LEADING CASES

I. CONSTITUTIONAL LAW

A. Criminal Law and Procedure

1. Fourth Amendment — Reasonable Expectation of Privacy. — Over two decades ago, in *O'Connor v. Ortega*,[1] the Supreme Court attempted to provide guidance on the scope of the Fourth Amendment's privacy protection for government employees in the workplace. Although the *O'Connor* Court ruled that public employees retain their Fourth Amendment rights, the Justices splintered regarding the proper standard for delineating those rights.[2] Last Term, in *City of Ontario v. Quon*,[3] the Supreme Court used *O'Connor* as guidance to hold — on the specific set of facts in the case — that a police chief did not violate the Fourth Amendment by auditing a SWAT team member's messages sent from a government-issued pager.[4] Yet instead of clarifying whether a government employee enjoys a reasonable expectation of privacy when using government-issued equipment, the Court provided no helpful guidance for similar cases in the future, declining to decide whether the Fourth Amendment provides such a reasonable expectation in technological contexts. Although the Court would prefer to allow technological norms to develop before crafting rigid rules, its reluctance to devise an intelligible principle for Fourth Amendment rights regarding technology will have the negative effect of causing lower courts to rely on *O'Connor* to an even greater extent. Because the *O'Connor* test is flexible and fact-specific, judges will often be able to reach whatever conclusion they want. The Court should have ruled

---

[1] 480 U.S. 709 (1987).

[2] A four-Justice plurality, led by Justice O'Connor and joined by Chief Justice Rehnquist and Justices White and Powell, held that a two-step analysis applies: First, a court must consider the "operational realities of the workplace," *id.* at 717 (plurality opinion), to determine whether a government employee's constitutional rights are implicated in his or her specific government office. *Id.* at 717–18. Second, in situations where an employee does have a legitimate privacy expectation, "public 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." *Id.* at 725–26. In a concurring opinion, Justice Scalia posited that "[i]t is privacy that is protected by the Fourth Amendment, not solitude." *Id.* at 730 (Scalia, J., concurring in the judgment). As a result, Justice Scalia suggested that the Fourth Amendment should protect the privacy of government employees in the workplace as a general matter and "that government searches to retrieve work-related materials or to investigate violations of workplace rules . . . do not violate the Fourth Amendment." *Id.* at 732.

[3] 130 S. Ct. 2619 (2010).

[4] *Id.* at 2633.

that public employees do not enjoy a reasonable expectation of privacy when sending text messages from government-issued devices.

In October 2001, the City of Ontario, California, purchased two-way alphanumeric pagers for its employees, including Jeff Quon, a member of the police department's SWAT team.[5] The City issued pagers to SWAT team members specifically to improve their coordination and responsiveness.[6] As part of the City's contract with its pager service provider, Arch Wireless, each employee had a monthly limit of 25,000 characters; Arch Wireless charged overage fees if an employee used more than the allotted character amount.[7]

Although the Ontario police department had a policy in place providing that "[u]sers should have no expectation of privacy or confidentiality" when using the internet or sending emails on city-owned computers[8] and prohibiting "inappropriate, derogatory, obscene, suggestive, defamatory, [and] harassing language in the e-mail system,"[9] the policy made no explicit reference to pagers. Instead, Lieutenant Steven Duke, the officer responsible for the Arch Wireless contract, made verbal comments to the police department's staff — and to Quon in particular — that pager messages would be considered email messages under the City's policy, and thus were eligible for auditing.[10] In practice, however, Lieutenant Duke would not audit employees' pager messages whenever overages occurred so long as employees paid the overage fees out of pocket.[11] During the first several months after the pagers were issued, "Quon exceeded his character limit three or four times," and paid the City for his overages each time.[12] Eventually, Lieutenant Duke told Chief Lloyd Scharf that he was "tired of being a bill collector,"[13] and Chief Scharf "decided to determine whether the existing character limit was too low"[14] for official use. Chief Scharf subsequently ordered an audit of transcripts of pager messages sent by Quon and by another employee who had incurred multiple overages.[15]

An internal affairs officer's report revealed that out of 456 messages Quon sent during work hours in August 2002, "no more than 57

---

5 Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1122–23 (C.D. Cal. 2006).

6 *Id.* at 1123.

7 *Id.*

8 *Id.*

9 *Id.* at 1124.

10 *Quon*, 130 S. Ct. at 2625; *Arch Wireless*, 445 F. Supp. 2d at 1124. These statements were later memorialized in writing. *Id.*

11 *Arch Wireless*, 445 F. Supp. 2d at 1124–25.

12 *Quon*, 130 S. Ct. at 2625.

13 *Id.* at 2626 (citation omitted) (internal quotation marks omitted).

14 *Id.*

15 *Id.* The police department obtained the transcripts from the service provider, Arch Wireless. *Id.*

were work related."[16] Furthermore, on average, Quon sent or received only three work-related messages per workday.[17] Instead of using the pager mostly for SWAT communications, Quon sent many sexually explicit messages during work hours both to his estranged wife and to his mistress, a female officer on the force.[18] Quon was allegedly disciplined for his use of the city-issued pager[19] and brought suit against the City of Ontario, alleging violations of his Fourth Amendment right to privacy and the Stored Communications Act[20] (SCA), and against Arch Wireless, alleging violations only of the SCA.[21]

The district court found that any lessened expectation of privacy as a result of the pager's belonging to the City "was canceled out by what the City, through Lieutenant Duke, communicated to its officers on how they could use that equipment."[22] As for the reasonableness of the audit, however, the district court recognized that the proper result depended on the purpose of the audit: If the purpose was to see whether Quon was using his pager to "waste time," then the audit was not reasonable. However, if the purpose was to determine whether the existing character limit was sufficient so that officers were not paying for work-related costs, then the audit was reasonable.[23] Following a jury determination that Chief Scharf had ordered the audit to evaluate the character limit, the district court entered judgment in favor of the City on Quon's Fourth Amendment claim.[24]

The Ninth Circuit affirmed in part, reversed in part, and remanded for further proceedings.[25] Judge Wardlaw, writing for the panel, agreed with the district court that Quon had a reasonable expectation of privacy in the pager messages, but held that "the issue regarding Chief Scharf's intent in authorizing the search never should have gone to trial because the search was unreasonable as a matter of law."[26] Although the circuit court held that Lieutenant Duke's search was reasonable "at its inception"[27] per *O'Connor*, the court held that "the search was not reasonable in scope."[28] In doing so, Judge Wardlaw interpreted *O'Connor*'s prescription — that a search's measures be "rea-

---

[16] *Id.*
[17] *Id.*
[18] Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1126 (C.D. Cal. 2006).
[19] *Quon*, 130 S. Ct. at 2626.
[20] 18 U.S.C. §§ 2701–2712 (2006).
[21] *Quon*, 130 S. Ct. at 2626.
[22] *Arch Wireless*, 445 F. Supp. 2d at 1142.
[23] *Id.* at 1146.
[24] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 899 (9th Cir. 2008).
[25] *Id.* at 911.
[26] *Id.* at 903.
[27] *Id.* at 908 (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987) (plurality opinion)) (internal quotation marks omitted).
[28] *Id.*

sonably related to the objectives of the search and not excessively intrusive"[29] — to mean that "if less intrusive methods were feasible . . . the search would be unreasonable."[30]

The Supreme Court reversed and remanded.[31] Writing for the Court, Justice Kennedy[32] reasoned that regardless of which approach from *O'Connor* the Court applied — the four-Justice plurality's two-part test or Justice Scalia's approach — the result would be the same.[33] Justice Kennedy explained that an inquiry into the "operational realities" of Quon's workplace would involve probing questions about what Lieutenant Duke said about the application of the City's policy toward pagers, as well as questions about whether searches of pager messages sent on City equipment could be justified for other reasons.[34] The Court noted that it must "proceed with care"[35] when addressing the issue of privacy expectations with respect to communications made on government-issued electronic equipment: the evolution of technology and of technological norms makes it difficult for the Court to predict "how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable."[36] As a result, the Court opted to decide the case on narrower grounds, assuming arguendo that Quon had a reasonable expectation of privacy in the pager messages sent on his city-issued device.[37]

Justice Kennedy then explained that even if Quon had a reasonable expectation of privacy, "[the City] did not necessarily violate the Fourth Amendment by obtaining and reviewing the transcripts."[38] Per *O'Connor*, the Court noted, a warrantless search of a government employee in his workplace conducted for a "noninvestigatory, work-related purpos[e]" is reasonable if it is "justified at its inception" and if "the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of" the circumstances giving rise to the search.[39] Regarding the "justified at its inception"

---

[29] *Id.* (quoting *O'Connor*, 480 U.S. at 726 (plurality opinion)).

[30] *Id.* (quoting Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1336 (9th Cir. 1987)) (internal quotation mark omitted). The Ninth Circuit also held that Arch Wireless violated the SCA. *Id.* at 903; *see also Quon*, 130 S. Ct. at 2627. The Supreme Court denied certiorari on this issue. USA Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (2009).

[31] *Quon*, 130 S. Ct. at 2633.

[32] Justice Kennedy was joined in full by all of the Justices except Justice Scalia, who joined in all but Part III-A.

[33] *Quon*, 130 S. Ct. at 2628–29.

[34] *Id.* at 2629.

[35] *Id.*

[36] *Id.* at 2630 (citing O'Connor v. Ortega, 480 U.S. 709, 715 (1987) (plurality opinion)).

[37] *Id.*

[38] *Id.*

[39] *Id.* (alteration in original) (quoting *O'Connor*, 480 U.S. at 725–26 (plurality opinion)).

prong, Justice Kennedy explained that a jury and the Ninth Circuit agreed that the audit was for work-related purposes: "The City and [the police department] had a legitimate interest in ensuring that employees were not being forced to pay out of their own pockets for work-related expenses, or on the other hand that the City was not paying for extensive personal communications."[40] As for the search's scope, the Court held that the search was not "excessively intrusive."[41] Although Quon had gone over his monthly character limit several times, the search covered transcripts for only two months.[42] Furthermore, the transcripts were redacted to show only those messages sent while Quon was on duty — "a measure which reduced the intrusiveness of any further review of the transcripts."[43] Justice Kennedy explicitly took issue with the Ninth Circuit's interpretation of controlling precedent, noting that the Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."[44] Judges examining a case with the benefit of hindsight, Justice Kennedy explained, "can almost always imagine some alternative means by which the objectives of the government might have been accomplished."[45]

Justice Stevens concurred.[46] While he agreed with the Court's opinion, he wrote separately "to highlight that the Court has sensibly declined to resolve whether the plurality opinion in [*O'Connor*] provides the correct approach to determining an employee's reasonable expectation of privacy."[47] Justice Stevens pointed out that Justice Blackmun — who had agreed with Justice Scalia that an employee enjoys a reasonable expectation of privacy in the workplace — advocated an alternate approach in his dissent in *O'Connor*: that "the precise extent of an employee's expectation of privacy often turns on the nature of the search."[48] Thus, Justice Blackmun's analysis would focus on the specific circumstances of each particular search and would reject a categorical standard.[49] Justice Stevens concluded that under any of the three approaches identified in *O'Connor*, the result would be

---

[40] *Id.* at 2631.

[41] *Id.* (quoting *O'Connor*, 480 U.S. at 726 (plurality opinion)) (internal quotation marks omitted).

[42] *Id.*

[43] *Id.*

[44] *Id.* at 2632 (quoting Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 663 (1995)) (internal quotation marks omitted).

[45] *Id.* (quoting Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 629 n.9 (1989)) (internal quotation mark omitted).

[46] *Id.* at 2633 (Stevens, J., concurring).

[47] *Id.* (citation omitted).

[48] *Id.* (quoting O'Connor v. Ortega, 480 U.S. 709, 738 (1987) (Blackmun, J., dissenting)) (internal quotation marks omitted).

[49] *Id.*

the same. The decision of the Ninth Circuit should therefore be reversed.[50]

Justice Scalia concurred in part and concurred in the judgment.[51] He disagreed that courts should continue to use the "operational realities" rubric from *O'Connor* to determine whether a public employee has a reasonable expectation of privacy.[52] Instead, Justice Scalia argued, "the proper threshold inquiry should be not whether the Fourth Amendment applies to messages on *public* employees' employer-issued pagers, but whether it applies *in general* to such messages on employer-issued pagers."[53] In this case, the Court had no need to address this threshold inquiry, as "the city's search was reasonable, and thus did not violate the [Fourth] Amendment."[54] Given that posture, Justice Scalia criticized the Court for nonetheless expostulating on the difficulty of determining privacy expectations for emerging technologies:

> Applying the Fourth Amendment to new technologies may sometimes be difficult, but when it is necessary to decide a case we have no choice. The Court's implication that where electronic privacy is concerned we should decide less than we otherwise would . . . is in my view indefensible. The-times-they-are-a-changin' is a feeble excuse for disregard of duty.[55]

Furthermore, Justice Scalia suggested that by laying out an "instructive" explication of how *O'Connor* would apply under the circumstances of this case, the Court inadvertently sanctioned a specific test for lower courts to apply.[56] Justice Scalia noted that ironically, in recognizing the difficulty in applying the *O'Connor* plurality's standard to new technologies, "the Court underscores the unworkability of that standard."[57]

The Court's decision in *Quon* is a striking example of courts' recent difficulty in handling the intersection of the Fourth Amendment with technology.[58] In declining to decide the expectation of privacy ques-

---

[50] *Id.* at 2634.

[51] *Id.* (Scalia, J., concurring in part and concurring in the judgment).

[52] *Id.*

[53] *Id.* (citing *O'Connor*, 480 U.S. at 731 (Scalia, J., concurring in the judgment)).

[54] *Id.*

[55] *Id.* at 2635 (citation omitted).

[56] *Id.* (quoting *id.* at 2629 (majority opinion)) (internal quotation marks omitted).

[57] *Id.*

[58] For another example of courts' struggle in reconciling technology and the Fourth Amendment, see Recent Case, *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc), 123 HARV. L. REV. 1003, 1007–10 (2010), which argues that the Ninth Circuit overreacted to an unreasonable search and seizure in the digital context. In addition, compare *United States v. Maynard*, Nos. 08-3030, 08-3034, 2010 WL 3063788, at *1, *7–18 (D.C. Cir. Aug. 6, 2010), which held that warrantless use of a GPS tracking device violated the defendant's reasonable expectation of privacy, with *United States v. Pineda-Moreno*, 591 F.3d 1212, 1214–17 (9th Cir. 2010), which held that individuals have no reasonable expectation of privacy in their movements through public spaces and allowed the use of warrantless GPS tracking.

tion in *Quon* on more principled grounds, the Court has provided no more guidance than did *O'Connor* — a case that did *not* involve technological issues — more than two decades ago. In fact, by declining to apply the *O'Connor* "operational realities" test where issues of technology are involved and opting instead to evaluate Fourth Amendment cases involving technology on a case-by-case basis, Justice Kennedy opened the door to *O'Connor*'s continued application in such circumstances and inevitably to inconsistent results on account of the flexibility of *O'Connor*'s fact-specific approach. Essentially, the Court has left the issue for future litigants and future Justices to solve. Instead, the Court should have ruled that government employees have no reasonable expectation of privacy in text messages sent from a government-issued device.[59]

There exists a perplexing irony in this case: the "new technology" at issue in *Quon* consisted of two-way pager devices that were issued to employees a decade ago and that would likely be deemed antiquated by today's teenagers and young professionals. Pagers are undoubtedly not an "emerging technology" with which the Court must "proceed with care";[60] presumably, societal norms with respect to pagers are as developed as they will ever be. Similarly, while mobile devices have become more advanced over time, societal norms with respect to text messaging are arguably developed enough for the Court to decide whether sending text messages on government-issued devices constitutes activity covered by the Fourth Amendment. In this case in particular, Quon's pager was issued by the City (through a service provider for which the City, not Quon, was the subscriber) and given to Quon for work-related purposes. Such devices cannot objectively reach the level of "self-expression" or "self-identification" posited by Justice Kennedy in his opinion.[61] If anything, Quon's pager was a city-issued tool for police-related duties, much like a police officer's patrol cruiser or sidearm.[62] Yet instead of crafting an instructive guide for lower courts to follow that was tailored to narrow categories of technological use, the Court seemed to suggest that nearly any technological advancement can be considered "emerging." Such an ap-

---

[59] In her dissent from the Ninth Circuit's denial of rehearing en banc, Judge Ikuta stated that she would have used the principles from the *O'Connor* plurality to hold that police officers do not enjoy a reasonable expectation of privacy in text messages sent from a government pager: "[Such] principles establish that Quon's expectation of privacy in the text messages . . . was either significantly diminished or non-existent." Quon v. Arch Wireless Operating Co., 554 F.3d 769, 776 (9th Cir. 2009) (Ikuta, J., dissenting from denial of rehearing en banc).

[60] *Quon*, 130 S. Ct. at 2629.

[61] *Id.* at 2630.

[62] *See, e.g.*, DeMaine v. Samuels, No. 00-9372, 2002 WL 243113, at *2–3 (2d Cir. Feb. 15, 2002) (summary order) (applying the *O'Connor* test to hold that a state police detective does not enjoy a reasonable expectation of privacy in his desk or state-issued patrol car).

proach is unlikely to ever lead to more principled decisions at the crossroads of technological advancement and the Fourth Amendment.

Contrary to the Court's assertions, applying the *O'Connor* standard on a case-by-case basis to determine whether a reasonable expectation of privacy exists is often not difficult when technology with relatively developed norms is at issue. Courts have applied *O'Connor* with little difficulty in cases involving computer usage; in many such cases, the government employer had a computer usage policy in place. In *Biby v. Board of Regents*,[63] for example, the Eighth Circuit noted that one relevant factor from *O'Connor* in determining whether an employee enjoys a reasonable expectation of privacy in the workplace is the existence of a privacy policy.[64] Biby's employer, the University of Nebraska, sought to produce files from Biby's computer in the course of litigation.[65] As the university had a policy informing users "not to expect privacy if the university has a legitimate reason to conduct a search,"[66] the Eighth Circuit held that the search did not violate Biby's Fourth Amendment rights.[67]

In another case, *United States v. Simons*,[68] a CIA employee had downloaded child pornography onto his computer at work, which system administrators found while conducting a test of a system firewall.[69] Citing *O'Connor*, the United States District Court for the Eastern District of Virginia noted that "public employees' expectations of privacy in their offices, desks, and file cabinets[] may be reduced by actual office practices and procedures."[70] In Simons's case, a computer policy authorized audits "to support identification, termination, and prosecution of unauthorized activity."[71] As a result, the court found that Simons had no reasonable expectation of privacy "with regard to any Internet use."[72]

Thus, the Court in *Quon* was not sufficiently precise in discussing the broad issue of technology: technological norms may be more developed in some instances (for example, desktop computers in a government workplace), but less developed in others (for example, a cellular phone partially paid for by a government employer). One might argue that the "norms" in *Biby* and *Simons* are actually idiosyncratic consequences of a government employer's having a computer usage policy

---

63 419 F.3d 845 (8th Cir. 2005).
64 *Id.* at 850.
65 *Id.* at 847.
66 *Id.* at 850.
67 *Id.* at 851.
68 29 F. Supp. 2d 324 (E.D. Va. 1998).
69 *Id.* at 325–26.
70 *Id.* at 327.
71 *Id.*
72 *Id.*

in place, or that such policies play a role in employees' consent and do not eliminate a reasonable expectation of privacy.[73] Nonetheless, those cases — coupled with the fact that many government employees likely have their own personal cellular phones, personal digital assistants, or personal computers at home[74] — raise the question of whether government employees have or should have any "subjective expectation of privacy . . . that society is prepared to accept as objectively reasonable"[75] with respect to technological equipment provided exclusively by their employer for a specific work-related purpose, whether or not the employer has an official policy in place. While it may be true that technological advances and the increased availability of advanced mobile handsets to individual consumers have blurred the line between private life and the workplace,[76] it does not necessarily follow that a user has a reasonable expectation of privacy on workplace equipment provided by the employer. The fact that a public employee may have a desire or the ability to issue personal communications while at work does not itself make such conduct proper, nor does it generate a reasonable expectation of privacy under the Fourth Amendment. In fact, the proliferation of technology — along with the increased ease with which employers can access information on employer-issued equipment — could make users more conscious of what activity is appropriate on personal equipment versus employer equipment and could thereby inform their privacy expectations.[77] In this context, it is in-

---

[73] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1031 (2010) ("Terms of Service may have a role in defining Fourth Amendment rights as well, although I believe their role is in determining whether a user has consented or given [a] provider third-party consent rights, not whether the provisions in a Terms of Service eliminate a reasonable expectation of privacy."). Professor Kerr seems not to consider the idea, however, that if every employer adopted similar policies restricting users' privacy expectations on workplace equipment, then there would presumably be no subjective expectation of privacy that society could deem reasonable: it would be the rare exception that a user maintained her privacy on workplace equipment. Not all employers currently maintain such policies, of course, but an increasing number choose to do so. *See infra* note 77.

[74] The Court in *Quon* noted that "the ubiquity of [such] devices has made them generally affordable, so one could [argue] that employees who need cell phones or similar devices for personal matters can purchase and pay for their own." *Quon*, 130 S. Ct. at 2630.

[75] United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (citing California v. Greenwood, 486 U.S. 35, 39 (1988)).

[76] *See* John Soma et al., *Bit-Wise But Privacy Foolish: Smarter E-messaging Technologies Call for a Return to Core Privacy Principles*, 20 ALB. L.J. SCI. & TECH. 487, 494–95 & n.22 (2010); Amanda R. Higgins, *Not So Fast:* Quon v. Arch Wireless *Is Not Employees' License to Text the Workday Away*, OKLA. J.L. & TECH., Apr. 29, 2010, at 26, www.okjolt.org/images/pdf/2010okjoltrev48.pdf (positing that the "natural desire" for employees to communicate with others at home and at work, along with the technology that makes it possible to do so easily, blurs the line between public and private communications).

[77] A 2009 survey by the Society of Corporate Compliance and Ethics and the Health Care Compliance Association revealed that while 50% of employees surveyed reported that their companies have no policy for online activity in place, 34% reported that their companies have a gen-

structive to note that, mechanically, accessing one's personal web-based email account while at work[78] and sending personal communications via an employer-issued device are quite different: The former is protected by a personal password and ultimately sent, stored, and received via a third party's servers. The latter, by contrast, is protected by the employer's password system and sent via servers for which the employer pays (minus overages, in Quon's case). Whether access to personal email on a work device is covered by the Fourth Amendment, however, is outside the scope of this comment. What is important to note is that there is a substantive difference between accessing one's web-based personal email account on a workplace computer and sending personal messages on an employer-issued device. These differences in control, purpose, and ownership should inform the user's expectations. Therefore, regardless of how courts interpret access to personal email on a work device, they should recognize no reasonable expectation of privacy for personal messages.

To the Court's credit, applying *O'Connor* to the facts of this case may have been particularly difficult on account of the police department's conflicting policies — official and unofficial — with respect to how city-issued pagers would be treated.[79] At bottom, however, remains the critical question of whether society is prepared to recognize an expectation of privacy in such situations as objectively reasonable. Subsequent cases involving Fourth Amendment privacy rights in the digital realm are inevitable, and the Court should prepare itself to address those issues more definitively.

---

eral policy addressing online activity and the use of social networking sites, and another 10% reported that their companies have policies specifically addressing certain types of social networking sites. *See* HEALTH CARE COMPLIANCE ASS'N & SOC'Y OF CORPORATE COMPLIANCE AND ETHICS, FACEBOOK, TWITTER, LINKEDIN AND COMPLIANCE: WHAT ARE COMPANIES DOING? 2 (2009), *available at* http://corporatecompliance.org/staticcontent/09SocialNetworksSurvey_report.pdf. Furthermore, 24% of employees surveyed reported that their companies have disciplined individuals for improper use of Facebook, Twitter, or LinkedIn. *See id.* at 4. In addition, employers in the private sector have begun to specify for employees what may and may not be discussed using social media. *See, e.g.*, Lori E. Lesser, *Social Networks and Blogs*, *in* INFORMATION TECHNOLOGY LAW INSTITUTE 2010, at 101, 158 (PLI Patents, Copyrights, Trademarks, and Literary Property, Course Handbook Series No. 23460, 2010). These trends among private employers could signal an emerging consciousness: to the extent that these norms may be evolving, they are certainly evolving toward lower expectations of privacy while using workplace technology.

[78] There is healthy debate regarding whether an employee has a reasonable expectation of privacy in her computer usage while at the workplace. *Compare* Wilson v. Moreau, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (holding that an independent contractor working on a city library enjoyed a reasonable expectation of privacy with respect to his personal Yahoo! email account accessed on a city library computer), *with* United States v. Barrows, 481 F.3d 1246, 1248–49 (10th Cir. 2007) (holding that a city employee did not enjoy a reasonable expectation of privacy in his personal computer brought into the workplace for work-related use).

[79] *See Quon*, 130 S. Ct. at 2625.