No. 08-1332

IN THE
Supreme Court of the United States

CITY OF ONTARIO, ONTARIO POLICE DEPARTMENT, and LLOYD SCHARF,

Petitioners,

v.

JEFF QUON, JERILYN QUON, APRIL FLORIO, and STEVE TRUJILLO,

Respondents.

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

BRIEF FOR AMICUS CURIAE NEW YORK INTELLECTUAL PROPERTY LAW ASSOCIATION IN SUPPORT OF RESPONDENTS

MARK J. ABATE
President
New York Intellectual Property Law Association
GOODWIN PROCTER LLP
620 Eighth Avenue
New York, NY 10022
(212) 355-3333

JONATHAN E. MOSKIN
Counsel of Record
FOLEY & LARDNER LLP
90 Park Avenue
New York, NY 10016
(212) 682-7474
JMoskin@foley.com

Counsel for Amicus Curiae

228872

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Page

Cases

Cited Authorities

Cited Authorities

Cited Authorities

Statutes, Rules & Regulations

Page

Other Authorities

BRIEF FOR AMICUS CURIAE NEW YORK INTELLECTUAL PROPERTY LAW ASSOCIATION IN SUPPORT OF RESPONDENTS

STATEMENT OF INTEREST OF AMICUS CURIAE

This brief *amicus curiae* is submitted in support of Respondents by the New York Intellectual Property Law Association (the "NYIPLA" or the "Association"), a professional association of more than 2,000 attorneys in the United States and abroad whose interests and practices lie in the areas of patent, copyright, trademark, trade secret, privacy, and other intellectual property law and emerging technologies.[1]

The NYIPLA strives to educate the public and members of the bar in the fields of intellectual property law and privacy law and continually works with foreign associations to harmonize applicable international law. NYIPLA members and in particular its Privacy Law Committee, represent both plaintiffs and defendants in developing and protecting cutting edge technologies, including emerging communications technologies that give rise to the kinds of privacy concerns that arise in this case. As a result, the NYIPLA has a particularly

1. No counsel for a party authored this brief in whole or in part, and no such counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the *amicus curiae*, or its counsel, made a monetary contribution intended to fund its preparation or submission. The parties have consented to the filing of this brief and such consents are being lodged herewith.

strong interest in the meaning and application of privacy laws applied in the workplace on and in connection with such technologies. NYIPLA members include in-house attorneys working for businesses that own, enforce and challenge intellectual property interests and privacy interests, as well as attorneys in private practice who represent both intellectual property owners and accused infringers. NYIPLA members frequently engage in intellectual property licensing matters, and address workplace policy issues concerning ownership of intellectual properties, trade secrets and privacy rights.[2]

SUMMARY OF THE ARGUMENT

Much of the controversy surrounding this case has focused on whether, despite stated department policy to the contrary, a reasonable expectation of privacy was created by the verbal instructions of Officer Quon's superior, Lieutenant Duke, that Quon could avoid any review of his text messages on his department-issued

2. The arguments set forth in this brief were approved on or about March 22, 2010 by an absolute majority of the total number of officers and members of the Board of Directors (including those who did not vote for any reason, including recusal), but may not necessarily reflect the views of a majority of the members of the NYIPLA or of the organizations with which those members are affiliated. After reasonable investigation, the NYIPLA believes that no person who voted in favor of the brief, no attorney in the firms or companies with which such persons are associated, and no attorney who aided in preparation of this brief represents a party in this litigation. Some such persons may represent entities that have an interest in other matters that may be affected by the outcome of this proceeding.

pager simply by paying for any excess charges himself. However, the very nature of the specific technology here at issue – a mobile device – and the manner of use (outside any traditional workplace and both on and off duty) places this case directly amidst the currently (and rapidly) evolving universe of personal and mobile computing, and a swiftly changing and increasingly amorphous workplace. Even if the broad outlines of the law governing workplace privacy rules are reasonably clear in upholding most company policies permitting monitoring of office emails and computer use, this case resides at the very periphery of that workplace. Thus, to speak of "operational realities of the workplace" as Petitioners repeatedly do, is only to begin to frame the question, not to provide an answer. Unlike the era of the office cubicle or even private office-room, when *O'Connor* v. *Ortega*, 480 U.S. 709, 107 S. Ct. 1492 (1987), was decided, the "operational realities of the workplace" are today in rapid and fundamental transition. New mobile computing technologies, new electronic storage media, as well as new communications media, such as Facebook, Twitter and other so-called "Web 2.0" applications, are reshaping where and how Americans work.

The NYIPLA submits this brief to attempt to clarify that, above and beyond the wide acceptance of the premise that employers (public and private) can and do set privacy policies regarding employees' use of office computers and email communications, the most vexing issues raised by this case - and its broader implications for workplace privacy in general - are not whether the City of Ontario could have set reasonable policies for monitoring computer use on its own servers; how that

policy applied to email use in an office setting, nor whether Officer Quon would have had a reasonable expectation of privacy in emails sent over the City of Ontario network. Petitioners' own formal policy confirms he most likely would not.

Rather, five factors place this case outside the scope of the typical office privacy policy dispute: (i) the Respondents used mobile pagers, not office computers; (ii) the mobile pager, by its very nature, could be and was used when officer Quon was off duty as well as on; (iii) the network over which the text messages were sent was not the government's network but that of a third party, Arch Wireless; (iv) text messaging on a third party's network did not expressly fall within the scope of the Petitioners' written privacy policy (and hence was the subject of a dispute as to whether advice was given orally extending the written privacy policy to such uses); and (v) for this specific and arguably more personal handheld mobile device, the Petitioners' computer use policy was further placed in doubt by instructions of Lieutenant Duke and actual office practices, arguably permitting private use of the pagers, provided that the officers paid for any overages in use.[3]

At the very most there was in this case an informal (verbal) policy extending the formal email policy to the

3. Because the communications here at issue did not occur on the Petitioners' email system, arguably less directly relevant is the question whether Respondents' personal uses of the wireless pagers fell within the exception to the Petitioners' written privacy policy under which "[s]ome incidental and occasional personal use of the e-mail system is permitted if limited to 'light' personal use." (Pet'r Br. 4.)

pagers; yet, there was also an actual practice of not enforcing that informal policy, to the extent it did exist. In such circumstances, the operational realities of this workplace (and others like it) may well support a reasonable expectation of privacy under developing legal doctrines requiring at least some form of notice and consent before privacy protections are lost.

The existence of public records laws permitting potential public scrutiny of police department records, such as the text messages here at issue, raise questions that may best be viewed against the backdrop of the parallel pressures in civil litigation from electronic discovery. Without questioning that the public has *some* right to inquire into the operations of government-run entities, thus making electronic records *potentially* relevant to public inquiry and inspection, civil and criminal litigation now routinely requires private and public entities to save, search and share precisely such communications. Thus, the same evolving operational realities of the workplace require businesses (private and public) to develop not only privacy policies that may increase their control over employee communications but also (and simultaneously) document retention policies freeing the businesses from many of the very same duties to maintain control over the same or similar types of electronic records – many of which are essentially private communications that simply happen to find their way onto office networks because of the ways employees increasingly blend their personal and business lives. However, merely because casual communications that, in an earlier era, would never have been recorded at all now leave electronic traces that can be stored or recovered, does not make all such records relevant to the operation of the workplace, even where the merging of

personal and business lives makes them a reality of that workplace. This Court and others have refused FOIA requests when the subject matter undermined privacy expectations. A ruling that there is no reasonable expectation of privacy in such communications may expose to public scrutiny many electronic records that businesses themselves would deem private and over which they do not wish to exercise control.

In summary, the NYIPLA submits that this case thus should not be the vehicle for calling into question any of the widely used office policies that courts have enforced without hesitation – in both public and private contexts – permitting employers to set reasonable limits on workplace privacy rights and to preserve and maintain needed controls over office computer and communications equipment. However, as communications technologies continue to evolve (at a pace unmatched historically); as social expectations regarding privacy in such communications evolve in parallel; and as applicable privacy law continues its own companion evolution (with considerable disagreement still evident among the courts on many issues); this case is also ill-suited for drawing any broad new legal rules (such as the presumption the United States Government proposes in its amicus brief (Amicus Br. 14) that employees – like mere invitees – have no legitimate expectations of privacy independent of those rights expressly granted by the employer). Rather, for these unique circumstances and these still-novel and still-evolving technologies, the incremental, case-by-case approach endorsed in *O'Connor* in 1987 remains singularly appropriate. The law should be allowed to continue to evolve as societal expectations of privacy or the lack thereof become better-settled.

Finally, the NYIPLA notes the similarity of the Fourth Amendment standard of a "reasonable expectation of privacy" to the common law standard of "intrusion upon seclusion" that would be "highly offensive to a reasonable person", which also turns on whether the party has a "reasonable expectation of privacy." *In re Asia Global Crossing, Ltd.*, 322 B.R. 247 (S.D.N.Y. 2005), explains:

> A right of privacy is recognized under both the common law, see Restatement (Second) of Torts, 652(B) (1977) (discussing the tort of "intrusion on seclusion") and the Fourth Amendment to the United States Constitution. In both cases, the aggrieved party must show a reasonable expectation of privacy.

Id. at 256. *See also*, *Hilderman* v. *Enea TekSci, Inc.*, 551 F. Supp. 2d 1183, 1203 (S.D. Cal. 2008); *Pietrylo* v. *Hillstone Rest. Grp.*, No. 06-5754 (FSH), 2008 WL 6085437, at * 7 (D.N.J. July 25, 2008); *Brown-Criscuolo* v. *Wolfe*, 601 F. Supp. 2d 441, 455 (D. Conn. 2009). Not surprisingly, the lower court decisions in *Quon* have been widely cited by other courts outside the scope of Fourth Amendment claims of privacy, but, rather, under state law privacy claims, and in the *private* employment context. *See*, *e.g.*, *Pure Power Boot Camp Inc.* v. *Warrior Fitness Boot Camp, LLC*, 587 F. Supp. 2d 548 (S.D.N.Y. 2008); *Stengart* v. *Loving Care Agency*, 973 A.2d 390 (N.J. Super. Ct. App. Div. 2009); *Louis Vuitton Malletier S.A.* v. *Akanoc Solutions, Inc.*, No. C 07-03952 JW, 2008 U.S. Dist. LEXIS 63115 (N.D. Cal. Aug. 7, 2008); *Flagg* v. *City of Detroit*, 252 F.R.D. 346 (E.D. Mich. 2008). The decision of this Court will undoubtedly cast an even

wider shadow in non-Fourth-Amendment cases than have the lower court decisions in this action.[4]

For these reasons, continued application of the case-by-case approach adopted in *O'Connor* v. *Ortega* counsels caution in defining the scope of privacy protections. The holding of the Ninth Circuit thus should be affirmed or the matter should be remanded to resolve any uncertainties what was the communications and privacy policy and to what extent it was enforced.

FACTUAL BACKGROUND

The record shows that the pagers at issue here were used by Respondents to create text messages on the Arch Wireless network. The messages were stored by Arch Wireless in a format capable of being retrieved. The messages were not emails sent on the network maintained by the City of Ontario Police Department ("OPD"). The messages were sent by Petitioners while both on duty and off duty, and the pagers were provided precisely because of the expectation that the officers might need to be available any time of day or night (*i.e.*, "24/7"). *Quon* v. *Arch Wireless Operating Co.*, *Inc.*, 554 F.3d 769, 770 (9th Cir. 2009).

The actual OPD "Computer Usage, Internet and E-mail Policy" provided in relevant part as follows:

> C. Access to all sites on the Internet is recorded and will be periodically reviewed by

4. The lower court decisions in *Quon* also had to consider California's constitutionally recognized right of privacy, which generally sets a higher privacy standard than recognized by other states. *See*, California Constitution, Article 1, § 1.

> the City. The City of Ontario reserves the right to monitor and log all network activity including *e-mail* and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.
>
> D. Access to the Internet and the *e-mail* system is *not* confidential; and Information produced either in hard copy or in electronic form is considered City property. As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.

Quon v. *Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 896 (9th Cir. 2008). Although the record indicates that, at a staff meeting, the officer responsible for use and provision of the OPD's electronic equipment, Lieutenant Steven Duke, advised the department that this policy would apply to text messages, Officer Quon, while present at the meeting, did not recall being told of the policy. *Id.* Minutes of the meeting include some brief mention of this announcement extending the email policy to pagers, yet the Ninth Circuit concluded that "[t]he record [was] clear that the City had no official policy governing the pagers." 554 F.3d at 770. At any rate, the department in practice did not follow this stated policy. Rather, the content of text messages remained private provided that individual officers simply reimbursed the department for any charges from exceeding the monthly limit of 25,000 characters. The District Court noted: "Only when the personnel in question disputed the

overages – either claiming that the use was work-related or otherwise – did Lieutenant Duke make it clear that he would endeavor to audit the contents of the messages sent and received on the pager." *Quon* v. *Arch Wireless Operating Co.*, *Inc.*, 445 F. Supp. 2d 1116, 1124 (C.D. Cal. 2006). At least three or four times when his monthly text messages exceeded the 25,000 character limit, Officer Quon availed himself of this offer to pay for any overages (and preserve his messages from wider scrutiny).

Moreover, the record provides no evidence of instances in which the informal verbal policy was actually enforced prior to the review of Respondents' email messages that gave rise to this litigation. To the contrary, the district court found that "before the events that transpired in this case the department did not audit any employee's use of the pager for the eight months they had been in use," 445 F. Supp. 2d at 1141, and that the practice "allowed, condoned and even encouraged" officers to exceed the character limit. *Id.* at 1144.

ARGUMENT

A. *The "Operational Realities" of the Workplace and Expectations of Privacy Are Rapidly Evolving*

Current law is well-settled that, under clear and reasonable office policies, employers are permitted to have access to and review employee emails and other documents and records created on office communications and computer equipment. Where such policies exist, the courts have consistently declined to recognize a reasonable expectation of privacy in emails

and other communications and records transmitted over or stored on company hardware. *See U.S.* v. *Ziegler*, 456 F.3d 1138, 1144 (9th Cir. 2006) (listing cases[5]). *See also Pure Power Boot Camp Inc.*, 587 F. Supp. 2d at 559-60 (listing cases[6]). The NYIPLA does challenge such settled law.

---

5. *Biby* v. *Bd. of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (no reasonable expectation of privacy existed where a policy reserved the employer's right to search an employee's computer for a legitimate reason); *U.S.* v. *Thorn*, 375 F.3d 679, 683 (8th Cir. 2004), *cert. granted and judgment vacated on other grounds by* 543 U.S. 1112, 125 S. Ct. 1065, 160 L. Ed. 2d 1050 (2005) (no expectation of privacy where public agency's computer-use policy prohibited accessing sexual images, expressly denied employees any personal privacy rights in the use of the computer systems, and provided the employer the right to access any computer to audit its use); *U.S.* v. *Angevine*, 281 F.3d 1130, 1133-35 (10th Cir. 2002) (no expectation of privacy where employer's computer-use policy included monitoring and claimed a right of access to equipment); *Muick* v. *Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002) ("Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy. . . "); *Wasson* v. *Sonoma County Jr. Coll. Dist.*, 4 F. Supp. 2d 893, 905-06 (N.D.Cal. 1997) (no expectation of privacy where policy gave the employer "the right to access all information stored on [the employer's] computers"). *See also*, *TBG Ins. Services Corp.* v. *Superior Court*, 96 Cal. App. 4th 443 (2d Dist. 2002) (permitting employer monitoring of e-mail where employee acknowledged monitoring policy as part of employee handbook notwithstanding California's constitutional right of privacy).

6. *U.S.* v. *Simons*, 206 F.3d 392, 398 (4th Cir. 2000) ("Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were

(Cont'd)

However, even against this background, courts have come to recognize areas where the lines between professional and personal, or between "business" and "nobody's business," are hard to draw. Business increasingly encroaches on personal life, and mobile computing and home office uses of even business equipment have begun to complicate the task of disentangling where work ends and personal life begins. For example, attorney-client communications – even when made using office equipment - have raised vexing questions, increasingly inclining courts to favor the privacy rights of the individual, even where the literal language of an office privacy policy might suggest otherwise. *Convertino* v. *U.S. Dep't of Justice*, 04-CV-0236, slip op. at 19 (D.D.C. Dec. 10, 2009); *Curto* v. *Medical World Communications*, *Inc.*, No. 03-CV-6327 (DRH)(MLO), 2006 WL 1318387, at * 9 (E.D.N.Y. May 15, 2006); *Stengart*, 973 A.2d 390; *Brown-Criscuolo*, 601 F. Supp. 2d 441. Similarly, personal records, such as medical or financial data, might merit privacy protections notwithstanding employee needs to

---

(Cont'd)

private, such a belief was not objectively reasonable after FBIS notified him that it would be overseeing his Internet use."); *Thygeson* v. *U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746, at *21 (D.Or. Sept. 15, 2004) ("[w]hen, as here, an employer accesses its own computer network and has an explicit policy banning personal use of office computers and permitting monitoring, an employee has no reasonable expectation of privacy."); *Muick* v. *Glenayre Electronics*, 280 F.3d 741, 743 (7th Cir. 2002). *See also*, *Silverberg & Hunter LLP* v. *Futterman*, No. 002976/02, 2002 WL 24461954 (N.Y. Sup. Ct. Jul 3, 2002) ("Protecting files with a password may not be used to bootstrap a privacy claim where the recognized expectation is that none exists.").

communicate such information using the most expedient means at their disposal: the office laptop, a PDA, cell phone or other such device. Individuals can and do use personal communications devices (such as Blackberries and other PDA's and cell phones) and new communications media (such as individual email accounts, Facebook, MySpace, Twitter, blogs and the like) in connection with the performance of their jobs. Some companies use internal social networks for various purposes and professional networks such as LinkedIn and Spoke are also widely used for business purposes. An automatic loss of privacy rights under such circumstances need not be implied. Similarly, when an employer issues to its employees communication devices that permit monitoring of physical location (*e.g.*, by GPS), it is hardly clear that such capability or mere use of such devices entails consent to monitoring. In all such instances, what is personal and what is not can be elusive. This case well exemplifies these challenges as the pagers were evidently issued to officers because of their need to be on-call "24/7". *See Quon*, 554 F.3d at 770.

While the legitimate needs of employers to monitor and control use of networks they maintain must be preserved, the salacious nature of at least some of the text messages here at issue should not unduly color the full range of privacy concerns raised by this case, the technologies involved, and the evolving nature of the workplace. These Respondents brought into the mobile workplace matrix an aspect of their personal lives less likely to elicit sympathy than would the concerns of cancer victims or AIDS patients needing to reach their doctors during the workday; or individuals requiring

advice of counsel or an accountant because of pressing legal or financial concerns. Use by such employees of office-issued BlackBerries or even office cell phones en route to work or while traveling as part of their job responsibilities may well be accompanied by a reasonable expectation of privacy. Innumerable other examples where individuals mix work and personal concerns on office communications devices (under circumstances perhaps more sympathetic than Officer Quon's), are readily imagined.

As the "operational realities of the workplace" change, *O'Connor* dictates that no one rule of law should sweep all such individual circumstances under one hardened standard. Indeed, *O'Connor* holds that even in the circumstances of public employment, a case-by-case analysis should be undertaken to determine if the employee might have a reasonable expectation of privacy. If so, that expectation should be balanced with the government's need for workplace efficiency, supervision and control. 480 U.S. at 725-726 ("[P]ublic employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.")[7] Given the nearly endless varieties of workplace environments, best practices suggest that the employer seeking to ensure a right to review employee records (and correspondingly limit expectations of

---

7. *See also*, Andrew B. Serwin, *Information Security and Privacy, A Practical Guide to Federal, State and International Law*, Volume 1, § 15:3, pp. 1315-1316 (2008).

privacy) should establish clear workplace rules and apply them with consistency. Similarly, the technology covered by such rules should be identified and expressly incorporated into the guidelines. Finally, the individual employee should have some fair notice of the rules – if not also a realistic opportunity to object or consent. As shown below, these standards are still evolving. They should be allowed to continue to evolve.

B. *A Mobile Pager Is Not An Office Computer and May Create Unique Expectations of Privacy*

As noted above, where there exist workplace rules establishing the employer's right of access to and review of records created on company computer networks or communications equipment, the law generally does not recognize a reasonable expectation of employee privacy in such records. However, given the evolving nature of the workplace and communications technologies, areas of uncertainty continue to emerge. *Stengart*, explained:

> Certainly, the electronic age – and now the speed and ease with which many communications may now be made - has created numerous difficulties in segregating personal business from company business. Today many highly personal and confidential transactions are commonly conducted via the Internet, and may be performed in a moment's time.

973 A.2d at 400. To be sure, *Stengart* involved a particularly sensitive issue (whether privilege was lost in attorney-client privileged emails stored on a password protected laptop), yet the court cast this narrow issue

against the backdrop of the broader dilemma. *Accord*, *Curto*, 2006 WL 1318387 at * 8-9 (finding a right of privacy and no waiver of work-product or attorney-client privileges where laptops were used in home office and where the company's computer policy was somewhat ambiguous and not often enforced, thus lulling the plaintiff into an expectation of privacy.) Precisely because the law is still evolving, it should come as no surprise that the cases are divided on such issues. *See Scott* v. *Beth Israel Med. Ctr.*, 17 Misc.3d 934, 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007) (attorney client privilege waived where, under email policy, "[e]mployees have no personal privacy right in any material created, received, saved or sent on the Medical Center's communication or computer systems."); *Long* v. *Marubeni America Corp.*, No. 05 Civ 639 (GEL)(KNF), 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006) (privilege waived); *TBG Ins. Servs. Corp*. v. *Superior Court*, 96 Cal. App. 4th 443, 451-52, 117 Cal. Rptr. 2d 155 (2002) (cited by Petitioner at p. 32, finding no reasonable expectation of privacy in computer provided for home use), and *Bohach* v. *City of Reno*, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996) (cited by Petitioner at p. 34, and finding that any expectation of privacy in police pagers was diminished by department order that messages would be logged onto the system, and banning certain types of messages).

Where the scope and clarity of company policies are less then lucid; where enforcement of those policies has been inconsistent, or where employee consent has been in doubt, courts have been readier to recognize the reasonableness of employee expectations of privacy. *Convertino*, slip op. at 19 (reasonable expectation of

privacy in emails to attorney sent over office network where "[t]he DOJ maintains a policy that does not ban personal use of the company email. Although the DOJ does have access to personal emails sent through this account, Mr. Tukel was unaware that they would be regularly accessing and saving e-mails sent from his account."); *Brown-Criscuolo*, 601 F. Supp. 2d at 449 (reasonable expectation of privacy of password-protected email files of school teacher where policy provided that "[s]ystem users a limited privacy expectation in the contents of their personal files…"); *Curto*, 2006 WL 1318387 at * 3 (in a home-office environment, "the lack of enforcement by MWC of its computer usage policy created a 'false sense of security' which 'lull[ed]' employees into believing that the policy would not be enforced"); *People* v. *Jiang*, 131 Cal. App. 4th 1027, 33 Cal. Rptr. 3d 184 (Ct. App. 2005) (reasonable expectation of privacy in password protected files of attorney-client communications upheld where office privacy policy covered emails and voicemails but did not expressly cover records saved on company-issued laptop but not communicated over employer's email server;); *Hilderman*, 551 F. Supp. 2d at 1204 (genuine issue of fact whether policy allowing individuals to purchase company laptops created a reasonable expectation of privacy, even where means of searching laptop contents ultimately was deemed reasonable"); *U.S.* v. *Slanina*, 283 F.3d 670, 676 (5th Cir. 2002) ("The city did not disseminate any policy that prevented the storage of personal information on city computers and also did not inform its employees that computer usage and internet access would be monitored."), *vacated on other grounds*, 537 U.S. 802, 123 S. Ct. 69, 154 L. Ed. 2d 3 (2002), *on appeal after remand*, 359 F.3d 356 (5th Cir. 2004)

(per curiam); *Leventhal* v. *Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (although means of search ultimately deemed reasonable, employee had reasonable expectation of privacy where insufficient evidence that employer "had a general practice of routinely conducting searches of office computers or had placed Leventhal on notice that he should have no expectation of privacy in the contents of his office computer."); *In re Asia Global Crossing*, *Ltd.*, 322 B.R. at 259 ("[t]he evidence is equivocal regarding the existence or notice of corporate policies banning certain uses or monitoring of employees emails."); *See also*, *Bloomberg*, *LP* v. *SEC*, 357 F. Supp. 2d 156 (D.D.C. 2004) (SEC chairman's electronic calendar was not an "agency record" even where it included personal and business appointments and even where it resided on agency server and was stored on agency back-up system where agency employees were "permitted 'limited use of office equipment for personal needs.").

Communications media are rapidly changing, and workplace realities are changing with the technology. Companies that today discourage use of Net 2.0 interactive media may decide tomorrow that they need such tools and will encourage workers to foster connections on Facebook, Twitter and other sites. The law is still unclear whether or to what extent accessing a Facebook or other personal site via a company's server entitles the company to have access to such activities. *See Thygeson* v. *U.S. Bancorp*, No. CV-03-467-ST, 2004 WL 2066746 (D. Or. Sept. 15, 2004) (finding at least some right of employer to monitor employee access of Netscape email account from work but only addressing of websites plaintiff visited, not content of emails);

Compare Pure Power Boot Camp Inc., 587 F. Supp. 2d 548 (employee's emails on personal "Hotmail" and "Gmail" accounts remained private even if viewed while at work, using employer's computers, and notwithstanding that user name and passwords were found on company computers); *Curto*, 2006 WL 1318387 at * 4-5 (discussing need for caution where two company-issued laptops were used by plaintiff in her home office, which were not connected to employer's computer server, and noting paucity of precedent in this mixed office/private environment); *Hilderman*, 551 F. Supp. 2d at 1203 (employee expected to be able to purchase his company-issued laptop). *Cf. Rozell* v. *Ross-Holst*, No. 05 CV 2936 (JGK), 2006 WL 163143 (S.D.N.Y. Jan. 20, 2006)(dispute over employer's right of access to employee's AOL account paid for by employers and used in part for work); *Van Alstyne* v. *Electronic Scriptorium, Ltd.*, 560 F.3d 199 (4th Cir. 2009) (finding a violation of the Stored Communication Act when a company improperly accessed an employee's personal email account (on AOL) that she had used "to conduct business from time-to-time"); *Guard Pub. Co.* v. *N.L.R.B.*, 571 F.3d 53 (D.C. Cir. 2009) (unfair labor relations practice in inconsistent enforcement of email policy against union organizer using company email system to communicate with other union members at company).

When the lines between personal and professional blur, the extent to which employees understand the scope of such policies or consent to be bound by such policies also comes into doubt. Petitioners themselves recognize that the expectation of privacy may vary depending on whether the officers using the pagers were off duty or on. (Pet'r Br. 31.) In *Pure Power Boot Camp*

Inc., 587 F. Supp.2d 548, the court noted that "[i]mplied consent, at a minimum, requires clear notice that one's conduct may result in a search being conducted of areas which the person has been warned are subject to search." *Id.* at 561. Where the employee merely left his personal email account password and username on company computers, the court thus "reject[ed] the notion that carelessness equals consent". *Id.* at 561. Although said of a waiver for failure to secure a password to a private email account, the same logic could easily apply to all unread workplace privacy policies. *Curto*, 2006 WL 1318387 at * 6 ("[n]ot only is the wording in the policy at issue ambiguous as to whether [employer] will conduct audits, because Plaintiff worked at home, …any such monitoring would have had to be preceded by notice to Plaintiff.").

In the context of a Fourth Amendment inquiry into a school teacher's expectation of privacy in her emails, *Brown-Criscuolo* set forth the following four-part test:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or email, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?

601 F. Supp. 2d at 449, citing *In re Asia Global Crossing, Ltd.*, 322 B.R. at 257-58. In this case, the OPD had a formal policy covering emails on the network but no formal policy concerning use of the pagers and related

texts transmitted outside the OPD network. To the extent there was an informal policy announced at a meeting (which Officer Quon said he did not recall) extending the privacy rules to the pagers, the existence of that informal policy would have to be reconciled with the actual practice of allowing officers (not simply Officer Quon) to preserve privacy rights simply by paying for overages. Although there is, as yet, no uniformity among the precedents on how to define the scope of employee privacy, the suggestion of the United States Government (Amicus Br. 14), that employees have no privacy rights except those granted by the employer is at odds with a considerable and growing body of precedent that the employer (public or private) must define the scope of its own needs, provide notice to the employee, and then act in accordance with its policy by enforcing it with some consistency. (*See* Pet'r Br. 29, suggesting a sender or recipient of text messages on a government employer's equipment may never have a legitimate expectation of privacy.)

C. *It Is Not Yet Possible to Assess What Scope of Employee Privacy "Society Is Prepared to Accept"*

Petitioners' contend that a "reasonable expectation of privacy" is best defined as "one that society is prepared to accept" (Reply in Supp. of Pet. for Cert. 9). Yet, the emerging body of statutory and regulatory guidelines, and case law precedents (which are often in conflict) suggests that no clear pronouncement can now be made whether or to what extent society has made any judgments as to the reasonableness of the expectation of privacy in most new forms of

communications, data collection and storage. Although the basic proposition is clear that reasonable employer workplace rules can and will be enforced, at the margins continued evolution of the law in this area will no doubt yield a clearer picture. Employers remain free in the meantime to experiment with new and differing policies. Consistent with the case-by-case approach endorsed in *O'Connor* v. *Ortega*, there is no need to draw any broad rules now.

At least two states, Delaware and Connecticut, recently have enacted statutes requiring notice of monitoring of employees' electronic communications. DEL. CODE ANN. Tit. 19, § 705 (2010); CONN. GEN. STAT. ANN. § 31-48D (West 2010). Likewise, as the court noted in *Stengart:* "Here we make no attempt to define the extent to which an employer may reach into an employee's private life or confidential records through an employment rule or regulation. *Ultimately these matters may be a subject best left for the Legislature*." 973 A.2d at 401. In short, federal and state law (statutory and common law) continue to evolve, creating an uncertain foundation on which to decide whether there has been any "societal judgment" on reasonableness.

In a related field of privacy protection, the Federal Trade Commission currently is considering possible rule-making to govern collection of personal data regarding internet use, so as to require heightened standards of "notice and consent" before such data regarding individual usage patterns can be used in targeting advertising at internet users. *See e.g.* FTC Staff Report, *Self Regulatory Principles for Online Behavioral Advertising* (February 2009), *available at*:

http://www/ftc/gpv/os/2009/02/P085400behavadreport.pdf. Expressing concern that there be fair notice and choice, the FTC states:

> Every website where data is collected for behavioral advertising should provide a clear, concise, consumer-friendly, and prominent statement that (1) data about consumers' activities online is being collected at the site . . . and (2) consumers can choose whether or not to have their information collected for such purpose. The website should also provide consumers with a clear, easy-to-use, and accessible method for exercising this option.[8]

See In re Sears Holdings Management Corp. v. FTC, No. C-4264 F.T.C. 082 3099 (Settlement announced June 4, 2009) (Sears over-reaching in collecting personal data concerning individuals' on-line browsing activity without proper notice and consent).

---

8. The FTC is currently engaged in Town Hall fact finding meetings to determine the extent to which individuals may need to assent affirmatively to tracking of their on-line behavior. David Vladeck, director of the FTC's Bureau of Consumer Protection, recently explained: "We're worried that consumers don't really know what information about their online browsing is being tracked . . . So our goal is to figure out how we can inject greater transparency, accountability and consumer control into this process." 15 *Electronic Commerce & Law Report* 145 (BNA Jan. 27, 2010). FTC Chairman Jon Liebowitz is also quoted as supporting "opt-in" consent as a condition to collecting and using such data. *Id.*

In determining what scope of employee privacy society is prepared to accept, what level of access employers genuinely need, or how to balance the two, some empirical research would be relevant to show (i) the extent to which employers have and enforce written policies; and (ii) the levels of employee awareness and understanding of or adherence to such policies. More comprehensive research of the nature and extent of abuses of such policies would also illuminate the actual risks presented to employers and employees, which may well vary by the nature of the work environment; by the nature of the industry, by levels of employee seniority or responsibility, and so forth. However, the record is bereft of such information. Although such empirical research might be most appropriate as a subject for legislative rather than judicial review, the difficulty of making any pronouncement whether there has been any "societal judgment" on reasonableness of employee expectations or the extent of employee or employer expectations, counsels caution in rendering any broad decision now.

D. *The Potential for Public Review Under Public Records Laws Differs Little From Electronic Discovery Rules in Setting Expectations of Privacy*

The NYIPLA does not express an opinion on the interpretation of the California Public Records Act ("CPRA") (Cal. Gov't Code § 6250 et seq.) or whether it precludes a finding that Respondents had a reasonable expectation of privacy in their text messages. Nonetheless, the NYIPLA believes it appropriate to comment on the parallel between the risk of potential

exposure under public records laws in the government employment context and the risk of potential exposure of otherwise non-public communications and other records under emerging practices governing electronic discovery, a risk that confronts both government and private employers and employees. *See Brown-Criscuolo*, 601 F. Supp.2d at 449-50 (reasonable expectation of privacy in school teacher's password-protected email files notwithstanding that school privacy policy specified that such records "may be discoverable" under Connecticut public records laws).

As ever-more electronic records are created by employees on mobile devices and in Web 2.0 interactive applications, employers increasingly are required to develop internal rules of document management (even in the face of radically reduced storage costs for electronic records). Somewhat paradoxically, incentives also increasingly arise for employers to *decline* to exercise control over certain such technologies, lest essentially private communications become part of the company records. Courts now are asked to decide whether businesses should be required to preserve and produce records created by employees when not physically at work and when, arguably, not within the scope of their employment duties. Were Officer Quon to have used his pager to express his personal disapproval of certain office policies, or to comment on other matters internal to the OPD but of public concern, difficult questions could arise whether his personal views were a fair subject of potential disclosure by virtue of nothing more than the fact that he used the most convenient device available as a tool to express (privately) his personal views. *See*, *e.g.*, *Pietrylo*, 2008 WL 6085437

(employee created MySpace account for other employees to vent criticisms of the employer). *Accord*, *Konop* v. *Hawaiian Airlines*, *Inc.*, 302 F.3d 868 (9th Cir. 2002).

The duty to preserve electronic records that may be requested in discovery reaches all electronic records within an employer's possession, custody or control, Federal Rules of Civil Procedure Rule 34, a duty defined broadly by the Advisory Committee. FED. R. CIV. P. 34 Advisory Committee's note. However, some courts, asked to order the production of electronic records, have begun to observe that simply because a record exists and can be retrieved does not make it sufficiently relevant to an area of legitimate inquiry to compel disclosure. *Rozell* v. *Ross-Holst*, 2006 WL 163143 at * 4; *Mackelprang* v. *Fidelity Nat'l Title Agency of Nev.*, *Inc.*, No. 2:06-cv-00788, 2007 WL 119149 (D. Nev. Jan. 9, 2007). Federal Rules of Civil Procedure Rule 26(c) similarly gives courts discretion to limit discovery to prevent undue burden, embarrassment and the like. Just so, text messages exchanged by an officer such as Quon at or about the time of a SWAT intervention could be relevant and subject to disclosure in the face of a public inquiry about that incident, even if unrelated messages sent or received when off-duty were not. However, uncertainty as to the proper bounds of records fairly within an employer's control nonetheless may require (minimally) that such records be secured and maintained.

It may well be, as the Petitioner asserts, that an officer reasonably can anticipate department or public review of a shooting or other controversial incident. However, with the scope of relevant information defined,

it is possible to filter out plainly personal messages when searching for what is relevant. The need for review of messages exchanged proximate to a controversial event need not automatically sweep in messages sent at other times, when the officer is off-duty.[9] That there will always be a need for line drawing does not mean that lines should be drawn arbitrarily or without regard to actual expectations. The very basis for the holding in *O'Connor* was the recognition that such lines would have to be drawn on a case-by-case basis. Indeed, it is perhaps a tautology to observe that privacy is by its very nature idiosyncratic and uniquely personal. This in turn creates an incentive for private businesses and governmental bodies to clarify their own privacy policies, to educate employees on proper usage, and to monitor social and technical developments to use "best practices."

In a similar manner, in cases interpreting the Freedom of Information Act, this Court has often recognized and protected privacy interests in materials such as deportation records, *U.S. Department of State v. Ray*, 502 U.S. 164, 112 S. Ct. 541 (1991); investigatory photographs, *National Archives and Records Administration v. Favish*, 541 U.S. 157, 124 S. Ct. 1570 (2004), and previously published arrest information, *Department of Justice v. Reporters Committee for*

9. Even independent of privacy issues, basic relevance-based line drawing reveals that simply because records exist in electronic format they can not automatically be subject to public disclosure. For instance, a public inquiry concerning a SWAT shooting incident on some given day need not compel public exposure of unrelated text messages the same day or even the same hour concerning a SWAT intervention in an unrelated private domestic dispute.

Freedom of the Press, 489 U.S. 749, 109 S. Ct. 1468 (1989). *See also*, *Bloomberg*, 357 F. Supp. 2d at 164 (SEC chairman's electronic calendar was not an "agency record" where agency permitted limited use of office equipment for personal needs); *Howell Educ. Ass'n. MEA/NEA* v. *Howell Bd. Of Educ.*, No. 288977, 2010 WL 290515 (Mich Ct. App. Jan. 26, 2010) (mere possession by the government of personal emails of public school employees does not render them public records under Michigan FOIA).

Line drawing between company or government data, on the one hand, and private data, on the other, is becoming and will continue to be critical, particularly as private companies and government entities seek to implement and maintain document retention policies. When an employee uses her office-issued computer to access a private email account to question company policy that even she has publicly upheld in her capacity as an employee, must the company produce such records in litigation? Must the employer store such records or place them under a litigation hold simply because the company may have the ability to monitor the personal email traffic? It is and will continue to be a matter of great concern whether businesses (including government entities) are responsible or (for purposes of Fed. R. Civ. P. Rule 34) have "control over" information stored in cloud computing; employee postings on Facebook, Twitter, LinkedIn and so forth. Similar questions may arise concerning personal data stored in separate folders on the hard drive of an office-issued computer, phone records from a cell phone paid for by the employer or instant-messages on an office-issued PDA.

As with private litigants, it is one thing for government employees to expect that such electronic records may be reviewed by a magistrate under the non-routine circumstance of a litigation or public records inquiry; it is another thing to say such records can or should be searched routinely or without cause or produced to third parties or adversaries. The mere "potential" for public review can not be the touchstone of a reasonable expectation of privacy as the Petitioners suggest (Pet'r Br. 40), because all electronic records can potentially become public – through unauthorized access or even lawful means, such as a potentially overbroad discovery response or inadvertent disclosure. Simply because privacy protection may be imperfect need not defeat the expectation entirely. That we all risk losing privacy protection does not mean we are unreasonable (despite the risks) in expecting otherwise. It is the reasonableness of the risk of lawful disclosure that is relevant, and here the analysis becomes entirely circular.

The NYIPLA shares completely the sentiment of Petitioners that "[t]his Court should take this opportunity to restore reasonableness and common sense to *O'Connor's* 'operational realities of the workplace standard.'" Where the NYIPLA has less confidence, however, is whether, on the facts and questions presented by this case, any broad rules can yet be enunciated as to when an individual has a reasonable expectation of privacy in a mobile communications device or other means of private communications using employer-provided equipment or networks not clearly delineated or enforced under the applicable company or government privacy policy. As the

United States notes in its amicus brief (Amicus Br. 18) employers (public and private) do face unique risks from networked devices. For just this reason, employers need to assess those risks and develop and implement policies consistent with their identified needs.[10] Employees who later disregard such policies may have little or no ground for complaint.

In *O'Connor*, this Court rejected "the contention . . . that public employees can never have a reasonable expectation of privacy in their place of work," 480 U.S. at 717, finding instead that "Given the great variety of work environments, . . . the question whether an employee has a reasonable expectation of privacy must be addressed on a case-by-case basis." *Id.* at 718. The variety and complexity of "work" environments today is changing so rapidly as to be unrecognizable to the *O'Connor* Court one generation ago. It will likely be equally unrecognizable to other courts another decade hence. For just these reasons, no broad rule is now appropriate nor can any certain or sweeping judgments be made what expectations employees have of privacy in such new and evolving circumstances or what "societal judgments" on reasonableness are appropriate.

---

10. Similarly, although the amicus, National School Boards Association, expresses concerns regarding the ability of schools to monitor their teachers, it does not address the simple prophylactic that schools can develop and implement clear rules. Curiously, the brief nowhere mentions *Brown-Criscuolo* v. *Wolfe*, *supra*, recognizing in a Fourth Amendment context that a school teacher may have a reasonable expectation of privacy in her emails.

Consistent with *O'Connor*, this case is not an appropriate vehicle in which to adopt any broad rules governing workplace privacy rights in mobile communications devices or in the absence of a formal office policy of which employees have notice and which is enforced. As noted, the only policy here even arguably applying to the subject pagers was an informal verbal policy that was at odds with actual office practice. The record provides no evidence of instances in which the informal policy was actually enforced prior to the review of Respondents' email messages precipitating this litigation.

CONCLUSION

For the foregoing reasons, the holding of the Ninth Circuit should be affirmed or the matter should be remanded to resolve any uncertainties as to what was the policy and to what extent it was enforced.

Respectfully submitted,

MARK J. ABATE
President
New York Intellectual Property Law Association
GOODWIN PROCTER LLP
620 Eighth Avenue
New York, NY 10022
(212) 355-3333

JONATHAN E. MOSKIN
Counsel of Record
FOLEY & LARDNER LLP
90 Park Avenue
New York, NY 10016
(212) 682-7474
JMoskin@foley.com

Counsel for Amicus Curiae