104 (Wash. Ct. App. 2000) (personal e-mails fell within public records act when used by county to justify termination of employee, but contents of e-mails exempt from disclosure on grounds of privacy). The fact that disclosure of purely personal documents is not the norm under the CPRA is yet another reason

why the statute does not undermine Officer Quon's reasonable expectation of privacy in his personal text messages.

## C. The Search Of The Text Messages Was Unreasonable In Its Scope.

The court of appeals correctly determined that on this record—the search was not reasonably related to its objectives and was excessively intrusive. Pet. App. 34-36.

It is common ground that the "least restrictive means" test is inapplicable to the *O'Connor* inquiry. And, contrary to petitioner's suggestions, Pet. Br. 45-50, the court below did not engage in "least restrictive means" analysis. Pet. App. 33-36; see also *id.* at 133 (Wardlaw, J., concurring in denial of rehearing en banc). Rather, the court below faithfully applied the *O'Connor* standard.

The jury concluded that the sole purpose for the search was to "determine the efficacy of the existing character limits to ensure that officers were not being required to pay for work-related expenses." Pet. App. 119. Although this purpose was permissible, the means chosen were excessively intrusive.

To begin with, the option chosen by petitioners was unlawful. The court of appeals held that disclosure of the text messages to petitioners violated federal law. The decision to utilize that search option was therefore necessarily unreasonable and excessively intrusive.

Even under petitioners' view of the privacy policy, which permits "light personal communications," Pet. Br. 4, moreover, the content audit could reveal embarrassing or inherently private information, such as a visit to an oncologist, a therapist, or a divorce attorney.

And there were a myriad of alternative options available to verify the efficacy of the character limit. For example, petitioners could, consistent with the Fourth Amendment, have compared the phone numbers on Officer Quon's bill against a list of Department phones. Compare Katz v. United States, 389 U.S. 347 (1967) (prohibiting the government from bugging a public telephone booth without a warrant), with Smith v. Maryland, 442 U.S. 735 (1979) (permitting the use of a pen register device to capture phone numbers dialed because that information is conveyed to the phone company). If the government found that Officer Quon frequently and consistently texted non-Department phones-such as his wife'spetitioners would have fulfilled the character-limit purpose of their audit.

Alternatively, the Department could have asked Officer Quon to review the messages himself and reveal work-related messages totaling more than 25,000 characters in a month. If he could not do so, the Department would know that the existing character limit was appropriate; if he produced messages exceeding the limit, the Department would know that the limit was too low. Pet. App. 35-36. Because the government could have fulfilled its interest fully without reviewing the messages itself, the approach it chose was excessively intrusive and violated the constitutional standard.

# D. Because The Search Of The Officers' Text Messages Was Unreasonable, Petitioners Also Violated The Fourth Amendment Rights Of The Private Individuals Who Sent Messages To The Officers.

If petitioners' search of Officer Quon's text messages violated his Fourth Amendment rights, then it also violated the Fourth Amendment rights of the persons who sent messages to him. As we have discussed (at pages 14-15, *supra*), the sender of a message does not lose his Fourth Amendment protection the moment the message is sent. If the content of the message is not obtained through voluntary disclosure by the recipient or compelled disclosure in compliance with the Fourth Amendment, the sender's rights are violated as well. The government must obtain access from either sender or recipient in a manner that comports with the Fourth Amendment.

On the other hand, if, contrary to our position, petitioners did not violate Officer Quon's Fourth Amendment rights in obtaining the messages, then the other respondents cannot claim that their constitutional rights were violated. The government's legitimate acquisition of the messages vitiates any constitutional claim that the senders otherwise could assert.

#### CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

DAN M. KAHAN SCOTT L. SHUCHART Yale Law School Supreme Court Clinic 127 Wall Street New Haven, CT 06511 (203) 432-4992

ANDREW J. PINCUS Counsel of Record CHARLES ROTHFELD Mayer Brown LLP 1999 K Street, NW Washington, DC 20006 (202) 263-3000 apincus@mayerbrown.com

STEVEN R. SHAPIRO American Civil Liberties Union Foundation 125 Broad Street New York, NY 10004 (212) 549-2500 GREGORY A. BECK Public Citizen 1600 20th Street, NW Washington, DC 20009 (202) 588-7713

#### Counsel for Amici Curiae

#### **MARCH 2010**