ELECTRONIC PRIVACY IN THE GOVERNMENT WORKPLACE AND *CITY OF ONTARIO, CALIFORNIA V. QUON*: THE SUPREME COURT BROUGHT FORTH A MOUSE

*Clifford S. Fishman**

* Professor of Law, The Columbus School of Law, The Catholic University of America. B.A., University of Rochester, 1966; J.D., Columbia Law School, 1969. From 1969 to 1977, Professor Fishman served as an Assistant District Attorney in the New York County District Attorney's Office and as Chief Investigating Assistant District Attorney in New York City's Special Narcotics Prosecutor's Office, where he tried dozens of cases, drafted and supervised the execution of more than forty wiretaps and eavesdrops and, among other triumphs, oversaw the purchase of the most expensive pound of pancake batter in the history of American law enforcement. Having cleaned up New York City's drug problem, he joined the faculty at Catholic University in 1977. He is the co-author of two multi-volume legal treatises which, together with his eighteen prior law review articles, contain more footnotes than any rational human being would ever read in one lifetime, let alone write. Professor Fishman expresses his gratitude to the National Center for Justice and the Rule of Law at the University of Mississippi School of Law, and to Tom Clancy, its director, for the honor of being chosen to give the James Otis Lecture in October, 2010. This Article is an outgrowth of that lecture. Prof. Fishman also wants to thank his treatise co-author, Anne T. McKenna; his research assistant, Eduardo Bertran, J.D., C.U.A. Law School, 2011; C.U.A. Law librarian Steve Young; and his C.U.A. faculty colleagues, Professors Cara Drinan and Mary Leary, for their assistance in researching and drafting this Article. Thanks, too, go to his administrative assistant, Julie Kendrick, for her help in this and in every other professional project he undertakes. Finally, Professor Fishman also wishes to acknowledge Washington, D.C.'s NFL, NBA, and MLB franchises, whose persistent mediocrity over the past few decades eliminated many distractions that might have interfered with his footnote production.

> Many years ago a mighty rumbling was heard from a mountain, which was said to be in labour. Thousands of people flocked from far and near to see what it would produce. After a long time of waiting in anxious expectation—out popped a mouse![1]

INTRODUCTION

A company gives an employee (E) a cellular phone to use on company matters. The phone is programmed to send and receive text messages. E is told that he may send and receive up to a certain number of alphanumeric characters per month, with no cost to E. The company makes a point of informing E that it reserves the right to review his use of the phone, including the text messages he sends and receives. Informally, however, his supervisor tells him that the company will not enforce this policy; instead, personal use of the phone and text messaging will be permitted, so long as E pays for any text message use that exceeds the contractual character limit per month. Does this informal understanding give E a right to privacy in the personal text messages he sends and receives? If so, and the company decides to review E's text messages, does it matter why the company did so? And what about the people who send text messages to E, and receive messages from him—do they have any right to privacy against the company's review of the messages? Does it matter whether those with whom E texts are aware that E is using a company phone, rather than his personal phone?

Suppose instead E works for a government agency—local, city, state, or federal. Would the privacy issues raised in the

---

[1] *The Mountain in Labour*, *in* AESOP'S FABLES 31 (Jack Zipes ed., 1992).

previous paragraph be resolved any differently? If so, how and why?

The Supreme Court confronted these issues in 2010 in *City of Ontario v. Quon*.[2] Sergeant Jeff Quon sued his employer, the Ontario Police Department, when he learned that the OPD reviewed the text messages he had sent and received on a department-issued pager.[3] The Ninth Circuit entered judgment for Quon;[4] the city appealed to the Supreme Court. The Court's decision in that case touches on a wide range of social, technological, and legal issues, including: (1) the role various electronic communications media play in our lives; (2) whether a government employee has a reasonable expectation of privacy when he uses equipment or systems provided by the government agency for which he or she works; (3) when, assuming such an expectation exists, the government employer is nevertheless justified in intruding upon that privacy; and (4) the legal standard against which those expectations and justifications are to be measured.

Quon is the third time the Supreme Court has addressed the issue of a government employee's right to workplace privacy from the agency that employs him or her. The first was *O'Connor v. Ortega*,[5] decided in 1987. That decision recognized an employee's rights to privacy, but provided no clear guidance as to how those rights are to be measured;[6] nor did the second decision, *National Treasury Employees Union v. Von Raab*,[7] decided in 1989, because although *Van Raab* did involve the employer-employee relationship, it is better understood when viewed from a different legal perspective.[8] When the Court granted cert in *Quon*,

---

[2] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010). *Quon* involved an alphanumeric pager, rather than a cell phone with texting capability. Cell phones with text-message capacity are probably now far more widely owned and used than pagers, and the issues presented by the text messages in *Quon* would apply equally to text messages sent by phone.

[3] *Id.* at 2621-22.

[4] Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008). See *infra* Part III.A and Part III.C for a more detailed discussion of the district court and circuit court decisions.

[5] O'Connor v. Ortega, 480 U.S. 709 (1987).

[6] See *infra* Part II for an extensive discussion of *O'Connor*.

[7] Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656 (1989).

[8] See *infra* notes 121-22 and accompanying text for discussion of *Von Raab*.

therefore, many scholars, judges, and practitioners hoped that the *Quon* decision would clarify the uncertainties left over from *O'Connor* and resolve new issues created by electronic communications technology. On the other hand, some observers feared that the Court in *Quon* might issue a broad, sweeping decision that could have a substantial, unforeseeable, and perhaps unfortunate impact on emerging communications technologies. As it turned out, *Quon* decided very little, and leaves the law more unsettled than it previously was.

This Article will begin with a very brief overview of fundamental Fourth Amendment principles and federal statutory regulation of electronic surveillance of communications. Part II consists of a detailed look at *O'Connor v. Ortega*, and the uncertainties the decision created in the law. Part III will examine the *Quon* case, and analyze what the Court did decide. Part IV examines the issues in *Quon* that the Court did *not* decide. Part V states my conclusions as to where the decision leaves the law. The Article ends with an "user's guide" to *Quon*, which outlines how litigants and judges should attempt to apply *Quon* if presented with a case involving privacy in the government or private sector workplace.

I. THE FOURTH AMENDMENT AND RELEVANT FEDERAL STATUTES

A. Fourth Amendment

1. Reasonable Expectation of Privacy

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[9]

---

[9] U.S. CONST. amend. IV.

It is clear from the language of the amendment that, to determine the scope of Fourth Amendment protection, it is necessary to define its key terms: "search" and "seizure." Application of the term "seizure" to some forms of electronic surveillance raises difficult questions,[10] but for purposes of this Article, its application is fairly straight-forward: a seizure occurs when someone acquires physical possession of either a printed or an electronic copy of a communication such as an e-mail, text message, etc.

One major focus of this Article is what constitutes a "search" in the workplace. Until the mid-1960s, legal definitions of "search," for Fourth Amendment purposes, focused upon whether a government investigator had intruded or trespassed upon a "constitutionally protected area."[11] The prevailing doctrine was

---

[10] For example, is a phone call "seized" if it is overheard by someone listening in on an extension phone or wiretap, or only when it is recorded? For a discussion of this issue, see CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 1:5 (3d. ed. 2007). Federal and state statutes regulating electronic surveillance finesse the issue by regulating, not the "seizure" of communications, but their "interception," which is defined broadly to include any "real time" acquisition of the contents of wire communications (i.e., telephone conversations), oral communications (i.e., face-to-face conversations), and electronic communications (i.e., e-mails, tweets, etc.), by means of any electronic, mechanical, or other device. *See* 18 U.S.C. § 2510(4) (2006) (definition of "intercept"). For a detailed analysis of this definition and related terms, see *id.* at §§ 2:61-2:110.

[11] *See* Hoffa v. United States, 385 U.S. 293, 301 ("What the Fourth Amendment protects is the security a man relies upon when he places himself or his property within a constitutionally protected area, be it his home or his office, his hotel room or his automobile."). The Court considered whether the government violated defendant Hoffa's Fourth Amendment rights when Edwin Partin, an acquaintance of Hoffa's, gained entrance to Hoffa's hotel room by concealing the fact that he was acting as a government informant. The Court held that no violation occurred because when Hoffa admitted Partin he assumed the risk that Partin might be an informant (Partin's testimony played a central role in convicting Hoffa of tampering with the jury in the case for which he had been on trial.). For a detailed discussion of the *Hoffa* case, see VICTOR S. NAVASKY, KENNEDY JUSTICE 418-24 (1971); *see also* Lopez v. United States, 373 U.S. 427 (1963). Lopez offered a bribe to IRS agent Davis to help resolve a tax matter; thereafter Davis went to Lopez's office, ostensibly to seal the deal, carrying a wire recorder which recorded the conversation. In upholding the admissibility of the recording, the Court commented that the Fourth Amendment protected against surreptitious electronic overhearing "only [if] the electronic device [is] planted by an unlawful physical invasion of a constitutionally protected area," *Lopez*, 373 U.S. at 348-439, and held that because Lopez had invited Davis into his office, there had been no unlawful "invasion" of the office. *Id.*; *see also* Lanza v. New York, 370 U.S. 139, 142 (1962) (holding that it did not violate the Fourth Amendment to surreptitiously record

that a Fourth Amendment "search" occurred only if the government physically intruded into such an area and thereby breached the defendant's "right to privacy."[12]

In 1967, in *Katz v. United States*, the Court rejected this "formulation" of what the Fourth Amendment protected.[13] Rather, Justice Stewart stated in his majority opinion:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[14]

Thus, the Court held that when Katz closed the glass door to a public phone booth, although he was *visible* to the public, the Fourth Amendment protected what he said from the uninvited listener.[15]

---

defendant's conversation with his brother in the visitors' room of a public jail, because that location was not a "constitutionally protected area.").

[12] The phrase "right to privacy" has a long and storied history. The phrase became common in American legal jurisprudence as a result of Samuel D. Warren and Louis D. Brandeis's famous article, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). That article is considered by many legal scholars to be the seminal work in the area of privacy rights and is still cited over a hundred years later. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514, 534 (2000); Toffoloni v. LFP Publ'g Grp., LLC, 572 F.3d 1201, 1206 (11th Cir. 2009); Brown v. Mortensen, 253 P.3d 522, 526 (Cal. 2011); Tarlton v. Kaufman, 199 P.3d 263, 273 (Mont. 2008) (Morris, J., dissenting). Interestingly enough, the phrase, "right to privacy," has also had its detractors. *See* Erin Miller, *Justice Stevens and the So-called Right to Privacy*, SUPREME COURT OF THE UNITED STATES BLOG (May 21, 2010, 3:07 PM), http://www.scotusblog.com/2010/05/justice-stevens-and-the-so-called-right-to-privacy/ (noting that the phrase "so called 'right to privacy'" first appeared in a 1902 decision by New York's highest court).

[13] Justice Stewart wrote:

> We decline to adopt this formulation of the issues. In the first place the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase "constitutionally protected area." Secondly, the Fourth Amendment cannot be translated into a general constitutional "right to privacy." That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all. Other provisions of the Constitution protect personal privacy from other forms of governmental invasion.

Katz v. United States, 389 U.S. 347, 350 (1967) (footnotes omitted).

[14] *Id.* at 351.

[15] *Id.* at 358-59.

Justice Harlan, concurring, pointed out that it is usually difficult to apply the Fourth Amendment without reference to the place in which the government surveillance occurred.[16] He read the Court's prior decisions as creating the rule that to enjoy Fourth Amendment intrusion from government surveillance, "there is a twofold requirement, first, that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[17] Although the *Katz* majority rejected the concept that Fourth Amendment protection and "privacy" were equivalent concepts,[18] the Supreme Court has since adopted the second part of Justice Harlan's formulation, and has held on several occasions that the Fourth Amendment protects only reasonable (or legitimate) expectations of privacy,[19] although in 2001, the Court acknowledged that the reasonable expectation of privacy test "has been criticized as circular, and hence subjective and unpredictable."[20]

2. Situations in which a Person Surrenders his Reasonable Expectation of Privacy

Over the years, the Supreme Court has recognized a variety of situations in which a person loses what otherwise would be a reasonable expectation of privacy. The Court articulated one such situation in *Katz*: "What a person knowingly exposes to the public,

---

[16] *Id.* at 361 (Harlan, J., concurring).

[17] *Id.* (Harlan, J., concurring) (internal quotation marks omitted).

[18] *Id.* at 350; *see supra* text accompanying note 13.

[19] *See, e.g.*, California v. Greenwood, 486 U.S. 35, 41 (1988) (holding defendant had no reasonable expectation of privacy in garbage set out on the curb for collection); Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that it did not intrude into Smith's reasonable expectation of privacy when the phone company made a record of the numbers he dialed from his home phone and turned the information over to the police).

[20] Kyllo v. United States, 533 U.S. 27, 34 (2001). The Court, per Justice Scalia, held that a person has a reasonable expectation of privacy against government use of surveillance equipment to learn any information about the inside of his home, at least if the equipment was not readily available to the general public, and therefore the use of a thermal imaging device to measure the amount of heat emanating from Kyllo's home was a search which, in the absence of a search warrant, violated that expectation. *Id.*

even in his own home or office, is not a subject of Fourth Amendment protection."[21]

Second, if a person consents to a search, the search is lawful.[22] The validity of consent is based on an assessment of all of the relevant circumstances.[23] In reality the term "consent" is a misnomer. The Supreme Court has held that a person's "consent" to a search is valid even though the officer did not inform the person of his right to refuse.[24] In essence, the officer may exploit the suspect's ignorance and the inherently coercive nature of the police-civilian encounter.[25] It suffices that—considering a totality of the circumstances[26]—the officer obtained the person's acquiescence to the search without engaging in overtly coercive conduct.[27] The consent-to-search concept also applies in the sometimes coercive employer-employee context as well.[28]

Third, whenever a person confides in someone else, he assumes the risk that individual is now working with or may later disclose the confidence to the authorities.[29]

---

[21] Katz v. United States, 389 U.S. 347, 351 (1967).

[22] Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973); *see also* United States v. Drayton, 536 U.S. 194, 207 (2002) ("In a society based on law, the concept of agreement and consent should be given a weight and dignity of its own. Police officers act in full accord with the law when they ask citizens for consent. It reinforces the rule of law for the citizen to advise the police of his or her wishes and for the police to act in reliance on that understanding. When this exchange takes place, it dispels inferences of coercion.").

[23] *Schneckloth*, 412 U.S. at 227.

[24] *Id.*; *Drayton*, 536 U.S. at 203.

[25] The Court has never explicitly stated, but this is the clear implication of cases such as *Florida v. Bostic*, 501 U.S. 429, 438 (1991). In *Bostic*, the defendant quite plausibly argued that no one in his right mind would consent to a search, knowing the police would find contraband, and the defendant's acquiescence to the search therefore must have been coerced. *Id.* at 435. The Court rejected this argument, holding that whether the police acted coercively was to be viewed from the perspective of a reasonable, innocent person in the defendant's situation. *Id.* at 437-38.

[26] *Drayton*, 536 U.S. at 207.

[27] *See Drayton*, 536 U.S. at 207; *Schneckloth*, 412 U.S. at 219.

[28] *See infra* Part III.A.

[29] *See* Hoffa v. United States, 385 U.S. 293 (1966); Lopez v. United States, 373 U.S. 427 (1963). In *United States v. White*, 401 U.S. 745 (1971), the Court held that an undercover agent did not violate White's Fourth Amendment rights when he surreptitiously transmitted to other agents his conversations with White in a variety of locations, including White's home.

B. Statutory Regulation of Surveillance of Communications

1. Title III

Congress responded to *Katz* and another Supreme Court decision, *Berger v. New York*,[30] by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[31] Designed to protect the privacy of wire and oral communications,[32] Title III made it a crime for private persons to intercept such communications, and forbade law enforcement officials to do so without a court order,[33] usually referred to as an "interception order." The legislation mandates that to obtain such an order, the prosecutor must submit an application to a judge that satisfies not only the Fourth Amendment requirements for a search warrant, but several additional conditions as well.[34] For example, an interception order may not be submitted to a federal judge unless it is first approved by a high-level official of the U.S. Department of Justice;[35] applications by state officials to a state judge must first be approved by the state attorney general, the county's chief prosecutor, or specific assistants designated by them.[36] An interception order may be sought and issued only where probable cause exists[37] for particularly serious, statutorily designated crimes.[38] The application must establish that other investigative procedures have been tried and failed, would be unlikely to

---

[30] 388 U.S. 41 (1967). The Court held New York's wiretapping statute unconstitutional because it was overly broad, lacked particularization with regard to what conversations could be listened to, authorized the indiscriminate use of electronic devices, and allowed for extension of the eavesdropping based solely on a showing that an extension was in the public interest. *Id.*

[31] 82 Stat. 197 (1968) (codified at 18 U.S.C. §§ 2510-2522 (2006)).

[32] Electronic communications were added to the statute as part of the Electronic Communications Privacy Act of 1986.

[33] 18 U.S.C. § 2511(1) (2006).

[34] *See generally* 18 U.S.C. § 2518 (2006). For an exhaustive discussion of this provision, see FISHMAN & MCKENNA, *supra* note 10, chs. 8-11.

[35] 18 U.S.C. § 2516(1) (2006) (wire and oral communications); *see* FISHMAN & MCKENNA, *supra* note 10, § 8:5. 18 U.S.C. § 2516(3) (2006) (electronic communications); *see* FISHMAN & MCKENNA, *supra* note 10, § 8:6.

[36] 18 U.S.C. § 2516(2) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:7-8:11.

[37] 18 U.S.C. §§ 2518(1)(b), 2518(3)(a), (b), (d) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:53-8:70.

[38] 18 U.S.C. § 2516(1) (2006) (federal orders); 18 U.S.C. § 2516(2) (state orders); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:35-8:40.

succeed, or would be too dangerous.[39] The orders must be executed to "minimize the interception" of communications unrelated to the crimes being investigated.[40]

Where a participant to the communication consents to its interception, however, the interception is lawful and no court order is needed.[41]

2. The ECPA and SCA

In 1986, Congress enacted the Electronic Communications Privacy Act (ECPA).[42] As its title implies, a primary purpose of ECPA was to protect the privacy of electronic communications from unauthorized acquisition by either private individuals or government agents.[43]

A major component of ECPA are provisions, codified at 18 U.S.C. §§ 2701-11, which regulate the disclosure of stored electronic communications such as e-mails and text messages. These provisions are often referred to as the "Stored Communications Act" (SCA).[44] The SCA makes it a crime to access stored wire or electronic communications without legal authorization.[45] Penalties for violating the statute range from six

---

[39] 18 U.S.C. § 2518(1)(c) (2006) (application); 18 U.S.C. § 2518(3)(c) (order); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:71-8:92.

[40] 18 U.S.C. § 2518(5) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 8:101-8:107.

[41] 18 U.S.C. § 2511(2)(c) (2006) (interceptions with the consent of a participant are lawful if made "under color of law"); 18 U.S.C. § 2511(2)(d) (interceptions by private individuals with the consent of a participant are lawful so long as the interception was not done for the purpose of committing a crime or a tort); *see* FISHMAN & MCKENNA, *supra* note 10, ch. 5.

[42] 18 U.S.C. §§ 1367, 2521, 2701-11, 3117, 3121-37 (2006).

[43] Among other things, ECPA amended Title III, *see supra* Part I.B, to make it a crime, and civilly actionable, for a private person or entity to intercept electronic communications as they are being transmitted. 18 U.S.C. § 2511(1) (2006).

[44] An astute reader (or one with nothing better to do) may have noticed that although the SCA and ECPA are both statutes, I refer to them as "the SCA" (with a "the") and "ECPA" (without a "the"). I do so because when "ECPA" is referred to aloud, it is usually pronounced as if it was a word—"Eck-pa"—without the "the," while the SCA is pronounced "the S-C-A."

[45] 18 U.S.C. § 2701(a) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:10-7:12. Where an employer is the service provider of an e-mail system for its employees, however, the employer may access stored or archived e-mail messages without the knowledge or permission of employees. This is so because 18 U.S.C. § 2701(1)(c) permits the service provider to do pretty much what it wants with regard to stored

months' to two years' imprisonment and fines ranging from $5000 to $250,000.[46] It is also unlawful for an individual or entity involved in the transmission or storage of the communication to improperly divulge the contents of such a communication.[47] Unauthorized access to or divulgence of stored communications is also civilly actionable.[48]

The scope of the SCA was an important issue at the *Quon* trial and on appeal to the Ninth Circuit.[49] Although the Supreme Court declined to grant certiorari on the statutory issues,[50] the Court did discuss the relevance of the statute to the issues on which it did grant cert.[51]

3. Other Legislation

Congress has enacted other statutes protecting communicational privacy and regulating government access to private communications,[52] but these statutes do not play a role in the *Quon* case, and this Article will offer no discussion of them.[53]

---

communications. *See* FISHMAN & MCKENNA, *supra* note 10, § 7:21. However, this situation did not apply in *Quon*, because the communications service was provided by a corporate ISP, Arch Wireless Operating Company.

[46] 18 U.S.C. § 2701(b) (2006); *see* FISHMAN & MCKENNA, *supra* note 10, § 7:13.

[47] 18 U.S.C. § 2702 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:33-7:34.

[48] 18 U.S.C. § 2707 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, § 7:30. The statute likewise spells out the circumstances in which the government may obtain access to such communications as part of a criminal investigation. 18 U.S.C. § 2703 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:45-7:55. Depending on the circumstances, the government may proceed either by search warrant, by subpoena, or by court order; the customer whose electronic "storage bin" is being pierced may receive prior notice that the government seeks access to stored records, thereby enabling the customer to move to quash the action; or he may receive notice only after the government has already obtained the records; or he may not receive notice at all. 18 U.S.C. § 2705 (2006); *see* FISHMAN & MCKENNA, *supra* note 10, §§ 7:57-7:58. These latter portions of the statute are not relevant to the *Quon* case, because the Ontario Police Department, Quon's employer, was not conducting a criminal investigation against Quon.

[49] *See infra* note 158.

[50] *See infra* Part III.D.

[51] *See infra* Part III.E.4.

[52] Government use of pen registers and trap-and-trace devices to record the numbers dialed by a particular phone, and the source of calls to that phone, is regulated by 18 U.S.C. § 2703(c), (d) and (e) and 18 U.S.C. § 3121-27; *see generally* FISHMAN & MCKENNA, *supra* note 10, ch. 4. Federal statutes protecting computer privacy include the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006). For detailed coverage of that and other computer-related legislation, see generally

C. Measuring the Validity of a Search

If a court concludes that government agents have conducted a Fourth Amendment search, the question then becomes whether the search was lawful. The Fourth Amendment does not prohibit all searches and seizures, it protects against only those which are unreasonable.[54] Other than the general requirement that to be lawful a search must not be "unreasonable," the only explicit guidance the amendment provides is that "no Warrants shall issue, but upon probable cause, particularly describing the place to be searched, and the persons or things to be seized."[55] The amendment does not define probable cause; nor does it explicitly state whether a search may be reasonable in the absence of probable cause; nor does it specify when a warrant is required.

1. The Warrant Requirement and Probable Cause

As to the latter issue, the operative cliché is that "as a general matter, warrantless searches are *per se* unreasonable under the Fourth Amendment," subject to "a few specifically established and well-delineated exceptions" to that general rule.[56] The Court has said so in almost exactly the same words twenty-four times[57]—once for each blackbird baked in the nursery rhyme pie.[58] But "saying it's so doesn't make it so."[59] In fact, the

---

FISHMAN & MCKENNA, *supra* note 10, ch. 25. The Foreign Intelligence Surveillance Act (FISA), codified at 50 U.S.C. §§ 1801-12, regulates (among other things) the use of electronic surveillance of communications for national security purposes. *See generally* FISHMAN & MCKENNA, *supra* note 10, ch. 12 (Incidentally, this statute is generally pronounced "FIE-SUH" and is not preceded by a "the."). States have also passed legislation regulating the interception of communications and related subjects. For extensive coverage of these statutes, see generally *id.* §§ 1-11, 13-41.

[53] The footnotes in Parts I.B and I.C may set a new world's record for frequency of professorial self-citation per word of text; if not, I'll bet they come close.

[54] U.S. CONST. amend. IV.

[55] *Id.*

[56] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (citations omitted) (internal quotation marks omitted).

[57] Anyone interested in the complete list need only do a Westlaw search, data base U.S. Supreme Court, for the phrase "per se unreasonable under the Fourth Amendment." A search including minor variations on this phrase would no doubt produce additional cases.

[58] The first two lines of the rhyme read, "Sing a song of six pence, a pocket full of rye. Four-and-twenty blackbirds baked in a pie." For the full text of the rhyme, its history (apparently at one time, enclosing live birds inside a pie was a popular custom),

exceptions to the warrant requirement are many rather than few,[60] and some are not at all well-delineated,[61] as even a superficial perusal of the leading treatises on the Fourth Amendment will quickly reveal.[62] The vast majority of searches conducted by government agents are lawful despite the absence of a warrant;[63] a substantial number of these are lawful despite the

---

theories concerning its deeper meaning, and cultural references to it in literature and popular culture (my reference to it in this Article enrolls me in a roster of luminaries including, among others, William Shakespeare and Paul McCartney), see *Sing a Song of Sixpence*, *in* THE OXFORD DICTIONARY OF NURSERY RHYMES 394-95 (Iona Opie & Peter Opie eds., Oxford Univ. Press 2d. ed. 1997) (1951); WILLIAM SHAKESPEARE, TWELFTH NIGHT act 2, sc. 3; THE BEATLES, *Blackbird*, *on* THE BEATLES (Apple Records 1968).

[59] I tried to find the original source for this phrase. My edition of BARTLETT'S FAMILIAR QUOTATIONS did not list it in the index. A Google search produced 14,600 hits. I examined the first several; none cited the original source. I would have dutifully continued down the list, but my wife insisted that I help put away the Passover dishes.

[60] Examples: search of the person incident to arrest; search of the area incident to arrest; stop-and-frisks; searches conducted during hot pursuit of a fleeing suspect; searches conducted to prevent the impending destruction of evidence; searches of vehicles; searches of containers in vehicles; consent searches; and an impressive variety of inspection, regulatory, and other "special needs" searches. *See* discussion *infra* Part I.C.2.

[61] Consider, for example, the search-of-the-area incident to arrest doctrine first announced in *Chimel v. California*, 395 U.S. 752 (1969), in which the Court held that at least in some circumstances, after the police have arrested someone within a premises, they may search the immediate area for weapons or destructible evidence. Lower courts have debated ever since whether the right to conduct such a search continues after the arrestee has been secured and moved to a different location. The Supreme Court returned to that issue in *Arizona v. Gant*, 129 S. Ct. 1710 (2009), a case involving the search of an automobile, in which the plurality and dissenting opinions each cited *Chimel* more than twenty times, without clarifying the issue much, if at all.

[62] *See, e.g.*, THOMAS CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION ch. 6 (2008) (discussing arrests and seizures of persons, only a small fraction of which require a warrant); *id.* ch. 8 (discussing searches incident to arrest, virtually none of which require a warrant); *id.* ch. 9 (discussing protective weapons searches and sweeps, none of which require a warrant); *id.* ch. 10 (discussing automobile and consent searches, few if any of which require a warrant); WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT chs. 6-10 (4th ed. 2004) (discussing these same topics).

[63] I do not intend to cite any particular source to defend this statement; anyone who practices criminal law or teaches Criminal Procedure—I've done one or the other for more than forty years—knows it is true (Consider, by analogy, FED. R. EVID. 201(b), which permits a court to take judicial notice of an adjudicative fact that is "generally known within the court's geographic jurisdiction."). Law review editors and judges and attorneys who practice or adjudicate in other areas of law, please keep in mind that the assertion to which this footnote is attached is merely background information in the

lack of probable cause.[64] Probably a more accurate statement would be that as a general rule, warrants based on probable cause *are* required to authorize the police to make a non-consensual entry into a home, office or other private premises; to search someone's mail; to open some packages; and to intercept oral, wire or electronic communications without the consent of a participant.[65]

2. Administrative, Regulatory, and Other "Special Needs" Searches

The government is often called upon to conduct searches in contexts unrelated (or at least not directly related) to criminal law enforcement. These are sometimes referred to as "special needs" searches.[66] The Court has long recognized that the reasonableness of such searches and seizures, conducted outside the traditional criminal law enforcement context, must be measured by standards different from those that apply in criminal cases.[67] The Court has upheld the applicability of this doctrine to inspections of homes[68] and business locations;[69] and to border searches[70] of mail,[71]

---

introductory section of the Article. I respectfully request you simply take my word for its accuracy.

[64] *See supra* note 63.

[65] *See supra* note 63.

[66] *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619, 2628, 2630 (2010) (using the phrase and citing other cases in which it appears).

[67] Each of the cases cited in the next ten footnotes so holds.

[68] *See, e.g.*, Camara v. Mun. Court, 387 U.S. 523 (1967) (holding that a warrant is required before police may search a home pursuant to fire, health, and housing code inspection programs, but that such warrants need not be based on probable cause of criminal wrongdoing or code violations; rather, they may be issued pursuant to reasonable administrative or legislative standards).

[69] *See, e.g.*, New York v. Burger, 482 U.S. 691 (1987) (holding that where a business is closely regulated by the state, searches by the police without a warrant are permissible if carefully limited in time, place, and scope); Marshall v. Barlow's, Inc., 436 U.S. 307 (1978) (holding that a warrant could be issued to search a business location if issued on the basis of a general administrative plan based on neutral principles).

[70] United States v. Ramsey, 431 U.S. 606, 616 (1977) ("That searches made at the border, pursuant to the long-standing right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border, should, by now, require no extended demonstration.").

automobiles,[72] and individuals;[73] to sobriety checkpoints;[74] and regulations requiring drug tests of school children,[75] law enforcement officials,[76] and mass transit employees.[77] The Court has rejected the application of "special needs" standards with regard to drug interdiction roadblocks,[78] and to regulations

---

[71] *Id.* at 623-24. In *Ramsey*, the Court upheld a statute authorizing customs officials to search first class mail coming from overseas whenever reason existed to suspect it might contain contraband.

[72] United States v. Flores-Montano, 541 U.S. 149 (2004) (upholding border agents' removal, disassembly, and search of a vehicle's gas tank despite the lack of probable cause or reasonable suspicion that it contained contraband).

[73] *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985); Carroll v. United States, 267 U.S. 132, 154 (1925). 19 U.S.C. § 1582 (2006) directs that "all persons coming into the United States from foreign countries shall be liable to detention and search by authorized officers or agents of the Government under such regulations [promulgated by the Secretary of the Treasury]." In *Montoya de Hernandez*, the Court held that where customs agents "reasonably suspect" that a traveler has swallowed contraband in an attempt to smuggle it into the country in her digestive system, the traveler may be detained until the suspicion is verified or dispelled, i.e., until she submits to an X-ray or, if she refuses, until she has a bowel movement. *Montoya de Hernandez*, 473 U.S. at 541.

[74] Mich. Dep't. of State Police v. Sitz, 496 U.S. 444 (1990) (holding that, given the magnitude of the drunk driving problem, sobriety checkpoints that subjected all motorists to a very brief detention was constitutional).

[75] Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646 (1995) (upholding a school regulation requiring all students seeking to participate in interscholastic athletics to submit to random drug testing); *see also* Bd. of Educ. v. Earls, 536 U.S. 822 (2002) (upholding a similar regulation regarding all students seeking to participate in any extracurricular activities). In each case the Court held that the school district had documented a serious problem with drug use among children, and that the testing regime was reasonably calculated to help address the problem. In *Safford Unified Sch. Dist. No. 1 v. Redding*, 129 S. Ct. 2633 (2009), however, the Court held that, even though "the [public] school setting 'requires some modification of the level of suspicion of illicit activity needed to justify a search,'" it was unreasonable for an assistant principal who suspected that a thirteen-year-old middle school student possessed over-the-counter pain relief pills to compel the child to submit to a virtual strip search. *Id.* at 2639, 2641-43 (internal citations omitted).

[76] Treasury Emp. Union v. Von Raab, 489 U.S. 656 (1989). See *infra* notes 121-22 and accompanying text for further discussion of *Von Raab*.

[77] Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 611 (1989) (holding that it was reasonable "to require [certain categories of railroad employees] to submit to breath or urine tests" if they were working on a train that was involved in certain kinds of collisions or other incidents).

[78] City of Indianapolis v. Edmond, 531 U.S. 32, 37-38, 40-42 (2000) (The Court held that because such traffic stops (which are Fourth Amendment "seizures") were essentially conducted to enforce criminal laws against drug possession and trafficking, they did not qualify as "special needs" searches and were unlawful absent an individualized suspicion of wrongdoing as to any vehicle that was stopped.).

requiring drug testing for political candidates[79] and for pregnant women seeking free medical treatment at a public hospital.[80]

In 1985, in *New Jersey v. T.L.O.*,[81] a case involving the search of a fourteen-year-old high school freshman,[82] the Court ruled that once it had been determined that a "search" occurred (i.e., that a government agency intruded into a litigant's Fourth Amendment-protected "reasonable expectation of privacy"), the lawfulness of these searches should be assessed by a two-part analysis: "[F]irst, one must consider 'whether the . . . action was justified at its inception,' second, one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place.'"[83]

More recently, the Court has applied somewhat differently worded tests in assessing searches in "special needs" situations, even in the absence of individualized suspicion of wrongdoing,[84]

---

[79] Chandler v. Miller, 520 U.S. 305, 319 (1997) (holding unconstitutional a state requirement that all political candidates submit to drug testing because, among other things, the requirement was "not well designed to identify candidates who violate antidrug laws").

[80] In *Ferguson v. Charleston*, 532 U.S. 67 (2001), the Court held that this procedure, done as part of program in which a pregnant woman who tested positive would be threatened with prosecution unless she agreed to submit to treatment, violated the privacy of the women involved because criminal law enforcement was too central an aspect of the program.

[81] New Jersey v. T.L.O., 469 U.S. 325 (1985).

[82] T.L.O. was caught smoking in a bathroom. The assistant principal looked in her purse and saw a pack of cigarettes. When he removed it, he saw cigarette rolling paper, which he associated with marijuana use. At this point, he searched the purse thoroughly and found evidence that the child was selling marijuana to other students at the school. *Id.* at 328.

[83] *Id.* at 341. The Court took this test from, and quoted, *Terry v. Ohio*, 392 U.S. 1 (1968), in which the Court held that a police officer may stop to question someone whom the officer reasonably suspects is committing or is about to commit a crime, and that if the officer reasonably suspects that person is armed, the officer may "frisk" the person (i.e., may run his hands along the outer layer of the person's clothing to see if he is in fact carrying a weapon). *Id.* at 20. In *T.L.O.*, the Court, applying this two-part test, upheld the assistant principal's actions, ruling that each step was justified by what he had discovered by the previous step. *T.L.O.*, 469 U.S. at 347-48.

[84] "In limited circumstances, where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion, a search may be reasonable despite the absence of such suspicion." Skinner v Ry. Labor Execs. Ass'n, 489 U.S. 656, 624 (1989) (quoted approvingly in Chandler v. Miller, 520 U.S. 305, 314 (1997)).

and has offered yet another two-part formula for assessing searches generally.[85]

In *Quon*, the Court addressed, but did not decide, whether the *T.L.O.* formula is appropriate when a government agency searches an employee's workspace or his on-the-job communications solely for internal administrative purposes, unconnected with larger government policies or responsibilities. *Quon*, however, was not the first case in which the Court pondered that issue; it had done so twenty-three years earlier, in *O'Connor v. Ortega.*[86] Because an understanding of *O'Connor* is necessary to understand *Quon*, it is to the *O'Connor* case that this Article now turns.

II. *O'CONNOR V. ORTEGA*

A. Facts and Issues

Dr. Magno Ortega had served as Napa State Hospital's Chief of Professional Education for seventeen years.[87] In 1981, Dr. Dennis O'Connor, the hospital's Executive Director, received allegations that Dr. Ortega had engaged in various kinds of wrongdoing.[88] Dr. O'Connor ordered an investigation, during which Dr. Ortega was barred from hospital grounds while hospital

---

[85] Wyoming v. Houghton, 526 U.S. 295, 300 (1999) (stating that the reasonableness of a search is determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests"). In *Houghton*, the Court upheld a search of all containers in the passenger compartment of an automobile where probable cause existed that at least one occupant possessed a controlled substance. Court quoted and applied the *Houghton* formula in *United States. v. Knights*, 534 U.S. 112, 118-19 (2001), wherein the Court held that a state may legitimately impose, as a condition of probation, that a police officer may search the probationer or his home whenever the officer has a reasonable suspicion that the suspect is engaged in wrongdoing, and in *Samson v. California*, 547 U.S. 843, 848 (2006), where the Court held that a state may legitimately require, as a condition of parole, that a parolee consent to a search whenever asked to do so by a parole officer or law enforcement officer even in the absence of reason to suspect the parolee of any wrongdoing.

[86] O'Connor v. Ortega, 480 U.S. 709 (1987).

[87] *Id.* at 712. Dr. Ortega's primary responsibility was training young physicians in psychiatric residency programs. *Id.*

[88] *Id.* Dr. Ortega was accused of coercing contributions from residents in order to purchase a computer for his office, of sexually harassing two female hospital employees, and of taking inappropriate disciplinary action against a resident. *Id.*

officials searched Dr. Ortega's office.[89] The underlying reason for the search was a hotly disputed issue at trial, but in any event, the search was quite thorough: hospital personnel went through his desk drawers and filing cabinets and seized a wide range of objects, including a substantial number of clearly personal items.[90] Dr. Ortega sued the hospital per 42 U.S.C. § 1983,[91] alleging that the search of his office was motivated by a desire to find evidence to support the allegations against him, and therefore violated his Fourth Amendment right against unreasonable searches and seizures.[92] The hospital asserted that the search was conducted to secure state property in the office, and was therefore reasonable.[93] The district court, accepting this defense, granted summary judgment for the hospital.[94] The Ninth Circuit reversed,[95] holding that as a matter of law (1) Dr. Ortega had a reasonable expectation of privacy in his office, desk, and file drawers,[96] and (2) that the search violated that expectation.[97] The Ninth Circuit concluded that the only issue for the trial court to resolve was the amount of damages to which Dr. Ortega was entitled.[98]

---

[89] *Id.* at 712-13.

[90] *Id.* at 714. These included billing documents of a private patient of Dr. Ortega's. *Id.*

[91] 42 U.S.C. § 1983 (2006) ("Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress . . . .").

[92] *O'Connor*, 480 U.S. at 714.

[93] *Id.* As it turned out, the investigators seized certain items during their searches, but "did not otherwise separate Dr. Ortega's property from state property because, as one investigator testified, '[t]rying to sort State from non-State, it was too much to do, so I gave it up . . . .'" *Id.* at 713-14. No formal inventory was ever made of the contents of the office; "[i]nstead, all the papers in Dr. Ortega's office were merely placed in boxes, and put in storage for Dr. Ortega to retrieve." *Id.* at 714.

[94] Ortega v. O'Connor, No. C-82-4045-JPV, 1993 WL 87804 (N.D. Cal. Mar. 23, 1993) (unreported case).

[95] Ortega v. O'Connor, 764 F.2d 703, 706-07 (9th Cir. 1985), *rev'd sub nom.* O'Connor v. Ortega, 480 U.S. 709 (1987).

[96] *Id.* Concerning the centrality of the "reasonable expectation of privacy" concept to current Fourth Amendment jurisprudence, see *supra* Part I.A.1.

[97] *Ortega*, 764 F.2d at 706-07.

[98] *Id.* at 707.

The hospital appealed and the Supreme Court granted certiorari.[99] Issues before the Supreme Court included: (1) Did Dr. Ortega have a reasonable expectation of privacy in his desk, file drawers, and office? (2) If so, against what standard should that expectation, and the hospital's justification for the search and seizure, be measured? (3) Was the Ninth Circuit correct in ruling that, as a matter of law, Dr. Ortega's right to privacy existed, and that the hospital's actions violated those rights?

In a 5-4 decision, the Supreme Court held that Dr. Ortega indeed did have a Fourth Amendment-protected right to privacy in his desk, file drawers, and office, but concluded that the record below had not been adequately developed to determine whether the hospital's search of his office was reasonable.[100] The Court therefore reversed the Ninth Circuit decision, and remanded.[101] This brief summary of the result, however, is a significant over-simplification. The case produced three separate opinions: Justice O'Connor's plurality opinion (joined by Chief Justice Rehnquist and Justices White and Powell); Justice Scalia's (mostly) concurring opinion;[102] and Justice Blackmun's dissenting opinion[103] (joined by Justices Brennan, Marshall and Stevens).

---

[99] O'Connor v. Ortega, 474 U.S. 1018 (1985) (granting certiorari).

[100] *O'Connor*, 480 U.S. at 727-29.

[101] *Id.* The case has a convoluted history thereafter. After a trial, the judge directed a verdict for the defendants; the Ninth Circuit reversed, ruling the trial judge had improperly precluded Dr. Ortega from calling several witnesses. Ortega v. O'Connor, 50 F.3d 778, 780 (9th Cir. 1995). On retrial, a jury found for Dr. Ortega and awarded him $400,000 in damages; the Ninth Circuit affirmed. Ortega v. O'Connor, 146 F.3d 1149 (9th Cir. 1998). The verdict seems well-justified. During the search, hospital personnel closely scrutinized obviously personal items; the hospital did not permit Dr. Ortega to reclaim his personal property for several months; and it even used some highly private items scrutinized during the search to impeach witnesses who testified on Dr. Ortega's behalf at the post-remand trial. *Id.* at 1152.

[102] Justice Scalia was in the unusual (for him) position of being the swing justice. Of the four issues before the Court, he agreed with Justice O'Connor's plurality on two issues, the Blackmun dissent on one issue, and with neither on yet another issue. *O'Connor*, 480 U.S. at 729 (1987) (Scalia, J., concurring).

[103] *Id.* at 732 (Blackmun, J., dissenting).

B. Reasonable Expectation of Privacy

All nine Justices agreed that Dr. Ortega had a reasonable expectation of privacy in his desk and file drawers.[104] The Court divided, however, as to whether such an expectation existed in his *entire* office. The plurality Justices, after an extensive discussion of the need to consider "[t]he operational realities of the workplace"[105] in order to determine whether an employee's Fourth Amendment rights are implicated by a search of the office as a whole, declined to decide the issue.[106] The four (otherwise) dissenting Justices and Justice Scalia, however, concluded that as a general rule, a government employee *does* have a reasonable expectation of privacy in his or her office. As Justice Scalia put it: "one's personal office is constitutionally protected"[107] except in "unusual situations" in which the office is subject to "unrestricted public access."[108] Thus, a clear 5-4 majority exists as to the office.[109]

---

[104] *Id.* at 718 (plurality opinion); *id.* at 729 (Scalia, J., concurring); *id.* at 732 (Blackmun, J., joined by Brennan, Marshall, Stevens, J.J., concurring with the other five Justices on this issue, although dissenting on pretty much everything else).

[105] *Id.* at 717 (plurality opinion).

[106] *See id.* at 714-18. The plurality declined to decide it, reasoning that the office question was superfluous because the search of his desk and file cabinet clearly had intruded upon Dr. Ortega's reasonable privacy expectations; thus, regardless of how the Court ruled regarding the office, it was necessary for the Court to consider the appropriate standard against which those searches should be measured. *Id.* at 718-19.

[107] *Id.* at 730 (Scalia, J., concurring).

[108] *Id.* at 731.

[109] *Id.* at 732. Despite the unusual source of the five votes on this issue (one concurring Justice and four otherwise dissenting Justices), their conclusion, that Dr. Ortega had a Fourth Amendment-protected expectation of privacy in his office, probably can be considered a "holding" of the Court. In *Marks v. United States*, 430 U.S. 188 (1977), the Court commented: "When a fragmented Court decides a case and no single rationale explaining the result enjoys the assent of five Justices, the holding of the Court may be viewed as that position taken by those Members who concurred in the judgments on the narrowest grounds." *Id.* at 193. (citation omitted) (internal quotation marks omitted). Although the Court certainly "fragmented" in *O'Connor*, the four dissenting and one concurring justices did agree on the rationale for recognizing Dr. Ortega's privacy expectations in his office. *See supra* note 104 and accompanying text.

C. Appropriate Standard to Determine "Reasonableness"

Given the Court's conclusion that Dr. Ortega had a reasonable expectation of privacy in his desk, file drawers, and office, it necessarily follows that when hospital officials examined and boxed up the items they found there, they had conducted a Fourth Amendment "search" of those areas and a Fourth Amendment "seizure" of those items.[110] The Court next addressed the question: What standard should be used to measure the reasonableness of a government employer's search of an employee's private work space? Should a court apply the same standard as the one that police must satisfy when they are seeking evidence of criminal activity, which would generally require a warrant based on probable cause; or a different standard and, if so, what should that standard be?[111]

1. Justice O'Connor's Plurality Opinion

The plurality concluded that the warrant and probable cause requirements should not apply to a search prompted by "special needs," such as a search, like this one, that was based solely on administrative concerns and not possible criminal violations.[112] Justice Scalia agreed.[113] Thus, a 5-4 majority rejected imposing the probable cause and search warrant requirements to "non-criminal" searches by government officials of a government employee's private workspace.[114] Moreover, the plurality and

---

[110] *See supra* Part I.A.1.

[111] The dissent argued that the Court should not have addressed the question at all. *See infra* Part II.C.3.

[112] *O'Connor*, 480 U.S. at 721 (plurality opinion).

[113] *Id.* at 731-32 (Scalia, J., concurring).

[114] Since *O'Connor*, there has been little discussion in opinions of the Court concerning an application of the warrant requirement in non-criminal law contexts. In *Skinner v. Railway Labor Executives Association*, 489 U.S. 602, 611 (1989), the Court held that it was reasonable "to require [specified categories of railroad] employees to submit to breath or urine tests" if a train on which they were working was involved in certain types of accidents or incidents. *Id.* at 611. A six-three majority held that based on the exigencies involved—if blood and urine samples were not taken promptly, the railroad employee's body would eliminate evidence of alcohol or drug use—neither probable cause nor a search warrant was needed. *Id.* at 634. Only Justice Marshall, joined by Justice Brennan, dissented, arguing that while exigencies excused obtaining a warrant before drawing the samples, a warrant should be required before those samples are tested. *Id.* at 642-43.

Justice Scalia explicitly rejected those requirements, whether the search in question was a simple search for a file in the employee's absence, or a search prompted by suspicions that the employee had engaged in wrongdoing. The plurality expressed it thus:

> An employer may have need for correspondence, or a file or report available only in an employee's office while the employee is away from the office. Or, as is alleged to have been the case here, employers may need to safeguard or identify state property or records in an office in connection with a pending investigation into suspected employee misfeasance.[115]

Justice Scalia used the same examples.[116] Thus, a 5-4 majority of the Court decided against applying the warrant and probable cause requirements to a government employer's "special needs" search of an employee's office.

No majority emerged, however, as to what the appropriate standard should be. Justice O'Connor's plurality opinion applied the two-step process that the Court had articulated two years earlier in *New Jersey v. T.L.O*: "[F]irst, one must consider 'whether the . . . action was justified at its inception,' second, one must determine whether the search as actually conducted 'was reasonably related in scope to the circumstances which justified the interference in the first place.'"[117] Given that this two-part test, or similar tests,[118] have been applied in so many other contexts,[119] it may seem sensible enough to apply it as well to government employer-employee searches. But consider: in each of the other cases applying such a formula, the government entity, whether an agency of the federal, state, city, county, or local government, was acting in its capacity *as the government* in the furtherance of *government* goals.[120] Even in *National Treasury*

---

[115] *O'Connor*, 480 U.S. at 721-22 (plurality opinion).

[116] *See id.* at 732 (Scalia, J., concurring) (rejecting the warrant and probable cause requirements for "searches to retrieve work-related materials or to investigate violations of workplace rules").

[117] *Id.* at 726 (quoting New Jersey v. T.L.O., 469 U.S. 325, 341 (1985)); *see supra* note 75 and accompanying text.

[118] *See supra* notes 84-85 and accompanying text.

[119] *See supra* Part I.C.2.

[120] *See supra* Part I.C.2.

Employees Union v. Von Raab,[121] which involved a regulation requiring certain government employees to submit to urine testing, the underlying purpose was not merely the internal administration of the agency, but the broader goal of assuring the honesty and competence of law enforcement officials so they would effectively carry out their public duties.[122]

In *O'Connor v. Ortega*, however, the hospital was *not* acting as a government agency per se; rather, it was acting *strictly* as an *employer* seeking to determine whether one of its employees had misappropriated hospital property or violated hospital policies.

2. Justice Scalia's Concurrence

Justice Scalia, whose concurrence provided the fifth vote rejecting the probable cause and warrant standards, rejected the plurality's two-part formula, protesting that it was so vague as to be almost meaningless.[123] He proposed an alternative: if a government agency searches an employee's workspace while acting solely as an employer, and not in furtherance of any

---

[121] 489 U.S. 656 (1989).

[122] In light of the U.S. Customs Service's responsibilities in interdicting and seizing illegal drugs smuggled into the country, the service implemented a program requiring service employees to submit to urinalysis tests if they sought transfer or promotion to positions having a direct involvement in drug interdiction or requiring the incumbent to carry firearms. The Supreme Court upheld the program, concluding that it came within the area of "special government needs beyond the normal need for law enforcement," *id.* at 665-66, i.e., "to deter drug use among those eligible for promotion to sensitive positions within the Service and to prevent the promotion of drug users to those positions." *Id.* at 666.

[123] Justice Scalia objects with some frequency that rules promulgated by the Supreme Court are so vague as to give almost unbridled discretion to judges. See, for example, *Kyllo v. United States*, 533 U.S. 27 (2001), in which the Court, per Justice Scalia, noted criticism of the *Katz* "reasonable expectation of privacy" test as "circular . . . subjective and unpredictable." *Id.* at 34. It was on the same basis that Justice Scalia, in *Crawford v. Washington*, 541 U.S. 36, 62-63 (2004), persuaded the Court to abandon its previous approach to the Sixth Amendment Confrontation Clause and replace it with an entirely different approach (as a result, Confrontation Clause issues are now resolved simply, clearly, concisely, and without the contaminant of judicial subjectivity). To paraphrase Artemus Ward, President Lincoln's favorite humorist, the previous parenthetical "is rote sarcastikul." CHARLES FARRAR BROWNE (ARTEMUS WARD), ARTEMUS WARD: HIS BOOK, A VISIT TO BRIGHAM YOUNG (1862); *see* BARTLETT'S FAMILIAR QUOTATIONS 616:11 (Little, Brown & Co. 15th ed. 1980). For an example of the rather unsettled state of Confrontation Clause law after *Crawford*, see *Michigan v. Bryant*, 131 S. Ct. 1143 (2011).

broader governmental function, then the search is lawful so long as the search would be considered reasonable if conducted in a non-governmental workplace. Thus, for example, if the government agency conducts a search "to retrieve work-related materials or to investigate violations of *workplace* rules—searches of the sort that are regarded as reasonable and normal in the private-employer context," then the search is ipso facto reasonable under the Fourth Amendment. [124]

Although Justice Scalia did not elaborate further, he appears to have reasoned that when a government agency is acting strictly as an employer, and not as a government agency per se, a government employee should enjoy no greater (and no lesser) right to privacy than an employee of a non-government entity. Presumably, therefore, when a government agency conducts a non-criminal-law oriented search, a court should not look to, or create, a body of *Fourth Amendment* law, but should apply *tort and employment law* to determine whether an actionable invasion of privacy has occurred.

3. Dissent

The dissenting Justices accepted the Ninth Circuit's factual conclusion that hospital personnel conducted the search looking for evidence of Dr. Ortega's alleged misconduct, and therefore the search was investigative in nature. Based on this conclusion, the dissent insisted that an *investigative* search of this kind, though it did not involve suspicion of *criminal* conduct, could be lawful only if authorized by a search warrant based on probable cause, albeit with some adjustment of probable cause reflecting the noncriminal nature of the investigation and suspected wrongdoing.[125] Given that the Court remanded the case for further fact-finding, Justice Blackmun also criticized the plurality for "announc[ing] a standard concerning the reasonableness of a public employer's search of the workplace,"[126] adding: "This does not seem to me to be the way to undertake Fourth Amendment analysis, especially

---

[124] O'Connor v. Ortega, 480 U.S. 707, 733 (1987) (Scalia, J., concurring) (emphasis added).

[125] *Id.* at 732, 741-47 (Blackmun, J., joined Brennan, Marshall and Stevens, J.J., dissenting).

[126] *Id.* at 733.

in an area[—searches of a government employee's work space—]with which the Court is relatively unfamiliar."[127] He also complained that the plurality's standard was so one-sided that it "makes reasonable almost any workplace search by a public employer."[128]

III. *CITY OF ONTARIO V. QUON*

It was not until the *Quon* decision, twenty-three years after *O'Connor*, that the Court again addressed the issue of government employee privacy.[129] During the interval, lower courts generally considered the *O'Connor* plurality approach to be the applicable law in invasion of privacy suits brought by government employees against their employer.[130] Indeed, in the lower court litigation in *Quon* and in their briefs and arguments before the Supreme Court, both sides in the *Quon* case assumed, federal statutory issues aside, that the *O'Connor* plurality *was* the law.[131]

A. Facts

The facts and lower-court proceedings in *Quon* are fairly complicated. For purposes of this Article, however, the essential facts are these:

1. Jeff Quon was a sergeant in the Ontario Police Department assigned to the SWAT team,[132] presumably a fairly important

---

[127] *Id.*

[128] *Id.* at 734. Despite these concerns, Dr. Ortega ultimately prevailed in his suit. *See supra* note 101.

[129] The Court did address the Fourth Amendment in the Government-as-employer context in *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989), but as noted *supra* note 121-22, that case fell into a "special needs" category of a very different nature than a simple employer-employee relationship.

[130] *See, e.g.*, Ralph V. Seep, Annotation, *Warrantless Search by Government Employer of Employee's Workplace Locker, Desk, or the Like as Violation of Fourth Amendment Privacy Rights—Federal Cases*, 91 A.L.R. FED. 226 (1989 & Supp.).

[131] City of Ontario v. Quon, 130 S. Ct. 2619, 2628 (2010).

[132] *See* BRUCE L. BERG, POLICING IN MODERN SOCIETY 133 (1999) ("Special Weapons and Tactics (SWAT) team[s] . . . [are] squads of specially trained officers [ ] regarded both by citizens and police personnel as elite teams of highly trained and skilled law enforcement agents. . . . Typically, SWAT teams are called to the scenes of ongoing, dangerous situations after more conventional strategies have failed, or when serious and imminent threats to peoples' lives exist . . . . In some jurisdictions, these units simply are called *tactical units*. . . . Members of these tactical teams have received firearms and strategic planning training, as well as training in climbing and

command within the OPD.[133] Each SWAT officer was issued an alphanumeric pager, to enable the officers to communicate with each other if an emergency arose which required their deployment.[134] The city contracted with Arch Wireless Operating Company to provide the wireless services for the pagers.[135] That contract included a set limit of characters per month for each pager.[136]

2. The officers were told officially that they had no reasonable expectation of privacy in any messages they sent or received on the pagers, and that the OPD and the city had the right to monitor or review all messages.[137] This admonition was consistent with the city's previously announced policy, applicable to all city personnel, that the city "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[138] However, OPD Lt. Duke, in charge of the pager system, informally told Sgt. Quon and the others that no one would monitor their messages if they paid for any excess messages (overages) beyond the monthly limit set in the contract between the OPD and Arch Wireless.[139]

3. Sgt. Quon and a few other officers frequently exceeded the limit and paid for the overages.[140] Eventually the OPD Police Chief directed Lt. Duke to obtain two months of text messages sent and received by two officers, including Sgt. Quon.[141] Arch Wireless dutifully provided the transcripts as requested. The parties disagreed as to the reason for the review. Plaintiffs

---

rappelling, handling highjackings and other hostage situations, and riot control tactics.").

133 *Quon*, 130 S. Ct. at 2624.

134 *Id.* at 2625.

135 *Id.*

136 *Id.*

137 *Id.* This was communicated to Sgt. Quon and the others verbally and in writing. *Id.*

138 *Id.*

139 *Id.* at 2615.

140 *Id.* at 2625-26.

141 *Id.* The other officer selected was not a party to the law suit, Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1126 (C.D. Cal. 2006), and the reported decisions in the case do not indicate anything about his messages.

claimed it was to investigate suspicions that Quon was spending too much on-duty time texting on personal matters.[142] Defendants insisted the decision was based on both Lt. Duke's complaints that some of the officers exceeded the limits so regularly that he had essentially become a collection agent for Arch Wireless and on departmental concern that perhaps the monthly character limit included in the contract was too low to cover the officers' on-duty needs.[143]

4. Reviewing Sgt. Quon's messages, Lt. Duke discovered that the overwhelming majority of his messages were not work-related.[144] In fact, Quon was using the pager to exchange sexually explicit messages with his wife Jerilyn, who was also an OPD police officer,[145] and to exchange similar messages with another woman, April Florio, a dispatcher for the OPD with whom he was having an extramarital affair.[146] The matter was referred to the Internal Affairs Bureau of the OPD.[147] An investigator determined that in one month, Quon had sent or received 456 messages during work hours (an average of twenty-eight a day), of which only 10% (an average of three a day) were work-related.[148]

---

[142] *Quon*, 445 F. Supp. 2d at 1144.

[143] *Id.*; *Quon*, 130 S. Ct. at 2626.

[144] *Quon*, 130 S. Ct. at 2626.

[145] *Quon*, 445 F. Supp. 2d at 1122. As the district court described it:

> Many of the text messages sent and/or received by Quon's pager while he was on-duty were, to say the least, sexually explicit in nature. Some of these messages were directed to or from his wife, Jerilyn Quon, while others were directed to or from his mistress, Florio. Other messages, while not sexually explicit were nonetheless private, were sent to and received from his co-worker.

Id. at 1126. This passage gives the distinct impression that Quon exchanged sexually explicit messages with his wife as well as Ms. Florio. However, the Supreme Court's decision in the case refers to "the other respondents, each of whom exchanged text messages with Quon during August and September 2002: Jerilyn Quon, Jeff Quon's then-wife, from whom he was separated . . . ." *Quon*, 130 S. Ct. at 2626. This suggests, albeit not conclusively, that Quon's texts to and from his wife were not sexually explicit.

[146] *Quon*, 445 F. Supp. 2d at 1126. It emerged during a parallel but separate investigation that another OPD dispatcher was tipping off the Hell's Angels motorcycle gang whenever an OPD officer conducted surveillance of a member of the gang, and Ms. Florio was aware of this but did not report it. *Id.* at 1122. Ms. Florio was subsequently fired. *Id.*

[147] *Quon*, 130 S. Ct. at 2626.

[148] *Id.*

5. Sgt. Quon was disciplined for violating OPD rules that forbade pursuing personal matters while on duty.[149]

6. Quon, his wife, and Ms. Florio sued the city, several OPD officials, and Arch Wireless[150] per 42 U.S.C. § 1983,[151] alleging violations of their Fourth Amendment right to privacy, and violations of 18 U.S.C. § 2701, the "Stored Communications Act" (SCA).[152] Sgt. Quon also apparently exchanged numerous non-work-related messages with Sergeant Steve Trujillo, another member of the SWAT team,[153] and Sgt. Trujillo joined as a plaintiff in the suit. The two sergeants and the two women are sometimes referred to collectively as the plaintiffs.[154]

7. The trial judge, attempting to apply the *O'Connor v. Ortega* plurality approach to plaintiffs' Fourth Amendment claim, ruled that the case depended on why the OPD initially decided to review Quon's transcripts—if it was to review the adequacy of the existing contract with Arch Wireless, then the judgment would be for the defendants; if it was to investigate possible wrongdoing by Quon, then judgment would be entered for the plaintiffs.[155] The jury concluded that the Chief of Police ordered the review of officers' text messages to determine whether the character limit on the city's contract with Arch Wireless was sufficient to meet the city's needs. Therefore, the District Court entered judgment for the city and the OPD. The plaintiffs appealed to the Ninth Circuit.

---

149 *Id.*

150 This may have made for some fairly interesting plaintiffs' conferences.

151 *Quon*, 130 S. Ct. at 2626. For the text of 42 U.S.C. § 1983, see *supra* note 91.

152 For a summary of the SCA, see *supra* Part I.B.2.

153 None of the court opinions describe the subject of the messages between the two sergeants, which presumably were not as titillating as Quon's texts to and from his wife and Ms. Florio.

154 Because they were victorious before the Ninth Circuit, the plaintiffs technically were the respondents before the Supreme Court.

155 The trial judge reasoned that Lt. Duke's informal assurance to the SWAT team members, *see supra* Part III.A., created a reasonable expectation of privacy and concluded that if the review of Quon's messages was investigative, rather than administrative, it violated that expectation. Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1144 (C.D. Cal. 2006).

B. The Technology

An explanation of the technology in question is now in order.[156] Most electronic communications involve one or more Internet service providers (ISPs). Well-known ISPs include G-mail, AOL, Yahoo!, etc. In addition, many companies, private entities like universities, and government agencies are also ISPs, because they provide their own Internet access to employees. When I send an e-mail or text message to a friend, for example, it goes from my computer (or pager or smart phone) to my ISP, whose computer system forwards it to my friend's ISP, which forwards it to my friend's computer or other receiving device. Each ISP must temporarily store the communication within its computer system until its part of the transfer is complete. For example, my friend's ISP retains the message at least until my friend opens it. Moreover, most ISPs retain a back-up copy, more or less indefinitely, even after the recipient deletes it from his or her inbox (Developments in communications technology may soon render this process obsolete, but this is how the Arch Wireless system worked in 2002.).[157] Thus, although Sgt. Quon and those with whom he texted had probably deleted their messages from the devices they were using, Arch Wireless retained copies, and therefore could, and did, provide transcripts of Quon's messages when the OPD asked for them.

C. The Ninth Circuit Decision

On appeal, the Ninth Circuit considered three issues. First, the court considered whether Arch Wireless violated the Stored

---

[156] For a detailed description of how the pager system, including the sending and receiving of text messages, worked, see *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 895-96 (9th Cir. 2008), *rev'd sub nom.* City of Ontario v. Quon, 130 S. Ct. 2619, 2633 (2010).

[157] Sgt. Quon was utilizing a two way alphanumeric pager which enabled him to send and receive text messages to other pagers, e-mail, etc. This same technology is used in cellular phones today. For a brief history of text messaging, see Collette Snowden, *Casting a Powerful Spell: The Evolution of SMS*, in THE CELL PHONE READER: ESSAYS IN SOCIAL TRANSFORMATION 107-24 (Anandam Kavoori & Noah Arceneaux eds., 2006).

Communications Act when it provided the OPD with printouts of the text messages. The Ninth Circuit held that it did.[158]

Second, the Court considered whether Quon and the other plaintiffs had a reasonable expectation of privacy with regard to his non-work related text messages. The Ninth Circuit, attempting to apply the *O'Connor v. Ortega* plurality approach, held that he did.[159] Third, having decided that the plaintiffs had a reasonable expectation of privacy, the court considered whether it was nevertheless reasonable for Lt. Duke to review two months' worth of Quon's text messages. The Ninth Circuit, attempting to apply the *O'Connor* plurality approach, reversed the district court, and held that, as a matter of law, the OPD review was unreasonably intrusive and therefore violated plaintiffs' Fourth Amendment rights.[160]

D. The Supreme Court Decision: Overview

The City of Ontario and Arch Wireless appealed three issues to the Supreme Court: (1) the Ninth Circuit's application of the SCA; (2) the circuit court's conclusion that the plaintiffs had a Fourth Amendment reasonable expectation of privacy in Quon's text messages; and (3) the Ninth Circuit's ruling that OPD's review of those messages constituted an unlawful search of them.

---

[158] *Quon*, 529 F.3d at 903. I believe the Ninth Circuit decided the statutory issue incorrectly. I will not go into detail here, except to note that in holding that Arch Wireless violated the SCA, the Ninth Circuit relied on its earlier decision, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004). In *Theofel*, defendant Farey-Jones made an unconscionably broad discovery demand upon Theofel's ISP and then improperly exploited the ISP's naïve attempt to comply with it. Theofel sued for damages. Anyone familiar with the facts would want to hit Farey-Jones and his attorney, and hit them hard. The difficulty is that, though their behavior was indefensible, they had not violated either of the federal statutes on which Theofel based his case: the Stored Communications Act and the Computer Fraud and Abuse Act. Faced with this dilemma, the Ninth Circuit proceeded to completely "rewrite" those two statutes to its own satisfaction so Theofel could sue Farey-Jones (For my analysis of *Theofel*, see FISHMAN & MCKENNA, *supra* note 10, § 7:11. If I had the time, I would write an article about that case, whose title would be: "I do not like thee, Theofel. The reason why is plain to tell: you've warped these statutes all to hell! I do not like thee, Theofel.").

[159] *Quon*, 529 F.3d at 904.

[160] *Id.* at 908-09. The Ninth Circuit denied a petition for rehearing en banc. Quon v. Arch Wireless Operating Co., 554 F.3d 769 (2009). Judge Ikuta, joined by six other Circuit Judges, dissented. *Id.* at 774-79. Judge Wardlaw, who voted to deny re-hearing, wrote an opinion responding to Judge Ikuta's dissent. *Id.* at 769-74.

The Supreme Court denied Arch Wireless's cert application on the statutory issue,[161] but granted certiorari on both Fourth Amendment issues.[162]

As it turned out, however, although the Court granted certiorari on the expectation of privacy issue, ultimately, to the disappointment of some and to the relief of others, it did *not* resolve whether Quon had a reasonable expectation of privacy in those text messages.[163] Instead, the Court decided only one issue: the reasonableness of the OPD's review of Sgt. Quon's text messages. Rejecting both the District Court's and the Ninth Circuit's attempts to apply the *O'Connor* plurality approach, the Supreme Court unanimously held that the review of Quon's text messages was reasonable under the circumstances.[164]

But in *Quon*, as in *O'Connor*, unanimity in the result did not lend clarity to the law. A majority of the Court in *Quon*, per Justice Kennedy, explicitly acknowledged that neither the *O'Connor* plurality nor Justice Scalia's *O'Connor* concurrence was firmly established as the law defining how the Fourth Amendment applied to government workplace searches.[165] Justice Kennedy's majority opinion then proceeded to discuss how the *O'Connor* plurality approach might apply to the reasonableness of the review of Quon's text messages.[166] Justice Scalia wrote a somewhat scornful concurring opinion in which he derided the majority's explanation of why it did not decide the expectation of privacy issue,[167] complained that the majority placed too much emphasis on the *O'Connor* plurality approach in addressing the reasonableness of the OPD's review of the text messages,[168] and insisted that his approach to the government workplace privacy issue was and still is the best approach.[169] Justice Stevens, also concurring in the result, argued that neither the *O'Connor*

---

[161] USA Mobility Wireless, Inc. v. Quon, 130 S. Ct. 1011 (2009).

[162] *Id.*

[163] The Court's discussion of this issue, and its explanation why it did not decide it, is addressed *infra* Part IV.A.1.

[164] City of Ontario v. Quon, 130 S. Ct. 2619, 2632-33 (2010).

[165] *Id.* at 2628.

[166] This discussion occurs in Part III.B of Justice Kennedy's majority opinion. *Id.* at 2630-32; *see also infra* Part III.E.2.

[167] *Quon*, 130 S. Ct. at 2634-35 (Scalia, J., concurring); *see infra* Part III.F.

[168] *Quon*, 130 S. Ct. at 2635.

[169] *Id.*

plurality nor the Scalia *O'Connor* concurrence approaches was a good idea, and urged that the Court should eschew any sweeping generalities and decide each case on its facts.[170]

E. The Majority Opinion

At the outset, Justice Kennedy, for the Court, reviewed the dispute between the *O'Connor* plurality and Justice Scalia's *O'Connor* concurrence as to the appropriate standard applicable in government-as-employer search cases.[171] The majority then made three assumptions (without deciding those issues) for the sake of its opinion.

1. Three Assumptions

The Court first assumed that Quon had a reasonable expectation of privacy in his non-work-related text messages.[172] Second, the Court assumed that the OPD's review of the message transcripts constituted a Fourth Amendment search. This assumption follows logically from the first because a Fourth

---

[170] *Id.* at 2633-34 (Stevens, J., concurring) (citing O'Connor v. Ortega, 480 U.S. 709, 737-41 (1987) (Blackmun, J., dissenting)). Justices Stevens and Scalia are the only two Justices who had been on the Court when *O'Connor* was decided. They had disagreed in that case and resumed the dispute twenty-three years later in *Quon*. Justice Scalia, in a footnote in his concurrence, accused Justice Stevens of implying that the approach advocated by Justice Blackmun in his dissent in *O'Connor* was still a viable option, and then rejected that implication:

> There is room for reasonable debate as to which of the two approaches advocated by Justices whose votes supported the judgment in *O'Connor*—the plurality's and mine—is controlling under *Marks v. United States*. But unless *O'Connor* is overruled, it is assuredly false that a test that would have produced the *opposite* result in that case is still in the running.

Quon, 130 S. Ct. at 2634 n.* (Scalia, J., concurring). Justice Stevens footnoted back, insisting that the Blackmun approach was not precluded by the Court's decision in *O'Connor*. *Id.* (Stevens, J., concurring). Given that the *Quon* majority paid deference to Justice Scalia's *O'Connor* concurrence while making no reference to Justice Blackmun's *O'Connor* dissent, Justice Scalia wins the footnote battle by a technical knockout, and this Article will not refer further to Justice Stevens's opinion in *Quon*.

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

[172] *Id.* at 2630. Initially, Quon presumably did not have any such expectation; he was officially told that the OPD reserved the right to monitor messages sent and received. Thus, he would be entitled to a reasonable expectation of privacy only if Lt. Duke created such an expectation when he informally promised not to read Quon's messages so long as Quon paid for any excess over the contracted amount. *See supra* notes 137-39 and accompanying text.

Amendment search occurs when, and only if, a government entity has intruded into a reasonable expectation of privacy.[173] Third, the court assumed that the same principles applicable to a government employer's search of an employee's *physical office* apply as well in the *electronic* sphere.[174]

2. The OPD Review of the Transcripts was Reasonable; Applying the *O'Connor* Plurality Approach

The majority concluded that, even making all these assumptions, the OPD's decision to review Quon's text messages, and the scope and degree of intrusion involved in that review, were reasonable as a matter of law. In explaining this decision, Justice Kennedy, for the Court, stated that it need not decide whether to apply the *O'Connor* plurality approach to privacy in the government workplace, or the approach advocated in Justice Scalia's *O'Connor* concurrence, because the OPD's search in *Quon* was reasonable under either.[175]

Nevertheless, Justice Kennedy's majority opinion proceeded to apply the *O'Connor* plurality approach—first, one must consider whether the action was "justified at its inception," and second, one must determine whether the search as actually conducted was "reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances" which justified the interference in the first place.[176] The Court held that OPD's review of the messages (assuming that this was a "search" at all) was "justified at its inception" because it had a legitimate departmental purpose—to determine whether the monthly character limit was adequate.[177]

The Court also concluded that the manner and intrusiveness of the search were reasonable. First, an examination of the transcripts of Sgt. Quon's transcripts constituted "an efficient and

---

[173] *See supra* Part I.A.1.

[174] *Quon*, 130 S. Ct. at 2629-30; *see infra* Part IV.A.1.

[175] Quon, 130 S. Ct. at 2628-29.

[176] *Id.* at 2630 (quoting O'Connor v. Ortega, 480 U.S. 709, 725-26 (1987)) (internal quotation marks omitted). The Court's application of *O'Connor* to the OPD review of Quon's messages occurs in Part III.B of the Court's opinion.

[177] *Id.* at 2619, 2631 (citations omitted) (citing *O'Connor*, 480 U.S. at 726).

expedient way to determine whether Quon's overages were the result of work-related messaging or personal use."[178]

Second, the Court considered the nature and extent of Quon's expectation of privacy in his text messages (assuming he had one at all). The Ninth Circuit apparently concluded that Lt. Duke's promise that no one would audit Quon's messages so long as he paid for the overage gave Quon a nigh-absolute expectation of privacy.[179] Indeed, the only potential diminishment of that right the circuit court mentioned was the possibility that someone might seek Quon's private messages under the California Public Records Act (CPRA), CAL. GOV'T CODE § 6253,[180] a possibility the Ninth Circuit dismissed as so slight as to not be worth considering.[181]

The Supreme Court rejected this reasoning. Assuming Quon *had* a reasonable expectation of privacy in his personal messages, the Court insisted, it is necessary to assess the *degree* to which Quon has a reasonable expectation of privacy in those messages,[182] and the likelihood (from the OPD's viewpoint) that reviewing the transcripts "would intrude on highly private details of Quon's life."[183] The Court concluded that Quon could reasonably expect only limited privacy in his text messages, because as a law enforcement officer, he "would or should have known that his [use

---

[178] *Id.* at 2631.

[179] Quon v Arch Wireless Operating Co., 529 F.3d 892, 908-09 (9th Cir. 2008); *see also* Quon v Arch Wireless Operating Co., 554 F.3d 769, 773 (9th Cir. 2009) (Wardlaw, J., concurring in the denial of rehearing en banc).

[180] CAL. GOV'T CODE § 6253 (West 2009), directs that "public records are open to inspection at all times . . . and every person has a right to inspect any public record."

[181] "The CPRA does not diminish an employee's reasonable expectation of privacy [because t]here is no evidence . . . suggesting that CPRA requests to the department are so widespread or frequent" as to deprive OPD personnel of a reasonable expectation of privacy. *Quon*, 529 F.3d at 907 (citations omitted) (internal quotation marks omitted). But consider: suppose there had been no OPD review of Quon's messages, but Mrs. Quon began to suspect that her husband was cheating on her. The thought occurred to her: "Jeff enjoys sexually explicit texting with me. If he has a girlfriend, he probably does the same with her." After consulting with an attorney, she filed a disclosure request per the CPRA. Whither Sgt. Quon's reasonable expectation of privacy then?

[182] *Quon*, 130 S. Ct. at 2631.

[183] *Id.* at 2631.

of the pager was] likely to come under legal scrutiny" for a variety of legitimate reasons.[184]

3. Availability of "Less Intrusive Means"

The Supreme Court was particularly critical of one aspect of the Ninth Circuit's decision in the case. The circuit court, in ruling for the plaintiffs, held that reading Quon's messages was unreasonable because the OPD could have employed several less intrusive means to evaluate the adequacy of the contract with Arch Wireless.[185] The "least intrusive means" concept, and the Supreme Court's treatment of it, merit a somewhat detailed look.

The phrase "least intrusive means" was first used by the Supreme Court in a Fourth Amendment context in *Florida v. Royer*.[186] A plurality of the Court stated that an investigative detention in the absence of probable cause "must be temporary and last no longer than is necessary to effectuate the purpose of the stop," and that "the investigative methods employed should be the *least intrusive* means reasonably available to verify or dispel the officer's suspicion in a short period of time."[187] Since *Royer*,

---

[184] *Id.* The Court commented:

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

Id. The Court did not mention the CPRA.

[185] The Ninth Circuit suggested two such means. First, the OPD could have ordered Quon not to use the pager for personal messages in September; the OPD would thereby obtain an accurate count of the number of characters he used on work-related messages during that month. *Quon*, 529 F.3d at 909. Second, it could have asked Quon to count the characters himself, redact out the personal messages, and permit OPD to review the redacted transcript. *Id.*

[186] Florida v. Royer, 460 U.S. 491 (1983).

[187] *Id.* at 500 (plurality opinion) (emphasis added) (citations omitted). Police officers assigned to airport duty, suspecting that Royer was a drug courier, stopped him and asked him to accompany them to a small police room, retained his ticket and driver's license, and did not inform him that he was free to depart. *Id.* Ultimately the officers

the "least intrusive" principle has been quoted approvingly in an occasional concurring or dissenting opinion.[188] In several decisions prior to *Quon*, however, a clear majority of the Court explicitly rejected the idea that Fourth Amendment searches and seizures were subject to a general "least intrusive means" requirement—in a substantial number of these cases, reversing decisions by the Ninth Circuit in the process.[189] In *Quon*, the Court did so again:

---

searched Royer's luggage and found a significant quantity of marijuana. *Id.* The Court held that the initial stop was reasonable. *Id.* at 501. But the court concluded that the rest of the officers' actions were unreasonable, given that nothing in the record suggested that safety or other legitimate concerns made it inappropriate to question Royer in the open. *Id.* at 501-02 (The Court also upheld a lower court finding that Royer had not consented to the secluded detention. *Id.* at 502-03.). Justice Brennan, whose concurring opinion provided the fifth and decisive vote to suppress the evidence, protested that the plurality opinion constituted a dangerous extension of the stop-and-frisk doctrine promulgated in *Terry v. Ohio*, 392 U.S. 1 (1968), but took some comfort from the plurality's apparent imposition of the least intrusive means limitation on *Terry* stops. Florida v. Royer, 460 U.S. 491, 511 n.* (1983) (Brennan, J., concurring).

[188] *See, e.g.*, Arizona v. Gant, 129 S. Ct. 1710, 1724 (2009) (Scalia, J., concurring); Illinois v. Caballes, 543 U.S. 405 (2005) (Ginsberg, J., dissenting); United States v. Sharpe, 470 U.S. 675, 693-94 (1985) (Marshall, J., concurring).

[189] In *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 663 (1995), the Court reversed the Ninth Circuit and upheld a school system's random urine testing of student athletes without particularized suspicion. *Id.* The Court commented: "We have repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment." *Id.* Similarly in another special needs context, see *United States v. Martinez-Fuerte*, 428 U.S. 543, 556-57 (1976), in which the Court, reversing the Ninth Circuit, rejected the "least intrusive means" approach in upholding the constitutionality of permanent immigration checkpoints on major roads near the Mexican border. *Id.* Likewise, see *United States v. Montoya de Hernandez*, 473 U.S. 531, 542-43 (1985), in which the Court reversed the Ninth Circuit's suppression of evidence obtained as a result of a sixteen-hour border detention of a woman suspected (correctly) of attempting to smuggle drugs into the U.S. in her alimentary canal. *Id.* In *United States v. Sokolow*, 490 U.S. 1, 11 (1989), the Court held that, contrary to the Ninth Circuit's view, DEA agents had a reasonable suspicion that Sokolow was a drug courier, and that their temporary detention of him at Honolulu Airport to question him was lawful. *Id.* Stressing that *Royer* was a plurality decision, the Court limited the "least intrusive" principle to

> the length of the investigative stop, not at whether the police had a less intrusive means to verify their suspicions before stopping Royer. The reasonableness of the officer's decision to stop a suspect does not turn on the availability of less intrusive investigatory techniques. Such a rule would unduly hamper the police's ability to make swift, on-the-spot decisions—here, respondent was about to get into a taxicab—and it would require courts to indulge in unrealistic second-guessing."

Sokolow, 490 U.S. at 11 (citations omitted). The Court has rejected arguments based on the "least intrusive" principle in cases from other circuits as well. *See, e.g.*, Bd. of Educ.

> This Court has repeatedly refused to declare that only the least intrusive search practicable can be reasonable under the Fourth Amendment. That rationale could raise insuperable barriers to the exercise of virtually all search-and-seizure powers, because judges engaged in *post hoc* evaluations of government conduct can almost always imagine some alternative means by which the objectives of the government might have been accomplished. The analytic errors of the Court of appeals in this case illustrate the necessity of this principle. Even assuming there were ways that OPD could have performed the search that would have been less intrusive, it does not follow that the search as conducted was unreasonable.[190]

The Court's basic approach to the issue makes good sense and good law. Government officials should not be held to a rigid requirement that, in the absence of probable cause, they must always utilize the procedure that will intrude least into someone's privacy. A "least intrusive" test is equally inappropriate whether the officials are acting in a criminal law enforcement capacity, or in furtherance of "special needs" relating to various public policy concerns, or merely as employers. But the Ninth Circuit did *not* assert that the OPD was required to use the *least* intrusive means to resolve its concerns about Quon's messages and the contract with Arch. Rather, it attempted to apply the second prong of the *O'Connor* test: determining whether the measures adopted were "reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [justification for the intrusion]."[191] The ultimate mandate of the Fourth Amendment is that a search or seizure, to be constitutional, must be "reasonable."[192] The availability of other means, which would achieve the government's legitimate goals while intruding less

---

v. Earls, 536 U.S. 822, 837 (2002) (upholding a school drug testing regime); United States v. Sharpe, 470 U.S. 675, 686-87 (1985) (upholding the twenty-minute detention of a motorist until police could follow up on their suspicions).

[190] City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) (citations omitted) (internal quotation marks omitted).

[191] Quon v Arch Wireless Operating Co., 529 F.3d 892, 908 (9th Cir. 2008) (quoting O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

[192] Recall that the Fourth Amendment protects "[t]he right of the people to be secure . . . against unreasonable searches and seizures . . . ." U.S. CONST. amend. IV. See *supra* note 9 and accompanying text for the complete text of the amendment.

into someone's privacy, surely is relevant—not an above-all-else factor, but relevant—in assessing the reasonableness of what the government in fact did. The Ninth Circuit cannot be faulted for considering the availability of less intrusive means; its error, rather, was in giving too much weight to them, rather than assessing the overall reasonableness of what the OPD did in light of all the circumstances.

Indeed, the Court in *Quon* implicitly endorsed the principle that, in evaluating the reasonableness of a particular search, a court should consider where that search falls on a spectrum of least intrusive to most intrusive. The Court noted that the police department in fact had conducted its review of Quon's text messages in a way that minimized somewhat the intrusion into his privacy. Although Quon had gone over the character limit during several months, Lt. Duke asked Arch Wireless for only two months' transcripts of Sgt. Quon's text messages.[193] The manner in which the OPD handled the case after Lt. Duke discovered Quon's misfeasance also demonstrates that the OPD took reasonable measures to minimize the intrusion into the privacy of all the plaintiffs. The Internal Affairs investigator assigned to the case read only Quon's on-duty messages, not those Quon sent or received while off-duty.[194] Another point is worth making, although the Court did not mention it: apparently the sexually explicit nature of Quon's text messages with his wife and girlfriend was not disclosed generally within the department. There is no suggestion, in any of the published opinions in the case, that the content of these text messages became general knowledge until, inevitably, they became public as a result of the plaintiffs' law suit.[195]

---

[193] *Quon*, 130 S. Ct. at 2631 ("While it may have been reasonable as well for OPD to review transcripts of all the months in which Quon exceeded his allowance, it was certainly reasonable for OPD to review messages for just two months in order to obtain a large enough sample to decide whether the character limits were efficacious.").

[194] *Id.* at 2631. "[U]sing Quon's time sheets, [the Internal Affairs office] took the transcripts and redacted with a black marker those portions that were transmitted while Quon was off-duty." Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1127 (C.D. Cal 2006). Later Quon's messages with Ms. Florio were examined to see if Quon was in any way involved in the misconduct at the OPD's dispatch center, *see* Part III-A-4, but no such evidence was found. *Id.*

[195] Contrast the behavior of the officers in *Casella v. Borders*, 649 F. Supp. 2d 435 (W.D. Va, 2009). Police seized a cell phone from Ms. Casella's boyfriend, discovered

The Court also stressed that the reasonableness of the OPD's review of Sgt. Quon's messages should also be assessed against what department personnel reasonably *expected* to find. The Court correctly observed that when the OPD undertook to review his messages, his superior officers had no reason to expect that the transcripts would reveal "highly private details" of his life, his wife's, and Ms. Florio's.[196] Although they *did* reveal private details, that was Quon's fault, not the OPD's.

In short, OPD supervisors simply wanted a quick and efficient way to determine whether the characters-per-month package with Arch was adequate. Given all of these circumstances, and the limited privacy expectation (if any) that Quon had in his text messages in the first place,[197] what the department did was quite reasonable, despite the availability of less intrusive (and less efficient) means.[198]

---

that the phone contained sexually explicit photographs of Ms. Casella and her boyfriend, and, allegedly, shared the photographs with dozens of others in and outside the police department. *Id.* at 437. The federal district court dismissed Ms. Casella's § 1983 claim on the ground that even if the seizure of the phone from her boyfriend and subsequent search of the phone violated her boyfriend's rights, there was no violation of her Fourth Amendment rights. *Id.* at 439; *see supra* note 91 and accompanying text. The court pointedly observed that she could still pursue state claims for intentional infliction of emotional distress. *Casella*, 649 F. Supp. 2d at 440.

[196] "From OPD's perspective, the fact that Quon likely had only a limited privacy expectation, with boundaries that we need not here explore, lessened the risk that the review would intrude on highly private details of Quon's life." *Quon*, 130 S. Ct. at 2631. The Court also commented that OPD's audit of Quon's messages on the OPD-supplied pager "was not nearly as intrusive as a search of his personal e-mail account or pager, or a wiretap on his home phone line, would have been." *Id.* This latter observation is of course true, but it is also essentially irrelevant. Because these techniques would not have revealed whether the OPD's contract with Arch was adequate, their use would not have been "justified at [their] inception . . . ." O'Connor v. Ortega, 480 U.S. 709, 726 (1987).

[197] *See supra* note 196 and accompanying text.

[198] It was reasonable for OPD officials to reject the two "less intrusive" methods suggested by the Ninth Circuit, assuming those methods had occurred to them. *See supra* note 185. Ordering Quon not to use the pager for personal messages for a month would have delayed resolution of the OPD's concerns; providing Quon with a transcript of his own messages and relying on him to edit out the personal ones also might have occasioned delays.

4. The Stored Communications Act (SCA) and the Fourth Amendment

Although the Court did not grant certiorari on the statutory issue, it nevertheless discussed the impact of the statute on the constitutional question, and concluded that a federal statute designed to protect privacy plays little or no role in deciding whether a reasonable expectation of privacy exists for purposes of the Fourth Amendment.

Arch Wireless provided Quon's transcripts when asked for them by the OPD.[199] The Ninth Circuit held that Arch violated the SCA by doing so.[200] Although the Supreme Court declined to grant certiorari on that issue,[201] the Ninth Circuit's decision on the SCA provided Quon and the other plaintiffs with a plausible argument: (1) ECPA was enacted to protect the privacy of electronic communications.[202] (2) The SCA, a major component of ECPA, was explicitly enacted to protect the privacy of stored electronic communications, including text messages.[203] (3) The law of the case, based on the Ninth Circuit's decision, is that the OPD obtained copies of Quon's text messages as a result of a violation of the federal statute designed to protect the privacy of such messages.[204] (4) Ergo, in accessing the copies, the OPD unlawfully intruded upon Quon's reasonable expectation of privacy.

The Court gave little credence or attention to this argument:

> [E]ven if the Court of Appeals was correct to conclude that the SCA forbade Arch Wireless from turning over the transcripts, it does not follow that petitioners' actions were unreasonable. Respondents point to no authority for the proposition that the existence of statutory protection

---

[199] *Quon*, 130 S. Ct. at 2626. Arch presumably acted on the assumption that since the pagers were owned by the OPD and that OPD was paying Arch for their use, the OPD had a legal right to the transcripts. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 898 (9th Cir. 2008).

[200] *See supra* Part III.C.

[201] *See supra* Part III.D.

[202] *See supra* Part I.B.2.

[203] *See supra* Part I.B.2.

[204] *See supra* Part III.C.

> renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise.[205]

The Court's almost casual dismissal of the SCA as virtually irrelevant in assessing Fourth Amendment-recognized privacy expectations is disturbing for several reasons. First, the cases the Court cited do not truly support the principle for which they are cited. Second, in *Quon* itself, the Court strongly indicated that *state* statutes may be relevant in determining when expectations of privacy are reasonable. Third, the Court ignored prior precedents relying on federal statutes or regulations in applying the Fourth Amendment.

The precedents the Court cited in this passage do not bear the weight the Court places on them. Each precedent involved the impact of *state* law on the scope of the Fourth Amendment.[206] In each, the Court emphasized the need to have a uniform standard *nation-wide* as to what the Fourth Amendment protected and what it did not.[207] The SCA, however, does not involve state law. It was enacted by the United States Congress and therefore has nation-wide application.

The Court's opinion in *Quon* acknowledged that even *state* statutes may be relevant in determining when an expectation of privacy is reasonable. In explaining why it decided not to decide whether Quon had a reasonable expectation of privacy in his text messages, the Court, discussing society's evolving attitudes about workplace privacy and electronic communications media, cited two

---

[205] City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010) (citing Virginia v. Moore, 553 U.S. 164, 168 (2008)); California v. Greenwood, 486 U.S. 35, 43 (1988)).

[206] *Greenwood* held that a home owner gave up his Fourth Amendment-protected reasonable expectation of privacy in his household garbage when he placed the garbage at the curb for collection, even though California's Supreme Court, applying state law, had previously held that a home owner retained that expectation. *Greenwood*, 486 U.S. at 43. *Moore* held that a search of a motorist incident to his arrest for a traffic violation was reasonable despite a state statute that precluded custodial arrests for mere traffic violations. *Moore*, 553 U.S. at 178.

[207] In *Greenwood*, the Court, by a 7-2 vote, rejected Greenwood's implicit "suggestion that concepts of privacy under the laws of each State are to determine the reach of the Fourth Amendment." *Greenwood*, 486 U.S. at 44. In *Moore*, a unanimous Court, per Justice Scalia, held that the Fourth Amendment was not written to incorporate individual state's arrest statutes. *Moore*, 553 U.S. at 178.

state statutes that require employers to notify employees when monitoring their electronic communications.[208]

The Court's casual rejection of the SCA as irrelevant to the expectation of privacy issue is inconsistent with its prior considerations of federal legislation when applying the Fourth Amendment. In *United States v. Watson*,[209] the Court, in holding that the Fourth Amendment permitted warrantless arrests for felonies even where the agents had ample time to obtain a warrant, cited several federal statutes that authorize such arrests.[210] In *Florida v. Riley*,[211] a plurality of the Court, holding that no "search" occurred when a police helicopter flew over the defendant's barn at a height of 400 feet to check out a tip concerning marijuana cultivation, relied in part on the fact that although the flight was at a lower altitude than Federal Aviation Commission regulations permitted to fixed-wing aircraft, the flight had not violated that regulation because it did not apply to helicopters.[212] In *Riley*, therefore, the plurality considered a

---

[208] *Quon*, 130 S. Ct. at 2630 (citing Brief for New York Intellectual Property Law Ass'n As Amici Curiae in Support of Respondents, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (08-1332), 2010 WL 1186480, at *22). The Brief in turn cited CONN. GEN. STAT. ANN. § 31-48d (West 2003) and DEL. CODE ANN. tit. 19, § 705 (2005). *See infra* note 271 and accompanying text where these provisions are summarized.

[209] United States v. Watson, 423 U.S. 411 (1976).

[210] *Id.* at 415-16. "Because there is a strong presumption of constitutionality due to an Act of Congress, especially when it turns on what is 'reasonable,' . . . the Court should be reluctant to decide that a search thus authorized by Congress was unreasonable and that the Act was therefore unconstitutional." *Id.* at 416 (quoting United States v. Di Re, 332 U.S. 581, 585 (1948)) (some internal quotation marks omitted). In so holding, the Court reversed a contrary ruling by the Ninth Circuit.

[211] Florida v. Riley, 488 U.S. 445 (1989). Police arranged for a helicopter to fly over Riley's greenhouse. *Id.* Through its partially open roof, the officer observed marijuana plants. Based on this information he obtained a search warrant pursuant to which marijuana was seized. *Id.* at 448-49.

[212] The plurality observed: "We would have a different case if flying at that altitude had been contrary to law or regulation. . . . [I]t is of obvious importance that the helicopter in this case was not violating the law . . . ." *Id.* at 451. The plurality added that it was not saying "that an inspection of the curtilage of a house from an aircraft will always pass muster under the Fourth Amendment simply because the plane is within the navigable airspace specified by law." *Id.* It is worth noting, however, that five Justices (a majority of the Court)—Justice O'Connor, whose concurrence was the deciding vote, and four dissenting Justices—insisted that the reasonableness of Riley's expectation of privacy depended, not on whether the helicopter flight complied with FAA regulations, but on whether helicopter flights at that altitude occurred frequently enough that Riley could reasonably be said to have knowingly exposed the contents of

federal regulation not directly related to privacy would be relevant in determining whether a privacy expectation was protected by the Fourth Amendment. If a federal aviation regulation and state statutes are relevant in weighing someone's privacy expectations under the Fourth Amendment, certainly an act of Congress enacted to protect privacy also merits consideration. Moreover, Congress, which is directly elected by and answerable to "society" (i.e., the electorate), presumably reflects, far better than the Supreme Court, what expectations of privacy "society" accepts as reasonable,[213] particularly in an area as challenging and fluid as new electronic communications media.

I do not mean to suggest that Congress should always have the last word on the question. Legislation diminishing an expectation of privacy is properly subjected to a Fourth Amendment challenge. But in enacting the SCA, Congress explicitly *created and protected* an expectation of privacy in communications that are sent and stored by a particular use of technology. Surely the SCA merits greater consideration than the back-of-the-hand the Court gave it in *Quon*.

The Court also rejected petitioners' SCA-based argument on a second, more valid ground. Even if Arch Wireless violated the SCA in turning over the transcripts,[214] this did not involve any wrongdoing by members of the OPD, who reasonably (albeit

---

his barn to the public. *Id.* at 455 (O'Conner, J., concurring). See the dissents of Justice Brennan, who wrote for Justices Marshall and Stevens, and Justice Blackmun. *Id.* at 456, 467 (Brennan, J., dissenting) (Blackmun, J., dissenting). Justice O'Connor joined the plurality opinion because, unlike the four dissenters, she concluded that Riley, not the state, had the burden of proof on the likelihood of such over flights, and had failed to present any (nor had the state). It is worth noting that, under the approach urged by Justice O'Connor and the four dissenters, the result might well depend on where the events occurred. In some parts of the country, at least, low-flying helicopters are a frequent, almost an every-day, occurrence. *See* Adam Nagourney, *Helicopters Jam the Skies over Los Angeles*, N.Y. TIMES, July 25, 2011, at A-1, *available at* http://www.nytimes.com/2011/07/26/us/26choppers.html.

[213] Criticizing the plurality opinion in *O'Connor v. Ortega*, Professor Jeffrey Rosen commented: "It's not surprising that Supreme Court justices, who are secluded in a marble palace and have spent most of their careers in the cosseted solitude of lower courts and universities, aren't terribly good at predicting how much privacy ordinary Americans expect in the workplace." JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 63 (2000).

[214] I consider this a dubious proposition. *See supra* note 158 and accompanying text.

perhaps incorrectly) assumed that the department was entitled to them:

> Furthermore, respondents do not maintain that any OPD employee either violated the law him-or-herself or knew or should have known that Arch Wireless, by turning over the transcript, would have violated the law. The otherwise reasonable search by OPD is not rendered unreasonable by the assumption that Arch Wireless violated the SCA by turning over the transcripts.[215]

Given that this provided the Court with an adequate ground to reject the plaintiffs' SCA-based argument, there was no need for the Court to write so dismissively about the statute, which makes its denigration of the SCA doubly disturbing.

5. Conclusion; Lip Service Deference to Justice Scalia's *O'Connor* Concurrence

Justice Kennedy concluded his lengthy application of the *O'Connor* plurality approach[216] thus: "Because the search was motivated by a legitimate work-related purpose, and because it was not excessive in scope, the search was reasonable under the approach of the *O'Connor* plurality."[217] His majority opinion then added the following sentence:

> For these same reasons—that the employer had a legitimate reason for the search, and that the search was not excessively intrusive in light of that justification—the Court also concludes that the search would be "regarded as reasonable and normal in the private-employer context" and would satisfy the approach of Justice Scalia's concurrence.[218]

---

[215] City of Ontario v. Quon, 130 S. Ct. 2619, 2632 (2010).

[216] Part III.B of the Court's opinion is 1488 words long (according to the WordPerfect word-counting function), of which almost 1100 words are devoted to the Court's application of the *O'Connor* plurality approach.

[217] *Quon*, 130 S. Ct. at 2632 (citing O'Connor v. Ortega, 480 U.S. 709, 726 (1987)).

[218] *Id.* at 2633 (quoting *O'Connor*, 480 U.S. at 732 (Scalia, J., concurring)).

Part III-B ends thus: "The search was reasonable, and the Court of Appeals erred by holding to the contrary. Petitioners did not violate Quon's Fourth Amendment rights."[219]

F. Justice Scalia's Quon *Concurrence*

Justice Scalia made it quite clear in his concurring opinion[220] that he was not mollified by the majority's passing reference to his *O'Connor* concurrence.[221] First, he asserted his continued conviction that the "operational realities" rubric for determining the Fourth Amendment's application to public employees invented by the plurality in *O'Connor v. Ortega*[222] is standard-less and unsupported. "In this case," he insisted, "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."[223] This passage in Justice Scalia's concurrence was uncharacteristically poorly drafted. The Fourth Amendment has always been understood to apply only to searches and seizures *by the government or its agents*, not to the conduct of private persons or entities.[224] Presumably what he meant was that "the proper threshold inquiry should be not whether [a reasonable expectation

---

[219] *Id.*

[220] *Id.* at 2634.

[221] *See supra* Part III.E.5.

[222] *Quon*, 130 S. Ct. at 2634 (Scalia, J., concurring) (quoting O'Connor v. Ortega, 480 U.S. at 717). Referring to this concept, the *Quon* majority commented, "were we to assume that inquiry into 'operational realities' were called for," it would be necessary to determine whether Lt. Duke's informal assurance concerning text messages created an expectation of privacy. *Id.* at 2629 (majority opinion).

[223] *Id.* at 2634 (Scalia, J., concurring) (citations omitted).

[224] Burdeau v. McDowell, 256 U.S. 465 (1921) (holding that the Fourth Amendment, and its exclusionary rule, are "a restraint upon the activities of sovereign authority, and . . . not . . . a limitation upon other than governmental agencies."). They do not, therefore, apply to the acts of "a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." United States v. Jacobsen, 466 U.S. 109, 113 (1984) (citing Walter v. United States, 447 U.S. 649, 662 (1980)). Thus, if someone was acting as an informant at the time he conducted a search, his conduct is measured against Fourth Amendment standards. But if a private person or entity is acting strictly on his, her, or its own initiative, it may turn over the information or evidence thus obtained, and it is admissible at trial even if the private conduct, if it had been done by a government agent, would have violated the defendant's Fourth Amendment rights. *See, e.g.*, *id.*

of privacy exists with regard] to messages on *public* employees' employer-issued pagers, but whether [such an expectation exists] *in general* [with regard to] such messages on employer-issued pagers."

Second, Justice Scalia wrote, given the Court's unanimous conclusion under both approaches that the OPD's review of Quon's text messages was reasonable, it was unnecessary and misleading for the Court to provide its lengthy application of the *O'Connor* plurality approach. By discussing the *O'Connor* plurality approach at such length, Justice Scalia complained, the Court was hinting, or at least would be perceived as hinting, that this approach was the governing law.[225]

IV. WHAT THE COURT DID NOT DECIDE, AND WHY: EXPECTATIONS AND STANDARDS

Having reviewed what the Court *did* decide, this Article now addresses the more interesting issues: what the Court did *not* decide (including some that were not before the Court). First, against what standard should a government employee's privacy expectations be measured—the *O'Connor* plurality approach, Justice Scalia's approach, or neither—and whether "[t]he principles applicable to a government employer's search of an employee's *physical office* apply with at least the same force when the employer intrudes on the employee's privacy in the *electronic* sphere?"[226] Second, suppose the jury had found, as Quon maintained, that his OPD superiors' real reason for reviewing his text messages was to investigate suspicions of wrongdoing on his

---

[225] *See* City of Ontario v. Quon, 130 S. Ct. 2619, 2635 (2010).

> Despite the Court's insistence that it is agnostic about the proper test, lower courts will likely read the Court's self-described "'instructive'" expatiation on how the *O'Connor* plurality's approach would apply here (if it applied), as a heavy-handed hint about how they should proceed. Litigants will do likewise, using the threshold question whether the Fourth Amendment is even implicated as a basis for bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees' use of electronic media. In short, in saying why it is not saying more, the Court says much more than it should.

Id. (emphasis omitted) (citations omitted).

[226] *Id.* at 2630 (emphasis added).

part—would the review, as conducted, still be reasonable? Third, can someone who exchanges text messages, e-mail or the like with a government employee have a reasonable expectation of privacy as to those messages, even if the employee does not?

A. Measuring Expectations of Electronic Privacy

1. The Majority's Waffle: Part III.A of the Court's Opinion

In Part III.A of his majority opinion, Justice Kennedy provided a lengthy explanation of why it *would not decide* whether Quon had a reasonable expectation of privacy.[227] First, Justice Kennedy issued a paean to judicial restraint:

> The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.[228]

His majority opinion then identified the many uncertainties that the issue raised:

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

---

[227] *Id.* Part III.A is nearly 900 words long, of which nearly 800 are devoted to the explanation.

[228] *Id.* at 2629.

> employees, especially to the extent that such policies are clearly communicated.[229]

This passage is significant for several reasons.[230] First, it acknowledges uncertainty as to whether the *O'Connor* plurality approach is the right one.[231] Second, it also recognizes that what happens in the non-governmental workplace will, to some extent, shape what expectations will be reasonable in the government workplace—a concession that appears to be more than just an attempt to mollify Justice Scalia. Third, it acknowledges that no social consensus exists yet as to what privacy expectations might be reasonable in connection with emerging electronic communication media, let alone what expectations might be reasonable concerning their use in the workplace, whether private or governmental. The Court noted that "many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency,"[232] and also noted that at least a few states have enacted statutes that require employers to notify employees concerning when their electronic communications would be monitored.[233]

The pros and cons of the Court's decision not to decide are discussed in Part IV.A.3, *infra*.

---

[229] *Id.* at 2630 (citing O'Connor v. Ortega, 480 U.S. 709, 715) (citations omitted).

[230] Even though the Court decided nothing in this regard, Justice Kennedy's comments on this issue, and Justice Scalia's response, probably garnered more media attention than any other aspect of the case. *See, e.g.*, Orin Kerr, *The Fourth Amendment, New Technologies, and the Case for Caution*, VOLOKH CONSPIRACY (Apr. 20, 2010, 12:40 PM), http://volokh.com/2010/04/20/fourth-amendment-and-new-technologies-and-the-case-for-caution/; *see also*, Adam Liptak, *Justices are Long on Words but Short on Guidance*, N.Y. TIMES, Nov. 18, 2010, at A1, *available at* http://www.nytimes.com/2010/11/18/us/18rulings.html?_r=1.

[231] If five or more of the seven Justices who signed Justice Kennedy's opinion firmly believed that the O'Connor plurality approach was how the law should address these issues, they could have said so.

[232] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) (citing Brief of Electronic Frontier Foundation, Center for Democracy & Technology et al. as Amici Curiae in Support of Respondents, City of Ontario, California v. Quon, 130 S. Ct. 2619 (2010) (08-1332), 2010 WL 1063463, at *16-20).

[233] *Id.* at 2630 (citing Brief for New York Intellectual Property Law Association As Amici Curiae in Support of Respondents, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (08-1332), 2010 WL 1186480, at *22). The Brief in turn cited DEL. CODE ANN. tit. 19, § 705 (2005), and CONN. GEN. STAT. ANN. § 31-48d (West 2003). See *infra* note 271 for a brief summary of these provisions.

2. Justice Scalia's "I Told You So"

Justice Scalia, in his concurrence, agreed that "there is no need to answer [the] threshold question" about whether the plaintiffs had a constitutional expectation of privacy, because even if they did, the OPD's review of Quon's messages was reasonable.[234] But since no need existed to *decide* that "threshold question," Justice Scalia protested, there was no need for the Court to address it at all.[235] He predicted that the Court's unnecessary discussion of how the *O'Connor* plurality approach might apply to the issue would lead to mischief and confusion among litigators and lower court judges.[236] Moreover, he argued, the majority inadvertently demonstrated the inadequacies of the *O'Connor* plurality formula:

> [I]n fleshing out its fears that applying that test to new technologies will be too hard, the Court underscores the unworkability of that standard. Any rule that requires evaluating whether a given gadget is a "necessary instrumen[t] for self-expression, even self-identification, on top of assessing the degree to which the law's treatment of [workplace norms has] evolve[d]," is (to put it mildly) unlikely to yield objective answers.[237]

Justice Scalia also suggested that the majority exaggerated the difficulties in the question, and acerbically reminded his colleagues that, difficult or not, a case may someday arise that will require that issue to be addressed: "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-times-they-are-a-changin' is a feeble excuse for disregard of duty."[238]

---

[234] *Quon*, 130 S. Ct. at 2634 (Scalia, J., concurring).

[235] "To whom do we owe an additional explanation for declining to decide an issue, once we have explained that [the issue] makes no difference?" *Id.* at 2635 (Scalia, J., concurring) (emphasis omitted).

[236] *Id.*; *see supra* Part III.F.

[237] *Id.* at 2635 (Scalia. J., concurring) (citations omitted) (quoting *id.* at 2629-30 (majority opinion)).

[238] *Id.* The phrase Justice Scalia used—"the times they are a changin'"—is the title and refrain of a song Bob Dylan wrote in the fall of 1963, which captured the mood of

3. Evaluation; Comparing the Two Approaches

Despite Justice Scalia's scornful criticism, the Court's restraint was probably a good thing, for a variety of reasons. First, it appears from the oral argument that several of the Justices were confused or unclear as to how these pagers worked.[239] For example, some of the Justices may not have been aware that messages were sent through, and stored on, Arch Wireless's computers, rather than going directly from the sender's pager to the recipient's like a phone call.[240] An understanding of this technology would certainly prove useful, if not essential, in analyzing the degree to which privacy expectations in such messages would be reasonable.[241]

Second, at least some prominent scholars worried publicly that a broad decision on the privacy expectation issues in *Quon*

---

many during that troubled and tempestuous period. The basic message of the song is summarized in this verse:

> Come mothers and fathers/ Throughout the land/ And don't criticize/ What you can't understand/ Your sons and your daughters/ Are beyond your command/ Your old road is rapidly agin'/ Please get out of the new one if you can't lend your hand/ For the times they are a-changin'

The Times They Are A-Changin', BOBDYLAN, http://www.bobdylan.com/us/songs/times-they-are-changin (last visited Feb. 28, 2012). For a concise description of the song, its references and significance, see OLIVER TRAGER, KEYS TO THE RAIN: THE DEFINITIVE BOB DYLAN ENCYCLOPEDIA 624-27 (2004).

[239] During oral argument, Chief Justice Roberts asked, "Maybe—maybe everybody else knows this, but what is the difference between the pager and the e-mail?" Transcript of Oral Argument at 29-30, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 28-1332).

[240] During the presentation for the plaintiffs, Chief Justice Roberts asked, "Well, I didn't—I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing." *Id.* at 48. Justice Scalia chimed in: "You mean it doesn't go right to the other thing?" *Id.* Counsel explained: "It's—I mean, it's like with e-mails. When we send an e-mail, that goes through some e-mail provider, whether it be AOL or Yahoo, it's going through some service provider . . . ." *Id.*

[241] Unlike a telephone call, electronic communication technology requires the sender and receiver's ISP's to retain a copy of the contents of an electronic communication at least for a time (The technology is described in Part III.B, *supra*.). ECPA authorizes ISPs to access the contents of customers' messages with no significant restrictions, so long as the ISP does not disclose those contents to others. 18 U.S.C. § 2701(c) (2006); *see also* FISHMAN & MCKENNA, *supra* note 10, § 7:20. Commercial ISPs agree contractually not to do so; otherwise they would lose customers to competitors who do promise to respect their customers' privacy; but when an employer acts as ISP for its employees, it has less motive to make such a promise, and may have valid business or official reasons to monitor certain uses of its equipment and systems.

might put the law into a straightjacket that could cause enormous problems as technology, and society's attitudes toward that technology evolve.[242] As the Court acknowledged, society is still in the process of sorting out how these issues should be addressed.[243]

Justice Scalia's approach—that a government employee's constitutional right to privacy in the workplace should be the same as the legal privacy rights of employees in the private workplace—has its attractions. First, it provides courts with an already existing body of law to apply (assuming that body of law is of sufficient clarity) rather than requiring judges to grope in a vacuum. Second, it avoids creating an artificial distinction which arguably serves no real purpose. Assume two professors' offices and computers are searched by the universities at which they teach, each case involving suspected violations of similar school rules and regulations. Why should a professor at a public university enjoy any greater, lesser, or different right to privacy in

---

[242] It may be significant that Professor Orin Kerr, who is generally and deservedly acknowledged as one of the nation's leading legal experts on the SCA and on electronic communications generally, wrote several blog entries during the pendency of the case urging the Court not to offer a broad ruling governing expectations of privacy; and that in 2003, Professor Kerr took a leave of absence from George Washington Law School to serve as a law clerk for Justice Kennedy, who wrote the Court's opinion in *Quon*. *See* Orin Kerr, *Communicating With Those Who Have No Privacy Rights: The Hard Question in* City of Ontario v. Quon, VOLOKH CONSPIRACY (Mar. 31, 2010, 1:50 AM), http://volokh.com/2010/03/31/communicating-with-those-who-have-no-privacy-rights-the-hard-question-in-city-of-ontario-v-quon/; Orin Kerr, *Some Thoughts on the Reply Brief in* City of Ontario v. Quon, VOLOKH CONSPIRACY (Apr. 13, 2010, 7:58 PM), http://volokh.com/2010/04/13/some-thoughts-on-the-reply-brief-in-city-of-ontario-v-quon/; Orin Kerr, *Supreme Court Grants Cert on Fourth Amendment Protection in Text Messages*, VOLOKH CONSPIRACY (Dec. 14, 2009, 12:29 PM), http://volokh.com/2009/12/14/supreme-court-grants-cert-on-fourth-amendment-protection-in-text-messages/; Orin Kerr, *The Fourth Amendment, New Technologies, and the Case for Caution*, VOLOKH CONSPIRACY (Apr. 20, 2010, 12:40 PM), http://volokh.com/2010/04/20/fourth-amendment-and-new-technologies-and-the-case-for-caution/; Orin Kerr, *Thoughts on the Oral Argument in City of* Ontario v. Quon, VOLOKH CONSPIRACY (Apr. 19, 2010, 1:44 PM), http://volokh.com/2010/04/19/thoughts-on-the-oral-argument-in-city-of-ontario-v-quon/; Orin Kerr, *Will the Supreme Court Rethink Public Employee Privacy Rights in Quon?*, VOLOKH CONSPIRACY (Dec. 14, 2009, 10:00 PM), http://volokh.com/2009/12/14/will-the-supreme-court-rethink-public-employee-privacy-rights-in-quon/. Other scholars made similar arguments in the lead-up to the Quon decision. *See, e.g.*, Dale Carpenter, *Ninth Circuit Finds Fourth Amendment Protection in Text Messages*, VOLOKH CONSPIRACY (June 18, 2008, 4:39 PM), http://volokh.com/2008/06/18/ninth-circuit-finds-fourth-amendment-protection-in-text-messages/.

[243] *See supra* notes 220-42 and accompanying text; *infra* notes 244-74 and accompanying text.

her office, than would a professor at a private university? Why should the applicable legal standard be any different? Justice Scalia's approach argues that the standards should be the same.

The question arises: Is there a significant difference between the *O'Connor* plurality approach, and Justice Scalia's tort law, employment law standard?

The common law tort of invasion of privacy is generally divided into four different kinds of wrongdoing: (1) intrusion upon seclusion; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness.[244] Another tort often associated with these is the intentional, reckless or negligent infliction of emotional damage.[245] The latter four actions are based upon what a defendant did with information once it was obtained; the first, intrusion upon seclusion, is the common law tort that parallels the plaintiffs' claims in *Quon.*

Restatement of Torts, Second § 652B, Intrusion Upon Seclusion, defines that tort as follows: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[246]

Applied to a private sector workplace, to make out a prima facie case for intrusion upon seclusion, a plaintiff must produce evidence sufficient to support a finding that the employer intruded into plaintiff's subjective expectation of privacy; that this expectation was one that society would view as reasonable; that, under the circumstances, society would view the intrusion as highly offensive;[247] and that the employer had no reasonable

---

[244] RESTATEMENT (SECOND) OF TORTS §§ 652A-652E (1977); *see also* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 381, 389 (1960).

[245] RESTATEMENT (THIRD) OF TORTS § 45-46 (Tentative Draft No. 5, 2007) (intentional or reckless infliction and negligent infliction).

[246] RESTATEMENT (SECOND) OF TORTS § 652B (1977).

[247] Richard E. Kaye, *Cause of Action to Recover Damages for Invasion of Private Sector Employee's Privacy by Intrusion upon Seclusion*, *in* 42 CAUSE OF ACTION 2d 255, §§ 4-5 (West 2009); *see also* L. Camille Hebert, 1 EMP. PRIVACY L. § 8:13 (West 2010) (Employer searches as invasion of privacy: "[A] plaintiff generally is required to establish that the employer committed an unauthorized intrusion into the seclusion of the plaintiff that would be offensive to an ordinary person."). Another useful source may be available in the not-to-distant future. A Westlaw search of the RESTATEMENT

business justification for the intrusion.[248] In other words, the plaintiff must establish that (1) the employer engaged in a highly offensive intrusion upon the employee's privacy, and that (2) the intrusion was unjustified under the circumstances.[249]

First let us compare the common law tort and the *O'Connor* plurality approach with regard to the nature of the intrusion. The *O'Connor* plurality requires a plaintiff to produce evidence sufficient to support a finding[250] that her government employer intruded into her Fourth Amendment-protected reasonable expectation of privacy; in assessing whether the plaintiff has met this burden, a court must consider "the operational realities of the workplace."[251] This closely parallels the first element of the common law tort action. It is perhaps a bit easier for the public employee to establish the "intrusion" element of her cause of action under the *O'Connor* plurality approach because, unlike the private sector employee, she need not establish that the intrusion

---

(THIRD) OF EMPLOYMENT LAW (database REST-EMPL) for the word "privacy" produces a handful of sections in Chapter 4, each of which promises, "Issues of employee privacy are examined in Chapter 7 of this Restatement." However, accessing the RESTATEMENT's table of contents (by clicking on "table of contents" on the left, about a third of the way down from the top of the screen) reveals that at present the RESTATEMENT consists of only chapters 1-6 and chapter 8. I've been guilty of being tardy with a manuscript or two, so I didn't laugh too loudly when I noticed that.

[248] Kaye, *supra* note 247, § 7. Other defenses, including consent, are discussed in Kaye. *Id.* §6.

[249] *Id.* §§ 4-7.

[250] "Sufficient to support a finding" is the burden of proof a party must satisfy in order to avoid a summary judgment against it at the pleading stage, or a directed verdict at the trial stage. *See, e.g.*, Adickes v. S. H. Kress & Co., 398 U.S. 144, 175-76 (1970) (Blackmun, J., concurring); Law Co., Inc. v. Mohawk Const. & Supply Co., Inc., 577 F.3d 1164, 1170 (10th Cir. 2009); FED. R. CIV. P. 56(c). In *O'Connor*, the trial judge granted summary judgment for the defendants. Ortega v. O'Connor, 764 F.2d 703, 704 (9th Cir. 1985). This amounts to a ruling that, granting all of Dr. Ortega's factual allegations, he had failed to satisfy this burden. The Ninth Circuit reversed, ruling that Dr. Ortega did indeed satisfy his burden of showing an intrusion into his Fourth Amendment-protected privacy and that the defendants failed to satisfy its burden of producing evidence that its conduct was justified. *Id.* at 707. The Ninth Circuit therefore granted summary judgment for Dr. Ortega on the liability issue, and remanded for a trial strictly on the issue of damages. *Id.* The Supreme Court affirmed the Ninth Circuit decision that Dr. Ortega had satisfied his burden of production as to the intrusion, but concluded that a material issue of fact existed as to whether the intrusion was reasonable, and remanded for trial. O'Connor v. Ortega, 480 U.S. 709, 728-29 (1986); see *supra* note 101 for the ultimate disposition of Dr. Ortega's law suit.

[251] *O'Connor*, 480 U.S. at 709-10; *see supra* Part II.B.

was "highly offensive," but unless the intrusion was in fact highly offensive, plaintiff's suit is unlikely to succeed, either as a matter of law,[252] or as a factual issue for the jury.

With regard to the justification issue—here, too, the differences between the two bodies of law, if they exist, appear to be minor at most. If plaintiff satisfies her burden of production as to the intrusion, tort law and the *O'Connor* plurality both place the burden on the employer to establish that the intrusion is justified. Each recognizes that as a general matter, an intrusion is justified if the employer had a valid reason—business[253] or governmental[254]—for it. The *O'Connor* plurality's two-part test adds a bit of flesh to the skeleton, but its two considerations—"first . . . whether the . . . action was justified at its inception," and "second . . . whether the search as actually conducted was reasonably related in scope to the circumstances which justified the interference in the first place"[255]—are just as relevant in the private sector workplace as the governmental workplace.[256]

Each body of law also recognizes an additional defense, besides justification—consent.[257] In the context of electronic communications media, most courts have held that so long as the employer gives the employee specific notice that the employer reserves the right to monitor or review her use of employer-supplied equipment, her use of it constituted implicit consent to the monitoring or review.[258] In this context, as in the law enforcement context,[259] the word "consent," in its everyday

---

[252] If the plaintiff establishes only that her government employer made only a minor intrusion into her privacy, the agency will not have to establish much of a justification for it to be entitled to judgment as a matter of law.

[253] Kaye, *supra* note 247, § 7.

[254] *See infra* note 255-56 and accompanying text.

[255] *O'Connor*, 480 U.S. at 726; *see supra* Part II.B.

[256] "[T]he sufficiency of an employer's business justification for intruding on employees' privacy is a function of (1) the validity and veracity of the economic or health/safety rationales for the intrusion; and (2) whether the means or methods used were proportionate to the employer's purported justification for the intrusion." Kaye, *supra* note 247, § 7; *see id.* §§ 8-24 (reviewing the law as it applies to a variety of information-gathering techniques and the justifications asserted by employers).

[257] Concerning the private sector workplace, see Kaye *supra* note 247, § 6. Concerning consent generally as a defense to civil or criminal charges of unlawful electronic surveillance, see FISHMAN & MCKENNA, *supra* note 10, §§ 5:101-5:107.

[258] FISHMAN & MCKENNA, *supra* note 10, § 6:5.

[259] *See supra* Part I.A.2.

meaning, does not accurately reflect reality. "Consent" implies a choice. Here the employee's choice is stark: agree to the employer's policy, or lose the job.[260]

Many government agencies and private sector employers now require employees to sign a statement acknowledging that they have no reasonable expectation of privacy in their use of the employer's communications equipment and systems.[261] If an employer asked my advice on this matter, I would recommend that every employee be required to sign such a statement,[262] and would also advise the client to order supervisory personnel not to make any "informal" or "off-the-record" assurances to the contrary.[263] The odds are that this practice is, or soon will become, so pervasive and routine that employees are unlikely to have grounds to sue either a government employer based on the Fourth Amendment, or a private sector employer based on intrusion upon seclusion.[264] Such suits are likely to arise only against small, unsophisticated employers, and in cases where, like *Quon*, a supervisor gives employees "unofficial" or "off-the-record" assurances that, despite the official policy, no monitoring or review will be conducted.[265]

---

[260] *See, e.g.*, Frye v. IBP, Inc., 15 F. Supp. 2d 1032, 1041-42 (D. Kan. 1998) (holding that an employee's submission of a urine sample, in compliance with his employer's drug testing policy, constituted consent and therefore a defense under RESTATEMENT (SECOND) § 652B (2011), even though his refusal would have cost him his job).

[261] *See generally* WILLIAM S. HUBBARD, The NEW BATTLE OVER WORKPLACE PRIVACY ch. 7 (1998); MICHAEL R. OVERLY, E-POLICY: HOW TO DEVELOP COMPUTER, E-MAIL, AND INTERNET GUIDELINES TO PROTECT YOUR COMPANY AND ITS ASSETS (1999).

[262] For examples of such statements, see the books cited in the previous note.

[263] I would also advise the client: (1) not to monitor or review an employee's use of the equipment unless a good business reason presented itself; (2) where the need arises, monitor or review in a way that minimizes the intrusion into the employee's privacy to the extent reasonably practicable; (3) restrict dissemination of the information obtained to those with a clear need to know; and (4) use the information as discreetly as possible.

[264] If the employer makes inappropriate disclosure or use of the information obtained from the monitoring or review, this may give the employee a cause of action for example for public disclosure of private facts, false light, etc. *See supra* notes 244-46 and accompanying text.

[265] It is easy to understand what motivated Lt. Duke to give his informal assurance to the members of the OPD SWAT team. *See supra* notes 137-39 and accompanying text. He had no desire to snoop on the members of the SWAT team, and saw no harm in reassuring them of that. But if he had not made his informal reassurances, perhaps Quon would have been more discrete in his use of the pager; and if not, in all likelihood the district court and Ninth Circuit would have dismissed the plaintiffs' law suit on the

4. The Need for Legislation

Given that the *O'Connor* plurality approach and the common law regarding right to privacy in the workplace so closely resemble each other, does it really matter which ultimately becomes the law governing privacy in the governmental workplace?

I believe it does. To assess the Fourth Amendment reasonableness of government conduct solely by what is done by employers in non-government workplaces would be an abdication of the government's and (at least, in the absence of congressional legislation the Supreme Court's) responsibility to determine what intrusions by the *government* into individual privacy are reasonable. As Justice Brandeis famously admonished eight decades ago, "[o]ur government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example."[266] The *Quon* majority recognized that it would be wrong for the Court to ignore what is happening in the non-government workplace,[267] but there is merit to the proposition, implicit in the *O'Connor* plurality approach, that the Fourth Amendment should not blindly follow the practices of the private sector. This is particularly so given that, regarding workplace privacy (among other employment matters), private employers often can pretty much set whatever rules they please, because workers lack the individual or collective power to object.[268]

---

ground that Quon, and those with whom he texted, had no reasonable expectation of privacy in the first place.

[266] Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting) (protesting the admission at trial of evidence obtained by unlawful wiretaps by federal agents).

[267] City of Ontario v. Quon, 130 S. Ct. 2619, 2629-30 (2010).

[268] Federal and state law do protect workers in many fundamental ways, but from what experts in the field tell me, there is no explicit body of labor law legislation that addresses these issues. Labor unions can insist on some degree of protection of worker privacy, but can do so only in industries that are heavily unionized, and in recent decades, unions have represented a shrinking portion of the labor market. According to the Census Bureau's Statistical Abstract of the United States 2011, in 1985, nearly 17 million workers were union members and more than 19 million were covered by union contracts—18% and 20% of the labor market respectively; by 2009 those numbers had diminished to 15 million and 16.9 million (12.3% and 13.6%). This decline is even more noteworthy considering that the nation's population grew by roughly 70 million people during the intervening quarter century. Moreover, while in 1985, nearly two-thirds of those whose jobs were covered by unions were private sector workers, by 2009 less than

According to data collected by the American Management Association (AMA), private sector employers are monitoring their employees more than ever before. According to the AMA's 2007 Electronic Monitoring & Surveillance Survey, 66% of employers monitor their employees' Internet connections, 65% of companies use software to block connections to inappropriate Web sites, 43% of companies monitor e-mail, 45% monitor time spent on the telephone and numbers called, 16% record phone conversations, and almost half (48%) of the companies surveyed use video monitoring to counter theft, violence, and sabotage.[269]

Given these complexities, defining privacy expectations should be the responsibility of Congress, not the Court.[270] Legislative models exist from which Congress could construct a reasonable regime. As the Court noted in *Quon*, at least two state statutes require employers to notify employees in advance if they plan to monitor or review employees' use of employer-provided communications equipment, or if it reserves the right to do so.[271]

---

half were private sector workers—a total of 8.2 million. Given that fewer workers in the private sector are in industries with a strong union presence, most private sector workers will have little leverage to bargain for greater privacy. The labor statistics in this footnote are found in the CENSUS BUREAU STATISTICAL ABSTRACT 429 tbl. 663. The population figures for 1985 and 2009 may be found at *Population Estimates: Historical Data*, U.S. CENSUS BUREAU, http://www.census.gov/popest/national/national.html (last visited Feb. 21, 2012).

[269] Kaye, *supra* note 247, at 290. According to the AMA, of the 304 U.S. companies that participated in the survey: 27% represent companies employing 100 or fewer workers, 101-500 employees (27%), 501-1000 (12%), 1001-2500 (12%), 2501-5000 (10%), and 5001 or more (12%). AM. MGMT. ASS'N, 2007 ELECTRONIC MONITORING AND SURVEILLANCE SURVEY 12 (2008), *available at* http://www.amanet.org/download.aspx?filename=%2fimages%2felectronic-monitoring-surveillance-survey08.pdf&pid=41.

[270] I write this sentence assuming that Congress will somehow find the time to devote to anything other than not resolving the nation's debt ceiling and fiscal crises (I originally wrote the preceding sentence in late July 2011, as the fiscal apocalypse (defaulting on the nation's debt) drew nigh. In light of the temporary, jury-rigged "compromise" that was ultimately struck, I see no reason to revise it.).

[271] *Quon*, 130 S. Ct. at 2630 (citing CONN. GEN. STAT. § 31-48d (2003); DEL. CODE ANN. tit. 19, § 705 (West 2005)). Each statute requires advance written or electronic notice to the employee. CONN. GEN. STAT. 31-48d(b) (2003); DEL. CODE ANN. tit. 19, § 705(b) (West 2005). Each authorizes a state agency to impose a civil penalty on an employer who fails to comply with the provision. CONN. GEN. STAT. § 31-48f (2003); DEL. CODE ANN. tit. 19, § 705(d) (West 2005) (specifying in the latter provision that the civil penalty is not an exclusive remedy and does not preclude a suit for damages under any other state or federal law). Each statute contains exceptions where the monitoring or review is conducted in cooperation with law enforcement officials. CONN. GEN. STAT. § 31-48d(d) (2003); DEL. CODE ANN. tit. 19, § 705(b) (West 2005).

Many (perhaps most) federal agencies already provide such notice; Congress should make this mandatory. Beyond this basic step, consider the federal statute that regulates the interception of telephone calls. Although Title III is not a model of clarity in this regard, in essence it permits employers (whether in the private or governmental sectors) to surreptitiously monitor an employee's phone conversations only if, and to the extent, that it has a valid business purpose to do so. Excessive monitoring violates the statute and therefore is civilly actionable.[272] A similar regime would serve as well with regard to electronic communications, including e-mails, text messages, and the like.[273]

The federal government has attempted to encourage and inspire states and private entities to emulate it in a variety of contexts.[274] It is plausible to argue that, with regard to workplace privacy, Congress should take the initiative to set an example that enlightened non-government employers might choose to follow. Until it does, the *O'Connor* plurality approach to the issue, for all its vagueness and other shortcomings, is preferable to Justice Scalia's.

---

[272] The preceding sentence is a very brief summation of a somewhat complex subject. *See* FISHMAN & MCKENNA, *supra* note 10, §§ 6:3-6:13. Moreover, an employer may deprive employees of this protection merely by informing them that all calls may be monitored. As a general rule, an employee who uses a phone while on notice that it may be monitored is deemed to have consented to the monitoring. *See id.* § 6:5.

[273] Even if such a statute was enacted applying this approach to electronic communications media generally, and was made applicable to the private sector as well as to the government, employers could frustrate such a statute by requiring employees to sign an acknowledgement that they have no expectation of privacy when they use employer-supplied communications media. Even so, such a statute might have the aspirational impact of encouraging employers to act reasonably with regard to employee privacy.

[274] See, for example, Exec. Order No. 13,514, 3 C.F.R. § 248 (2009), on Federal Leadership in Environmental, Energy, and Economic Performance, setting forth the administration's plan to lead by example in the area of energy conservation and environmentally sensitive operations. Similarly, see the Telework Enhancement Act of 2010, 5 U.S.C. §§ 6501-06 (2010), setting forth the government's policy for allowing federal employees to telecommute and encouraging the private sector to do the same. *See* Steve Vogel, *Report Urges U.S. Government To Boost Workplace Flexibility*, WASH. POST (May 14, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/05/13/AR2009051303688.html (relating that a government report that led to the enactment of that statute urged the federal government to "lead by example" by including flexible work arrangements).

B. Suppose the Jury Had Found That the Review Was to Investigate Suspicions of Quon's Wrongdoing

At trial, the plaintiffs claimed that the real reason OPD personnel reviewed Sgt. Quon's text transcripts was to investigate suspicions of wrongdoing on his part, but the jury found that the review was motivated only by concerns over the adequacy of the OPD's contract with Arch.[275] Cases no doubt have arisen or will arise, however, in which an agency monitors or examines an employee's use of government-provided electronic communication equipment to investigate possible wrongdoing. Thus, it is worth considering how this might have affected the Court's resolution of the issues in *Quon*.

At first glance, the answer might be: not at all. In *O'Connor*, after all, the plurality opinion and Justice Scalia's concurrence each emphasized that their approaches applied whether the agency's search was for a needed file, or to investigate suspicions of employee wrongdoing.[276] In the latter situation, depending on what the employee is suspected of doing, the agency's need to act quickly might be more compelling than existed in *Quon*.[277] On the other hand, where the employee is suspected only of occasional use of the equipment to send and receive personal messages while on duty, the need for immediate action by the agency is less compelling. The agency, moreover, would have reason to suspect that the monitoring or review would reveal some personal details of the employee's life. In *Quon*, the Court, in upholding the reasonableness of the OPD's review of Quon's text messages, stressed that at the outset the OPD did *not* anticipate that the messages would include highly personal information.[278]

Given the unique facts in *Quon*—that he was told officially that he had no expectation of privacy in the messages; that he was given only informal assurances to the contrary; and that the nature of his job made it likely that some of his messages, at any rate, might become relevant evidence if a SWAT team action ever lead to litigation—I suspect the Court would have held that the

---

[275] *See supra* note 155 and accompanying text.

[276] *See supra* Part II.C.1 (plurality opinion) and II.C.2 (Justice Scalia's concurrence).

[277] Such would be the case, for example, if the employee was suspected of using the device to harass other individuals or reveal confidential information to outsiders.

[278] *See supra* Part III.E.2.

OPD's review of Quon's messages was reasonable even if the jury *had* concluded that the OPD reviewed Quon's messages to investigate suspicions that he was engaging in some kind of misfeasance. But professorial speculation is small comfort to public officials who must make on-the-spot decisions.

C. Privacy Expectations of Those With Whom Quon Texted

Given, as the Court unanimously agreed, that OPD's review of Sgt. Quon's text messages did not violate his Fourth Amendment rights, the question remained: did it violate the rights of the other plaintiffs? In Part III.C of the majority opinion, the Court acknowledged this issue, noting that the plaintiffs and defendants "disagree[d] whether a sender of a text message can have a reasonable expectation of privacy in a message he knowingly sends to someone's employer-provided pager."[279] It was not necessary for the Court to address that issue, however, because the other plaintiffs based their case solely on the theory that the OPD review violated Sgt. Quon's rights and, derivatively, their own.[280] Once the Court rejected Sgt. Quon's Fourth Amendment case, the other plaintiffs' claims also fell.[281]

The Court's refusal to discuss the issue was correct given the facts, and, given the facts, it is easy to assume that the other plaintiffs did not press any claims independent of Sgt. Quon's because they all knew Sgt. Quon was using a pager issued by the OPD. This aspect of the case would have been far more interesting if one of Sgt. Quon's text-correspondents did *not* know that the sergeant was using an OPD device to send and receive the messages.

Suppose, for example, a police department (PD) provided an officer with a pager, or a cell phone with text messaging ability, for use on official business. The officer used it to exchange sexually explicit messages with a woman who was not an employee of the PD and was unaware that the officer was using a

---

[279] City of Ontario v. Quon, 130 S. Ct. 2619, 2633 (2010).

[280] *Id.* In fact, all four plaintiffs (Quon, his wife, his girlfriend, and Sgt. Trujillo) were represented by the same attorney before the Court.

[281] *Id.* On this point, the Court was unanimous—neither Justice Scalia nor Justice Stevens commented on this aspect of the decision.

device issued to him by the PD. [282] After awhile, the PD decided, for legitimate departmental reasons, to review the officer's text messages, and did so in a reasonable manner, and thereby discovered the contents of the officer's and the woman's messages. The officer would have no Fourth Amendment claim against the PD for a variety of reasons.[283] Might the woman have a Fourth Amendment claim against the department, independent of the officer's?

At first blush, the answer is clearly no—if it was reasonable for the PD to review the text messages the officer sent and received, it logically follows that both sides of each exchange come within the scope of the review. This follows the approach the law applies to the surreptitious *interception* of communications authorized by Title III: if the authorities obtain a lawful tap or bug and execute it lawfully, the intercepted communications are admissible against each participant—those named in the application and intercept order, and also those, originally unknown, who are overheard engaging in crime-related conversations.[284] This logic arguably applies with equal force to an after-the-fact review of an employee's messages lawfully conducted pursuant to the Fourth Amendment's special needs doctrine—Or does it?

Title III authorizes the *surreptitious* interception of a suspect's wire, oral, or electronic communications, because the interception must be surreptitious if the government is to have any realistic chance of achieving its authorized goals—common sense suggests that a criminal will not plan or discuss his criminal activities over a phone that he knows is tapped or in a premises

---

[282] I am using this gender line-up in my hypothetical for convenience, and to parallel the facts in *Quon*. I acknowledge, of course, that the roles might be reversed—she might be the police officer and he might be the civilian; or they could both be of the same gender.

[283] If he had been informed that he had no reasonable expectation of privacy in his messages, and that the PD reserved the right to review them, that would be enough to deprive him of Fourth Amendment protection. Even if he did have some right to privacy, it presumably would be limited for the reasons the Court discussed in *Quon*. *See supra* Part III.E.2. Finally, even assuming he had some reasonable expectation of privacy, if the PD had a valid reason to review those messages and did so in a reasonable manner, although its review would intrude into his privacy, it would not violate it.

[284] *See generally* FISHMAN & MCKENNA, *supra* note 10, §§ 8:27-8:34.

that he knows is bugged.[285] Often, the officers reasonably expect, or learn as the investigation progresses, that many, even most, of those with whom the initial targets converse are also engaged in crime. Moreover, an interception order authorizes the interception only of communications relevant to the crimes under investigation; if the police learn that a particular individual is not involved in criminal activity, they must "minimize" the interception of his or her conversations.[286]

None of these circumstances, assumptions, or restrictions would apply to the woman in my hypothetical. Unlike the person who meets with, calls, or receives calls from a suspected drug dealer whose office is bugged or whose phone is tapped, there is no basis to assume that she is engaged in any wrongdoing.[287] More important, the PD has no compelling reason to avoid informing those with whom the officer texts, that he is using a PD device and the messages are subject to PD review.[288] Indeed, serving such notice would *enhance* the PD's interests, because it would

---

[285] Common sense is not always an accurate predictor of how people actually behave. Prison and jail inmates and those with whom they converse are on notice that their phone calls will be monitored or recorded, as will their face-to-face visits. Despite these warnings, many prisoners do use prison phones or face-to-face visits to discuss or plan crimes, and recordings of those conversations are routinely admitted into evidence against the participants in the conversations . . . (Perhaps these prisoners and those with whom they converse are not very bright, or perhaps they have a remarkable facility for denying reality, or are simply too bored to care.). For a discussion of the various legal theories justifying this result, see FISHMAN & MCKENNA, *supra* note 10, §§ 6:42-6:57; admissibility of the recordings against the non-prisoner participant is discussed *id.* §§ 6:51 (phone calls) and §§ 6:53-6:54 (oral communications during prison visits).

[286] Title 18 U.S.C. §2518(5) (2006) requires each interception order to contain a directive "that the authorization to intercept . . . shall be conducted in such a way as to minimize the interception of communications not otherwise" relevant to the investigation. It is universally acknowledged, of course, that even under the best of circumstances, some irrelevant conversations will be intercepted and recorded, including many involving people not engaged in criminal activity. For a detailed discussion of the "minimization clause," see FISHMAN & MCKENNA, *supra* note 10, §§ 8:101-8:107. For a discussion of how law enforcement officials should attempt to comply with the minimization provision, see *id.* ch. 15. For a discussion of the issues that arise at a pretrial "minimization hearing," see *id.* §§ 35:50-35:74.

[287] If she is aware that the officer is married, her conduct in exchanging sexually explicit text messages with him is immoral, but of itself, that is no business of the PD's, and she should not thereby forfeit an otherwise protected expectation of privacy.

[288] Obviously exceptions exist, such as where the officer is acting "under cover" of a different identity for investigative purposes.

(presumably) discourage others from sending personal messages to that device.

As a rule, whenever we make or receive a phone call, or send or receive an e-mail or text message, we assume that its privacy is legally and technologically protected. Those of us who are knowledgeable about the law or communications technology are aware that there are many ways in which that privacy may be breached;[289] but in general, the only real risk is that the person with whom we are communicating will share what was said with others.[290]

There are, of course, situations in which this assumption is not justified, but usually we are given notice. Many private companies and public agencies provide such notice on their telephone lines: after dialing a company or agency number, we have all heard messages advising us that the call might be "monitored for quality control purposes" or the like.[291] Similarly, many government agencies (and perhaps some companies) automatically include in each outgoing e-mail a notice to this effect,[292] or at least an advisory to examine the agency or company's privacy statement on its Web site.[293]

---

[289] Some of the legal means are discussed *supra* Parts I.A.2 and I.B.

[290] Each of us has from time to time been the victim of a betrayal of confidentiality; each of us has committed such a breach. A few decades ago, the betrayals were generally limited to the immediate acquaintances of those concerned. One of the dubious blessings of the Internet is that it is now possible for a betrayed confidence to circulate among thousands and even millions of strangers. *See, e.g.*, T.R. Reid, *Thanks for Last Night! (cc: The Entire World)*, WASH. POST, Dec. 18, 2000, at C1.

[291] This experience is becoming less and less frequent as companies and agencies switch to automated phone answering systems ("Please make a selection from the following menu. To start a new subscription, press 1 . . .") designed to prevent a caller from ever speaking to a human being.

[292] Florida's may be the most all-encompassing in this regard. FLA. STAT. ANN. § 119.01 (West 2012) provides, in pertinent part:

> (1) It is the policy of this state that all state, county, and municipal records are open for personal inspection and copying by any person. Providing access to public records is a duty of each agency.
>
> (2)(a) Automation of public records must not erode the right of access to those records. As each agency increases its use of and dependence on electronic recordkeeping, each agency must provide reasonable public access to records electronically maintained and must ensure that exempt or confidential records are not disclosed except as otherwise permitted by law.

Given all this, the woman in our hypothetical has a plausible argument that the failure to provide her with notice[294] falsely created the impression that her messages with the officer enjoyed the usual degree of privacy enjoyed by private text messages between two individuals; and that the absence of such notice means that the PD intruded upon *her* Fourth Amendment-protected reasonable expectations of privacy, even if it did not intrude upon the officer's.

Including such a notice in all outgoing e-mail and text messages would not completely protect outsiders from the risk that a nondescript e-mail address or phone number is actually a government or corporate device. If I exchange phone numbers with woman at a social event and decide to send her a rather personal text message describing the powerful impression she made on me and how her image haunts my dreams and fantasies,[295] I may have no way of knowing that the number to which I am texting is her FBI-issued smart phone; that realization would come only when I receive her reply, with privacy notice included. If for some reason her superiors at the Bureau are monitoring her text messages and therefore read what I sent her,

---

> (b) When designing or acquiring an electronic recordkeeping system, an agency must consider whether such system is capable of providing data in some common format . . .

I have corresponded with a police officer in Florida. The following appears at the end of each of his e-mails:

> PLEASE NOTE: Florida has a very broad public records law (F. S. 119). All e-mails to and from County Officials are kept as a public record. Your e-mail communications, including your e-mail address may be disclosed to the public and media at any time.

Incidentally, the officer informs me that this notice does not appear in each text message he sends.

[293] Even in the absence of such notice, common sense should warn us that when we receive an e-mail from or send an email to firstname.lastname@megacorp.com or Jeff.Quon@OntarioPD.gov, given the corporate or governmental nature of the entity involved, the possibility exists that someone in addition to the named recipient may read what we send.

[294] Such notice need not be elaborate or lengthy. The shortest I've been able to come up with is: "Official use only. See www.OPD.city/privacy," which consists of forty characters.

[295] This situation is entirely hypothetical. I have been happily married for more than forty-three years—without interruption, and to the same woman. *See supra* note 59.

well, tough luck on me. Government entities and private employers are not required to do everything conceivably possible to protect the privacy of those who communicate with their employees;[296] they should only be required to act reasonably. But it places no great burden on employers to include a brief notice about the lack of privacy in all outgoing e-mails, text messages and the like. Failure to do so might reasonably be held to create an expectation of privacy.

CONCLUSION

In *City of Ontario v. Quon*, the Supreme Court could have clarified many aspects of the law concerning (1) a government employee's claim that his employer improperly intruded upon his Fourth Amendment-protected reasonable expectation of privacy, and (2) the applicability of the Fourth Amendment to an employee's use of employer-supplied electronic communications equipment. It chose to resolve neither of these issues. In fact, it left the law more unsettled than it had been.

As to the first issue, prior to *Quon*, it had been generally understood that the plurality opinion in *O'Connor v. Ortega* was in fact the law.[297] In *Quon*, however, the majority explicitly declined to endorse this view, instead pointing out that the *O'Connor* plurality approach did not capture a majority of the Court, and that the deciding vote in *O'Connor* was cast by Justice Scalia, who rejected the idea of a discrete Fourth Amendment analysis to govern employer-employee searches, and instead argued that the law that governs workplace privacy in the non-government sector should apply as well to the government workplace.[298] The *Quon* majority explained why it would not resolve that issue in *Quon*,[299] and then proceeded to apply the *O'Connor* plurality approach to the facts of the case anyway.[300]

---

[296] Perhaps the technology exists which could interrupt any message I send to an employee of a government agency or private entity, informing me that all messages sent from or to that entity's system are subject to review by the entity, and asking whether, knowing this, I still want to send the e-mail or text message to Z.

[297] *See* Part III, introductory paragraph.

[298] City of Ontario v. Quon, 130 S. Ct. 2619, 2628 (2010).

[299] *Id.* at 2629.

[300] *See supra* Part III.E.2.

As a result, litigants and lower courts now must in essence litigate and decide the expectation of privacy issue twice: first they must address the facts of the case as if the *O'Connor* plurality approach was the law; second, they must do the same employing the approach Justice Scalia espoused in his *O'Connor* and *Quon* concurrences. Indeed, courts have begun to do so.[301] Fortunately, in the overwhelming majority of cases, the results will be the same under both approaches, because the law governing privacy issues in the non-governmental workplace is nearly indistinguishable from the Fourth Amendment approach outlined by the *O'Connor* plurality.[302]

As to the second issue, there are two compelling reasons why the Court was probably wise in declining to issue a broad ruling applying the Fourth Amendment to the use of employer-supplied electronic communications media in the workplace. First, in resolving the privacy implications of modern communications technology, it is helpful to understand how the technology works, and at least some members of the Court apparently lacked this knowledge.[303] Second, the technology is so new, and is evolving so quickly, that society's attitudes and expectations with regard to them are far from settled. Congress, rather than the Court, is the branch of government best equipped to study and resolve such issues by legislation, which, unlike a constitutional decision by the Supreme Court, can be amended to adjust to changing conditions and expectations.

The facts in *Quon* suggested, but did not actually present, two additional issues. First, should the employer be held to a more exacting standard if its inquiry is based on suspicions of the employee's misconduct, than if its purpose is merely to review the efficacy of workplace rules or practices? The logical answer is: It depends on the nature of the alleged misconduct, and the strength of the suspicions.[304] Second, assuming the *employee* lacked a reasonable expectation of privacy, does the government agency nonetheless have any obligations regarding the privacy

---

[301] *See, e.g.*, True v. Nebraska, 612 F.3d 676, 681-82 (8th Cir. 2010); Richards v. Los Angeles, 775 F. Supp. 2d 1176, 1182-86 (C.D. Cal. 2011).

[302] *See supra* Part IV.A.3.

[303] *See supra* Part III.E.3.

[304] *See supra* Part IV.B.

expectations of those with whom the employee communicated? A plausible argument exists that the agency should take reasonable steps to assure that the non-employee participants in the communication are informed of the non-private nature of the communication.[305]

These are questions of some significance. In the absence of congressional action (or a Supreme Court decision), private and public sector employers are in essence resolving them unilaterally, by requiring, as a condition of employment, that employees acknowledge that they lack an expectation of privacy regarding their use of employer-supplied communications equipment and media.[306] Perhaps ultimately this is good public policy—it assures that employers can intervene to prevent misuse of their communications media, and it puts employees on notice regarding personal use such equipment. As the *Quon* majority acknowledged, moreover, most people have ample opportunity to communicate without employer oversight by using their own personal computers, cellular phones, and "smart" phones with texting and Internet access, the price of which are now well within the reach of most Americans.[307] But privacy is a fundamental and cherished right in this country.[308] Those of us who are employed tend to spend roughly half of our weekday waking hours at work.[309] It is disquieting that our right to privacy during such an important and substantial part of our lives is being decided solely by our employers, based on what they perceive to be their own self-interest.

---

[305] *See supra* Part IV.C.

[306] *See supra* Part IV.A.4.

[307] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010); *see supra* Part IV.A.1. Inevitably, however, people who do own their own computers and smart phones will occasionally use office equipment to communicate on private matters.

[308] There are those among us who have renounced privacy and have chosen to share intimate details of their lives on the Internet, and some who, to the extent possible, live in front of video cameras. For my own rather dyspeptic view of these developments, see Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations and the Media*, 72 GEO. WASH. L. REV. 1503, 1511-15 (2004).

[309] This assumes that the average fully employed person is awake seventeen hours a workday and spends roughly 8.5 hours on the job. Given that many employees are now electronically accessible for work-related matters during their supposedly "off" hours, the latter estimate may be low.

Not so long ago, Congress had the interest and energy to consider issues like these, and the ability to make the difficult choices and compromises necessary to resolve them.[310] Unfortunately Congress in 2012 has not displayed any of these characteristics, and there is little immediate reason for confidence that it will soon acquire them. The likely result is that individual privacy in the workplace will erode, quietly, bit by bit, without the public attention and study the matter deserves. Although the Court was correct in declining to issue a broad, sweeping decision, the decision had done little to reverse or impede that erosion.

APPENDIX. *QUON*: A USER'S MANUAL

The Court's restraint in *Quon*, however appropriate it may have been under the circumstances, leaves litigators and lower courts with significant questions as to how to proceed in new cases that arise involving workplace privacy. The outline that follows may prove useful in any attempts to follow the holding in *Quon*, when a government employee sues, alleging that the agency for which he or she worked violated his or her workplace privacy under the Fourth Amendment. I make no claim that it is an "open sesame" that will ineluctably lead to a winning argument or reversal-proof decision. I hope, however, that it will give litigants and courts a structure that will assure that all relevant issues and arguments are considered.

A. Determine whether the investigation clearly did, or clearly did not, intrude into an employee's (E) reasonable expectation of privacy

Logically, the first issue to address is whether a "search" under the Fourth Amendment occurred at all. If it did not, then E

---

[310] Congress did so in 1968, when it enacted Title III, and in 1986 when it enacted the Electric Communications Privacy Act, and has amended each statute several times since, as in the U.S.A. PATRIOT Act and subsequent legislation. Congress did likewise when it enacted the many provisions designed to protect computer integrity and privacy. For an overview of such legislation, see FISHMAN & MCKENNA, *supra* note 10, §§ 1:10-1:21, 1:23.

has no Fourth Amendment claim,[311] and is unlikely to have a common law invasion of privacy claim under state law, either. Often this issue is easy to resolve applying both the *O'Connor* plurality and Scalia concurrence approaches.

> 1. Some information-gathering methods clearly *are* intrusions. Examples: physically searching E's desk, file drawers, office, and personal property within E's office;[312] concealing a microphone or camera in E's private workspace, without advance notice to E.[313] If there clearly was a Fourth Amendment search or a tort law intrusion, proceed to Part C.
>
> 2. Some information-gathering methods clearly are *not* intrusions. Examples: a supervisor standing in the hallway overheard what E said in his office. As Justice Stewart said in *Katz*, "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[314] The same is probably true if E negligently exposed the information—for example, by leaving personal documents in the company photocopier.[315] If no such intrusion occurred, then render judgment for the defendant on the Fourth Amendment and pendant intrusion upon solitude claims.[316]
>
> 3. If (as in *Quon*) it is unclear whether the agency's actions intruded into E's reasonable expectation of privacy, the court should then consider whether, as in *Quon*, it can duck that issue by assuming there was such an intrusion, and evaluating whether that intrusion was reasonable under the circumstances. See Part C, *infra*. If, as in *Quon*, the answer to

---

[311] Because the Fourth Amendment protects only against unreasonable searches and seizures, if no "search" has occurred, *see supra* Part I.A.1, plaintiff has no Fourth Amendment basis on which to complain.

[312] *See supra* Part II.B.

[313] In *O'Connor*, a majority of the Court concluded that, barring unusual circumstances, an employee does have a reasonable expectation of privacy in his or her office. *See supra* Part II.B. Surreptitious electronic surveillance of private space is a per se intrusion into that expectation. Electronic surveillance issues are discussed further in Part D and E of this appendix.

[314] Katz v. United States, 389 U.S. 347, 351 (1967).

[315] There is no reason that the Fourth Amendment or tort law should protect someone from his or her own negligence or inattention.

[316] If the agency made improper use of the information, plaintiff may still have state law claims for intentional infliction of emotional distress, etc. *See supra* notes 244-46.

the latter question is "Yes," then judgment is rendered for the defendant as to the Fourth Amendment and intrusion upon solitude claims.

4. If it is necessary to resolve the reasonable expectation of privacy issue, move on to Part B.

B. Resolving whether the agency intruded upon E's reasonable expectation of privacy—in general

A number of factors must be considered, including:

1. Did the agency have a published policy concerning privacy or monitoring that covered its conduct in the case?

a. How widely publicized was it; did E have actual or, at least, constructive notice?

b. Does the policy clearly incorporate the type of monitoring, review or surveillance that was conducted in E's case?

c. Was E given any "unofficial" or "off-the-record" assurance that the policy would not apply in his or her situation?

d. Do compelling factual or social policy reasons exist for ruling that E had a reasonable expectation of privacy despite being on notice that he or she did not?

2. Assuming the issue is not resolved in Part B.1:

a. Apply the *O'Connor* plurality approach. Given "[t]he operational realities of the workplace,"[317] did E have a subjective expectation of privacy against the investigative conduct by the agency? If so, is that expectation one society accepts as reasonable? Useful sources include leading treatises on the Fourth Amendment.

b. Apply Scalia's *O'Connor-Quon* concurrence approach, i.e., the law governing the tort of intrusion upon solitude in the workplace, which differs little from the *O'Connor*

---

[317] *O'Connor*, 480 U.S. at 717.

plurality approach set forth in the preceding paragraph.[318]

C. If there was an intrusion into E's reasonable expectation of privacy: Determine whether the intrusion was reasonable (or unreasonable) as a matter of law, or whether that is an issue for the jury.

Reasonableness is based on a variety of factors:

1. The goals and subject matter of the agency's investigation of E.

a. If the agency conducted its search or inquiry to enable it to fulfill its public policy responsibilities, a plausible argument exists (for whichever party it favors) that *only* the *O'Connor* two-step approach should apply, because (the argument goes), the case falls into a different "special needs" category than the employer-employee category. Example: the urine sample tests for law enforcement officials upheld in *National Treasury Employees Union v. Von Raab*.[319]

b. If the agency E worked for is not a law enforcement agency and the search was initiated and conducted by a law enforcement agency seeking evidence of criminal conduct, then the traditional Fourth Amendment requirements (probable cause that a crime was committed and, probably, a search warrant), not the "special needs" standard, should apply.[320]

c. If the agency E worked for is not a law enforcement agency and E was suspected of conduct that might be criminal but the search was conducted by the agency for

---

[318] Useful sources include L. CAMILLE HEBERT, 1 EMP. PRIVACY LAW § 8:13; RICHARD E. KAYE, CAUSE OF ACTION TO RECOVER DAMAGES FOR INVASION OF PRIVATE SECTOR EMPLOYEE'S PRIVACY BY INTRUSION UPON SECLUSION, 42 CAUSE OF ACTION 2D 255 §§ 4-5 (2007); and, once it is published, chapter seven of the RESTATEMENT (THIRD) OF EMPLOYMENT LAW. No doubt there are others.

[319] 489 U.S. 656 (1989). See *supra* note 122 for further discussion of *Von Raab*.

[320] Note that this applies only if E has established that what was done constitutes a search. If E was on notice that he had no expectation of privacy in his office e-mails, for example, the fact that the agency turned them over to a law enforcement official who requested them does not create an expectation of privacy in those messages.

which he worked, the presumption should be that the primary purpose of the investigation is to further administrative or workplace goals, in which case the "special needs" rule set forth in C.1.d, *infra*, should apply.

d. If the investigation was clearly intended to further workplace goals unrelated to broader public policy concerns and did not involve allegedly criminal activity, apply both the *O'Connor* plurality approach and Justice Scalia's tort-and-employment law approach to each information-gathering method which intruded into E's reasonable expectation of privacy.

2. Applying the *O'Connor* plurality approach:

a. Assess how important it was to the agency to obtain the information, how important it was to obtain the information promptly, and (where applicable) how important it was to obtain the information without notice to E. Within these parameters, afford high importance as to whether the agency's actions were an "efficient and expedient way" to obtain the needed information.[321]

b. Assess whether E's expectation of privacy was extensive, or only limited. *Quon* and *O'Connor* provide examples at the opposite ends of the spectrum. Compare what the Court categorized as Sgt. Quon's only limited (at best) reasonable expectation of privacy in his text messages, because as a police officer he should have known that they could be reviewed for a variety of reasons,[322] with Dr. Ortega's obvious and quite strong expectation of privacy in his office, desk and file drawers, particularly items that were obviously non-work-related papers and highly personal.[323]

c. Consider whether, when they conducted their search, the investigators reasonably expected to come across highly personal information, or not. If they reasonably did not expect to discover highly personal information, this is

---

[321] City of Ontario v. Quon, 130 S. Ct. 2619, 2631 (2010).

[322] *See supra* Part III.E.2.

[323] *See supra* Part II.B.

a significant factor in favor of reasonableness, even if they in fact learned highly personal information as a result.[324]

d. The availability of less intrusive means is *not*, of itself, a controlling consideration (except, perhaps, in extreme cases), and a litigant or judge should say so three or four times to make it clear that the writer[325] knows that this is not a controlling consideration;[326] but it is a relevant consideration nevertheless. If a litigant or judge cites these other means, however, he or she should include a factually specific discussion as to whether each of these means would have enabled the agency to obtain the equivalent information with equal, or nearly equal, efficiency.

e. Did the agency make reasonable attempts to minimize the intrusion at the outset, and (if applicable) after they realized that they were discovering highly personal information?

(1) Did the searchers restrict where they looked, or how intensely they read or listened or watched? *O'Connor* and *Quon* again provide useful contrasts. In *O'Connor*, hospital employees examined, and seized, obviously personal items in which the hospital had no legitimate interest;[327] in *Quon*, the OPD requested transcripts of only two months of Sgt. Quon's text messages,[328] and the Internal Affairs officer assigned to the case read only the transcripts of messages Sgt. Quon sent and received while on duty.[329]

(2) If the searchers seized personal items of E that were of no legitimate interest to the agency, how long did the agency retain them before returning them? A court should not expect instantaneous

---

[324] The Court so held in *Quon*. *See supra* Part III.E.2.

[325] I mean here, the attorney writing a brief or the judge writing an opinion.

[326] I exaggerate here for effect. If the court in question is the Ninth Circuit, it should raise the ante to at least a dozen times. *See supra* note 189.

[327] *See supra* notes 90, 93 and accompanying text.

[328] *See supra* note 193 and accompanying text.

[329] *See supra* note 194 and accompanying text.

> evaluation and return of personal items that get swept up in the search, but prolonged retention aggravates the degree of intrusion.[330]
>
> (3) How many individuals were given access to personal information that was discovered during the search, and what use (if any) was made of such information? Once again, *O'Connor* and *Quon* provide useful contrasts. In *O'Connor*, the hospital used obviously personal information gleaned from the search to impeach Dr. Ortega's witnesses at trial;[331] in *Quon*, it appears that no unnecessary disclosures about the text messages occurred.[332]

f. In some cases, it will be clear, as a matter of law, that the agency's intrusion into E's privacy was reasonable.[333] In others, it will be clear as a matter of law, that the agency's intrusion into E's privacy was unreasonable.[334]

---

[330] *See supra* note 101.

[331] *See supra* note 101.

[332] *See supra* text accompanying note 195.

[333] The Supreme Court so held in *Quon*. *See supra* Part III.E.2.

[334] *See, e.g.*, Richards v. Los Angeles, 775 F. Supp. 2d 1176, 1176 (C.D. Cal. 2011). The L.A. Department of Public Works received an anonymous tip that one dispatcher, Richards, had engaged in sexual intercourse with a visitor when she was assigned, alone, to the dispatch room at night. *Id.* at 1179. To investigate this allegation, a camera was hidden in the dispatch room—a location with a locked door, no windows, and limited access, particularly at night, when the building was largely deserted. *Id.* at 1179-80 (The judge ruled that the circumstances gave dispatchers a reasonable expectation of privacy, *id.* at 1182, which seems correct given the facts.). The camera ran continuously for more than two months (until it was discovered by a dispatcher), recording the conduct of every dispatcher during that period. *Id.* at 1181. Dispatchers, when they were on duty alone, "engaged in a number of private acts in the dispatch room," including changing their clothing, pumping breast milk, picking zits, "and . . . other acts normally reserved for private spaces." *Id.* at 1180. The officer assigned to watch the videos was instructed to check out the behavior of all of the dispatchers, not just Richards's. *Id.* After the discovery of the cameras, the dispatchers sued. *Id.* at 1881. The judge held that the surveillance of the rest of the dispatchers (who were suspected of no wrongdoing) was per se unreasonable, and granted them summary judgment on that issue, a ruling that seems completely indisputable. *Id.* at 1185 (The judge held likewise for Richards—that ruling strikes me as somewhat debatable.).

g. In some cases, however, reasonableness under the circumstances will be a contested issue of fact, for the jury to resolve.[335]

3. Apply Justice Scalia's tort-and-employment law approach:

a. All of the factors in C.2.a through C.3.e logically would be relevant here, as well.

b. The ultimate question of fact, however, is somewhat different, or at least must be worded differently, because to succeed in a tort suit for intrusion upon seclusion, plaintiff must establish that, given all the circumstances, "the intrusion would be highly offensive to a reasonable person."[336]

D. Special circumstances—Claims involving "real-time" electronic surveillance: intercepting "wire, oral, or electronic communications"; video surveillance

1. Apply Parts A, B, and C, *supra*.

2. Keep in mind as well that if the employer's conduct constituted the "interception" (in essence, real-time monitoring, or recording) of the "contents" of a "wire, oral or electronic communication" by means of any "device," the conduct may constitute a felony in violation of 18 U.S.C. §2511(1), and may also be civilly actionable pursuant to 18 U.S.C. §2520, independent of any Fourth Amendment or common law claim.[337]

3. By contrast, there is no federal law that punishes or regulates the use of video surveillance. Thus, if such surveillance involved observation or recording only of E's physical conduct, without audio, a federal cause of action can

---

[335] The Supreme Court so held in *O'Connor*. *See supra* note 101.

[336] RESTATEMENT (SECOND) TORTS § 652B; *see supra* Part IV.A.3. Useful sources are suggested *supra* note 318.

[337] Each of the terms in quotation marks is defined in 18 U.S.C § 2510 (2006). For the definitions and their implications, *see generally* FISHMAN & MCKENNA, *supra* note 10, ch. 2. Many states have enacted similar statutes. For a detailed examination of crimes and civil actions relating to communications privacy, see *id*., ch. 3. See also JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE (2011), which also provides exhaustive coverage of these issues.

only be predicated on the Fourth Amendment, not on any federal statute.[338]

E. Claims involving review of stored electronic communications or use of office computers

1. Apply Parts A, B, and C, *supra*.

2. If the employer's conduct constituted unlawful accessing of stored electronic communications in violation of the SCA, the conduct may also constitute a crime in violation of 18 USC §2701(a), and may also be civilly actionable pursuant to 18 U.S.C. § 2707, independent of any Fourth Amendment or common law claim.[339]

3. If the employer's conduct involved surveillance of the employee's use of a computer, that may also provide a basis for a cause of action.[340]

4. Regarding the Stored Communications Act and the Computer Fraud and Abuse Act: if you are in the Ninth Circuit, *Theofel* and *Quon v. Arch Wireless* are controlling law; otherwise, although a party may cite them as persuasive authority, hopefully the judge will wisely decline to follow them.[341]

---

[338] For extensive coverage of these issues, see FISHMAN & MCKENNA, *supra* note 10, ch. 30.

[339] *See generally id.* ch. 7; *see also* CARR & BELLIA, *supra* note 337 (also providing extensive coverage of these issues); Orin S. Kerr, *A User's Guide to the Stored Communications Act—And a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

[340] *See generally* ORIN S. KERR, COMPUTER CRIME LAW (2d ed. 2009); FISHMAN & MCKENNA, *supra* note 10, chs. 21-27, which includes an exhaustive examination of all federal and state legislation on the subject.

[341] *See supra* note 158.