

ONTARIO V. QUON: IN SEARCH OF A REASONABLE FOURTH AMENDMENT

Miles K. Palley[†]

“That the individual shall have full protection in person and in property is a principle as old as the common law; but it has been found necessary from time to time to define anew the exact nature and extent of such protection.”¹

As the opening sentence of *The Right to Privacy* suggests, privacy is a moving target: technology develops, societal norms adjust, and bright line legal rules regulating privacy require updating. Today, society’s understanding of what privacy means is in tremendous flux. Technology tends to make it easier to gather information in powerful, beneficial, and profitable ways.² The last two decades have seen an explosion in the collection and use of personal information that poses new challenges to society’s conceptions of privacy.³ However, along with the challenges to privacy in the current environment, there are some considerable benefits. Easy and instant communication with loved ones, customized access to information of all kinds, and the ability to build and use massive searchable databases of information are just a few key features of the information age. As society continues to embrace rapidly developing technology—with all its myriad benefits and risks to private life—privacy can no longer plausibly be characterized simply as “the right to be let alone.”⁴

A modern conception of privacy protection should require courts to balance the benefits of information sharing, collection, and use against the

© 2011 Miles K. Palley.

† J.D. Candidate, 2012, University of California, Berkeley School of Law. I offer my sincere thanks to Chris Hoofnagle for his mentorship and comments as I researched and wrote this Note. Thanks also to my friends and peers that carefully edited my work: Elizabeth Eraker, David Stark, Yan Fang, and Daniel Park.

1. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

2. See DANIEL J. SOLOVE, *THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE* 2 (2004) (“Shards of data from our daily existence are now being assembled and analyzed—to investigate backgrounds, check credit, market products, and make a wide variety of decisions affecting our lives.”).

3. See *id.*

4. Warren & Brandeis, *supra* note 1, at 193.

sensitivity of the information at issue.⁵ When the collection serves an important purpose or confers a substantial benefit on the public, legal restrictions on information collection and use should be tempered by these benefits. On the other hand, when the collection or review of information is avoidable or of limited public benefit, and the information's use or dissemination is potentially damaging, legal restrictions should be developed both to provide relief to individuals who have their information improperly released and to give clear guidance to potential defendants. Courts and legislatures have been slow to adopt this proportional approach to privacy in many cases, but it is beginning to gain recognition in certain contexts.⁶

Courts have interpreted the Fourth Amendment to protect individuals' privacy from unreasonable government intrusion. It limits government activity in a wide variety of contexts, including criminal investigations, routine traffic stops, student searches, and public employee drug screenings. Courts look to societal expectations when determining what sorts of intrusions merit protection under the Fourth Amendment. Yet as social norms adjust to new technologies, the Supreme Court has struggled to place its finger on the emerging social consensus of what the Amendment should protect.⁷ The Court's recent privacy decision, *Ontario v. Quon*,⁸ is a perfect example of this struggle. Although the Court's decision was unanimous, it provides little, if any, guidance or clarity to the already murky legal landscape of the Fourth Amendment.⁹

For decades, scholars have decried the unpredictable and incoherent application of the Fourth Amendment. Many are concerned that the fact sensitive proportional balancing of government interests and individual interests, which the Warren Court announced as the touchstone of the

5. Andrew B. Serwin, *Privacy 3.0—The Principle of Proportionality*, 42 U. MICH. J.L. REFORM 869, 875 (2009).

6. *See id.* at 889 (“Proportionality is . . . consistent with the theoretical underpinning of recent FTC enforcement actions . . .”).

7. *Compare* *Olmstead v. United States*, 277 U.S. 438 (1928) (holding that wiretapped phones do not violate the Fourth Amendment), *with* *Katz v. United States*, 389 U.S. 347 (1967) (overruling *Olmstead*). The telephone's use had grown exponentially in the years leading up to the *Olmstead* decision, but universal telephone use was, by some accounts, not commonplace until as late as the 1940s. CLAUDE S. FISCHER, *AMERICA CALLING: A SOCIAL HISTORY OF THE TELEPHONE TO 1940*, at 182 (1992).

8. *Ontario v. Quon*, 560 U.S. ___, 130 S. Ct. 2619 (2010).

9. *See* *Rehberg v. Paulk*, 611 F.3d 828, 844 (2010) (commenting on *Quon*'s “marked lack of clarity” in privacy expectations of electronic communications); Adam Liptak, *Justices Are Long on Words but Short on Guidance*, N.Y. TIMES, Nov. 18, 2010, at A1 (discussing *Quon*, and noting that “[i]n decisions on questions great and small, the court often provides only limited or ambiguous guidance to lower courts.”).

Fourth Amendment's application, has given way to a results-driven, unpredictable chaos that offers no clear guidance on the metes and bounds of privacy's protection from government intrusion. *Quon* is unlikely to assuage these concerns.

This Note reviews the Fourth Amendment's development and its application to the *Quon* case. It draws on recent privacy scholarship to discuss gaps in the Court's analysis and application of the Fourth Amendment. Part I discusses the Fourth Amendment's historical development, particularly the protection of "privacy" as a concept separate from property in response to increasingly sophisticated communication technologies. Part II discusses and critiques the *Quon* decision. Finally, Part III considers three scholarly perspectives on privacy that enhance an understanding of *Quon*'s gaps and suggests that the Fourth Amendment can and should adopt stronger protection for certain forms of sensitive information.

I. BACKGROUND

This Part begins with a brief description of the Fourth Amendment's application today, particularly in the context of public employees. After laying out the relevant basics of the Fourth Amendment's application, three Sections address aspects of this law in greater detail. These three aspects are: the reasonable expectation of privacy test, the Court's approach for evaluating a search's reasonableness, and the protection of workplace privacy under the Fourth Amendment.

A. BASIC FOURTH AMENDMENT DOCTRINE

Current Fourth Amendment jurisprudence is inexorably linked with the concept of privacy.¹⁰ A Fourth Amendment analysis begins by asking whether the Amendment can be applied to the facts at issue.¹¹ This turns on the reasonable expectation of privacy test: if the complaining individual believes the collected information to be private and "society is prepared to

10. See, e.g., *Katz*, 389 U.S. at 360 (Harlan, J., concurring). The Fourth Amendment explicitly protects "[t]he right of the people to be secure . . . against unreasonable searches and seizures," but does not mention privacy. U.S. CONST. amend. IV.

11. See, e.g., Justin Holbrook, *Communications Privacy in the Military*, 25 BERKELEY TECH. L.J. 831, 835 (2010) ("For purposes of the Fourth Amendment, a 'search' is conducted when the government, acting on its own or through an authorized agent, intrudes into a person's 'constitutionally protected reasonable expectation of privacy.'") (citation omitted).

recognize [this belief] as reasonable,”¹² then the government conduct is characterized as a search and the Fourth Amendment applies.

The next inquiry is into the reasonableness of the search or seizure. A search must be reasonable in both its inception and its scope. In other words, it must have been conducted for a legitimate purpose, and its breadth “must be ‘strictly tied to and justified by’ the circumstances which rendered its initiation permissible.”¹³ The reasonableness of a search can also be influenced by the factors that shape the expectation of privacy in the first place.¹⁴ Although courts frame the reasonable expectation of privacy as a binary question up front—the expectation is either reasonable or it is not—the extent of its reasonableness can limit the Fourth Amendment’s protection of a close case.¹⁵

Fourth Amendment issues regularly emerge from police investigations of criminal activity. In those situations, a warrant supported by probable cause and issued by a judge is often required to deem a search reasonable. However, the Amendment extends beyond police activity and prevents anyone working for the government from conducting unreasonable searches or seizures. Because requiring a warrant in every instance of government information-gathering would create insuperable barriers to conducting government business of all sorts, courts have identified a number of special circumstances in which a warrant is not required.¹⁶

One such case is when a government employer investigates or otherwise collects information about one of its employees. Although the Fourth Amendment still regulates this conduct, public employers are excused from the warrant requirement,¹⁷ and a public employee’s expectation of privacy is typically considered in light of the ‘operational realities’ of the workplace.¹⁸ This means that both the official workplace privacy policies and their actual enforcement in the workplace are given great weight in determining the degree of privacy the employee reasonably could have expected.

12. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

13. *Terry v. Ohio*, 392 U.S. 1, 19 (1968) (quoting *Warden v. Hayden*, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)).

14. *Ontario v. Quon*, 130 S. Ct. 2619, 2631 (2010).

15. *See, e.g., Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 654–60 (1995) (discussing the limitation to a student athlete’s legitimate expectations of privacy and holding that a school’s drug testing policy does not violate the Fourth Amendment).

16. *See, e.g., Nat’l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 665–66 (1989) (applying the special needs doctrine to permit the Customs Service to drug test some of its employees without a warrant or particularized suspicion of any kind).

17. *O’Connor v. Ortega*, 480 U.S. 709, 722 (1987); *id.* at 732 (Scalia, J., concurring).

18. *Id.* at 717; *see also infra* Section I.D.

B. PROPERTY, PRIVACY, AND REASONABLE EXPECTATIONS: WHEN DOES THE FOURTH AMENDMENT APPLY?

When the government directly seizes one's property or person, the Fourth Amendment's applicability is relatively uncontroversial; these cases tend to focus on whether the seizure is reasonable or not.¹⁹ When the government collects information about an individual without seizing their property, the application of the Fourth Amendment becomes less clear. Caselaw plainly establishes that the Fourth Amendment covers cases where the search does not directly violate a property or autonomy interest. This protection of "privacy," as a separate interest from "property" and "autonomy," is easy to articulate, but largely remains an open question. This Section discusses the recognition of a privacy interest protected by the Fourth Amendment and the extent of that protection.

The Fourth Amendment's language emphasizes security from unreasonable searches and seizures in certain realms—"persons, houses, papers, and effects."²⁰ Until the 20th century, the Amendment's contours were largely understood by reference to property law.²¹ Before the 19th century revolution in communication technology, property rights and privacy rights overlapped more than they do today.²² Still, early Fourth Amendment cases did acknowledge that "security" protection meant something different than protection against intrusion into or onto a person's property.²³ Tangible items and other facts—such as conversations²⁴—in one's home were protected from unreasonable collection; what existed in the open was not. In

19. *E.g.*, *Illinois v. McArthur*, 531 U.S. 326, 337 (2001) (holding a search of a man's home reasonable under the Fourth Amendment); *United States v. Place*, 462 U.S. 696, 710 (1983) (holding the seizure and search of a suitcase unreasonable under the Fourth Amendment).

20. U.S. CONST. amend. IV.

21. Tamar R. Gubins, Note, *Warshak v. United States: The Katz for Electronic Communication*, 23 BERKELEY TECH. L.J. 723, 730–31 (2008).

22. *See id.* at 731.

23. *See, e.g.*, *Boyd v. United States*, 116 U.S. 616, 630 ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but . . . the invasion of his indefeasible right of personal security . . ."); *Ex parte Jackson*, 96 U.S. 727, 733 (1877) ("[T]o invade the secrecy of . . . sealed packages in the mail [violates] the great principle embodied in the [F]ourth [A]mendment of the Constitution.").

24. *See* DANIEL J. SOLOVE, MARC ROTENBERG & PAUL M. SCHWARTZ, *PRIVACY, INFORMATION, AND TECHNOLOGY* 64 (2006) ("'Eavesdropping' . . . [means] to 'listen under walls or window . . . to hearken after discourse, and thereupon to frame . . . mischievous tales.' [P]eople could easily avoid eavesdroppers by ensuring that nobody else was around during their conversations.") (quoting WILLIAM BLACKSTONE, *COMMENTARIES* 168 (1769)).

Ex parte Jackson, the Court acknowledged that “the great principle embodied in the [F]ourth [A]mendment”²⁵ protected sealed letters as they traveled through the post office. The packages were not, strictly speaking, the individual’s property any more, but security in one’s sealed packages required this protection.²⁶ While this decision represented a small step outside the bounds of property protection, the “great principle”²⁷ of security in person and property would be developed much further in the twentieth century. As technology pushed the content of private communication (and private life generally) further and further from the traditional confines of well recognized property interests, the need to distinguish property from privacy to achieve the Fourth Amendment’s guarantees became more and more obvious.

In the late 19th century, Warren and Brandeis observed in their article *The Right to Privacy* the importance of more developed privacy protection in the face of advancing technology.²⁸ Their article gave vitality to the concept of privacy that has pervaded ever since.²⁹ The authors identified several ways that new technology, the camera in particular, created new harms that demanded recognition and protection. They concluded that the common law could develop to protect the “inviolable personality” that new technology and social practices were threatening.³⁰ Over the next few decades, their vision of tort protection of “the right to be let alone” was slowly recognized in a variety of circumstances.³¹ Seventy years after Warren and Brandeis’ article, William Prosser organized the disparate cases addressing the right to privacy (described by one federal judge at the time as a “haystack in a hurricane”³²) into four discrete torts: intrusion, public disclosure of private facts, false light publicity, and appropriation.³³ The American Law Institute adopted this

25. *Ex parte Jackson*, 96 U.S. at 733.

26. *Id.*

27. *Id.*

28. Warren & Brandeis, *supra* note 1, 195.

29. See William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383–89 (1960); Serwin, *supra* note 5, at 870–71.

30. Warren & Brandeis, *supra* note 1, at 220.

31. See Prosser, *supra* note 29, at 384–88 (cataloguing state court recognition of a right to privacy in the first half of the 20th century).

32. *Ettore v. Philco Television Broadcasting Corp.*, 229 F.2d 481, 485 (3d Cir. 1956).

33. Prosser, *supra* note 29, at 389. These distinctions eventually made their way into the Second Restatement of Torts, edited by Prosser. RESTATEMENT (SECOND) OF TORTS §§ 652A–652D (1976).

categorization in the *Restatement (Second) of Torts*³⁴ and the courts quickly followed suit.³⁵

It was in the context of privacy's mid-twentieth century common law development that the concept of privacy began to take its central role in the Fourth Amendment.³⁶ Although the Amendment's focus on personal security plainly entailed some conception of "a right to be let alone" from the government, some believed that this right should be limited to the protection of property-based interests.³⁷

The most forceful articulation of this "property approach" to the Fourth Amendment's application can be found in *Olmstead v. United States*.³⁸ There, the Court concluded that wiretapping telephone conversations did not violate the Fourth Amendment, because conversations were transmitted outside the home on wires as public as "the highways along which they are stretched."³⁹ Discussing the Fourth Amendment's scope, the Court reasoned that "[t]he amendment itself shows that the search is to be of material things—the person, the house, his papers, or his effects."⁴⁰ Noting the trend of recent Fourth Amendment cases towards broader application of the Amendment—less tethered to property interests⁴¹—the *Olmstead* majority drew a line in the sand. Because the wiretapping involved no trespass, "[t]here was no

34. *Id.* §§ 652A–652E.

35. *E.g.*, Amy Gajda, *Judging Journalism: The Turn Toward Privacy and Judicial Regulation of the Press*, 97 CALIF. L. REV. 1039, 1050 n.63 (2009).

36. CHRISTOPHER SLOBOGIN, *PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT* 23–24 (2007).

37. *See, e.g.*, *Boyd v. United States*, 116 U.S. 616, 641 (1886) (Miller, J., concurring) ("The searches meant by the constitution were such as led to seizure when the search was successful. . . . [T]he framers of the constitution had their attention drawn . . . to the . . . searching [of] private houses and seizing [of] private papers."). Even in the 19th century, however, the majority in *Boyd* made it clear that the Fourth Amendment protected more than just property. *Id.* at 635 ("[C]onstitutional provisions for the security of person and property should be liberally construed It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.").

38. 277 U.S. 438 (1928), *overruled by* *Katz v. United States*, 389 U.S. 347 (1967); *see also* *United States v. United States District Court*, 407 U.S. 297, 313 (1972) ("Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.").

39. *Olmstead*, 277 U.S. at 465.

40. *Id.* at 464.

41. *Id.* at 458–64; *e.g.*, *Boyd*, 116 U.S. 616, 638 (holding a law requiring the submission of private papers to a court invalid); *Weeks v. United States*, 232 U.S. 383, 398 (1914) (restricting the admission of improperly obtained evidence at court); *Gouled v. United States*, 255 U.S. 298, 313 (1921) (forbidding the admission of papers taken from someone's office where admission to the office was gained under false pretenses).

searching. There was no seizure.”⁴² Because the Fourth Amendment did not apply to this sort of information collecting, the question of its reasonableness was not an issue.⁴³

Writing in dissent, Justice Brandeis argued that the Fourth Amendment was not limited to protection of property interests; it included some protection of the right to privacy he had first written about thirty-eight years earlier.⁴⁴ He noted that, as technology advances, “[s]ubtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.”⁴⁵ Six years after the Court’s ruling in *Olmstead*, Congress passed the Federal Communications Act restricting the Federal Government’s use of wiretapping. Although public sentiment and political discourse against the practice of wiretapping was pervasive in the years after *Olmstead*,⁴⁶ it would be almost forty years before the Supreme Court reversed its decision.

*Katz v. United States*⁴⁷—announcing this reversal—involved an FBI investigation of Frank Katz, who regularly placed illegal bets from a phone booth in Southern California. The FBI secretly recorded Katz’s half of his conversations in the booth. In cases leading up to the *Katz* decision, the Court had parted ways with the narrow trespass doctrine articulated by *Olmstead*, laying a foundation for its explicit embrace of a privacy interest protected by the Fourth Amendment.⁴⁸ The Court held that the secret recording violated Katz’s Fourth Amendment rights. The parties’ arguments focused on whether the phone booth was a private or public place, but the Court reframed the issue: “the Fourth Amendment protects people, not places. . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”⁴⁹ Although the “Fourth Amendment cannot be translated into a general constitutional ‘right

42. *Olmstead*, 277 U.S. at 464.

43. *Id.*

44. *Id.* at 479 (Brandeis, J., dissenting).

45. *Id.* at 473 (Brandeis, J., dissenting).

46. *E.g.*, JEROLD H. ISRAEL & WAYNE R. LAFAVE, CRIMINAL PROCEDURE: CONSTITUTIONAL LIMITATIONS IN A NUTSHELL § 2.2(a) (2006) (“[The] property approach was rejected in *Katz v. U.S.* (1967), in favor of a privacy approach.”).

47. 389 U.S. 347 (1967).

48. *Id.* at 353; *see, e.g.*, *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 304 (1967) (“The premise that property interests control the right of the Government to search and seize has been discredited.”).

49. *Katz*, 389 U.S. at 351.

to privacy,'⁵⁰ it does limit government intrusions on areas that are preserved and recognized as private.⁵¹

Justice Harlan's concurrence offered the most widely repeated articulation of the Court's holding. He stated "that an enclosed telephone booth is an area where . . . a person has a constitutionally protected reasonable expectation of privacy."⁵² More generally, for Fourth Amendment protection to apply "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.'"⁵³ Harlan would later caution against too heavy a reliance on expectations, which "are in large part reflections of" what the law allows,⁵⁴ but the reasonable expectation of privacy test has nevertheless become the unwieldy cornerstone of Fourth Amendment analysis.

More has been written about *Katz* than this Note has the space to summarize.⁵⁵ It has earned recognition as a major development in Fourth Amendment law for its definitive recognition of the privacy approach to the Fourth Amendment rejected in *Olmstead*. Although the language of *Katz* suggests a sweeping change in the Court's understanding of the Fourth Amendment,⁵⁶ by many accounts, this promise has not been met.⁵⁷ *Katz* clarified that privacy rights sometimes extend beyond property rights, but subsequent decisions have also made it clear that privacy can cover less than

50. *Id.* at 350.

51. *Id.* at 351.

52. *Id.* at 361 (Harlan, J., concurring).

53. *Id.*

54. *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

55. See, e.g., Aya Gruber, *Garbage Pail and Puppy Dog Tails: Is That What Katz Is Made Of?*, 41 U.C. DAVIS L. REV. 781 (2008); Christian M. Halliburton, *Letting Katz Out of the Bag: Cognitive Freedom and Fourth Amendment Fidelity*, 59 HASTINGS L.J. 309 (2007); H. Paul Honsinger, *Katz and Dogs: Canine Sniff Inspections and the Fourth Amendment*, 44 LA. L. REV. 1093 (1984); Michael D. Moberly, *Letting Katz Out of the Bag: The Employer's Duty to Accommodate Perceived Disabilities*, 30 ARIZ. ST. L.J. 603 (1998); Ric Simmons, *From Katz to Kyllo: A Blueprint For Adapting The Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303 (2002); David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 MISS. L.J. 143 (2002).

56. Justice Stewart's clerk Laurence Tribe was apparently primarily responsible for the majority opinion. See Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 3 n.14 (2009).

57. E.g., Gruber, *supra* note 55, 784.

what property does. For instance, the open fields doctrine explicitly limits Fourth Amendment protection of undeveloped private property.⁵⁸

Despite these divergences of property and privacy rights, Professor Orin Kerr convincingly observed that the overlap remains substantial.⁵⁹ Where bright line rules regarding expectation of privacy have been developed, they often track property rights.⁶⁰ This is generally true, for example, of privacy in one's dwelling, one's car, and in closed containers.⁶¹ There are, of course, exceptions to this generalization,⁶² but "property law provides a surprisingly accurate guide"⁶³ to courts' assessment of the reasonable expectation of privacy.

More generally, notions of ownership often inform notions of privacy rights. Even where property rights are conceptually distinct from privacy rights, the interests share a vocabulary that belies the conceptual overlap.⁶⁴ After all, we have a right to exclude others from those things and areas of our life that are "ours." The *Quon* case provides a perfect illustration of this. The City paid for the pager at issue in the case, but Quon paid for his accrued overage charges. Although the case did not turn doctrinally on determining ownership of the text messages, the notion of ownership of the messages is in the background of the scholarly and legal discussions of the case.⁶⁵ The allusion to an ownership or property interest of some kind helps

58. See, e.g., *Rakas v. Illinois*, 439 U.S. 128, 144 n.12 (1978) ("[E]ven a property interest in premises may not be sufficient to establish a legitimate expectation of privacy with respect to particular items located on the premises or activity conducted thereon.").

59. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809–15 (2004) [hereinafter *Kerr, Constitutional Myths*].

60. For instance, a homeowner or renter has a reasonable expectation of privacy in his home, but when eviction proceedings are initiated the expectation of privacy is extinguished along with his property rights. *Id.* at 810 (citing *Simpson v. Saroff*, 741 F. Supp. 1073, 1078 (S.D.N.Y. 1990)).

61. *Id.* at 809–13.

62. As discussed *infra* Section I.D, government employee privacy is one such circumstance that Kerr acknowledges has diverged from property law protection. Kerr, *Constitutional Myths*, *supra* note 59 at 815.

63. Kerr, *Constitutional Myths*, *supra* note 59, at 815.

64. *C.f.* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty* 113 YALE L.J. 1151, 1214 (2004) ("What matters in America, over the long run, is liberty against the state within the privacy of one's home."); Daniel Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1112 (2002) [hereinafter Solove, *Conceptualizing*] (discussing the link between property and privacy, and tracing the notion of a property right in information about themselves back to John Locke).

65. For instance, Chief Justice Roberts pressed the City's attorney at Oral Arguments of the *Quon* case about how, if Sergeant Quon paid for the overages, they were in some sense his. Transcript of Oral Argument at 5, *Ontario v. Quon*, 130 S. Ct. 2619 (2010) (No.

courts to this day to articulate the harm entailed in an invasion of privacy. Although this link to property rights is an inescapable—and at times helpful—one, it can limit a court’s ability to appreciate privacy invasions that technology makes possible outside the sphere of property.⁶⁶

C. REASONABLE SEARCHES: HOW DOES THE FOURTH AMENDMENT APPLY?

When an individual does have a reasonable expectation of privacy, that is, when the Fourth Amendment does apply, the reasonableness of the search or seizure is measured in two ways: its purpose and its scope.⁶⁷ Courts have applied these two requirements in a flexible way that permits them to avoid burdening public officials engaged in their duties while still minimizing harm to the public’s interests against arbitrary government intrusion.⁶⁸ Where the Fourth Amendment applies, the government’s interest in conducting the search is balanced against the interest invaded by the search. This balancing considers both the initiation of the search and the need to conduct it in the manner it was conducted.

One of the seminal modern Supreme Court cases discussing the reasonableness of a search is *Terry v. Ohio*. In *Terry*, a police officer stopped and frisked three men whom he had observed behaving suspiciously.⁶⁹ They appeared to be “casing” a store, preparing to rob it.⁷⁰ The officer approached the individuals and after patting them down found two guns on the three men and had them arrested for carrying concealed weapons.⁷¹ The Court held that the Fourth Amendment applied, but that under the circumstances the search was reasonable.⁷²

The *Terry* Court discussed at length the reasonableness of government searches. The basic rubric for reasonableness balances the “need to search (or seize) against the invasion which the search (or seizure) entails.”⁷³ In the criminal context, police conduct is often subject to the Warrant Clause of the Fourth Amendment, which requires a judge to balance these interests and approve of searches supported by probable cause that a crime has been

08–1332) (“Now, can’t you sort of put all [of Quon’s payments] together and say that it would be reasonable for him to assume that private messages were his business?”).

66. *See, e.g.*, *Olmstead v. United States*, 277 U.S. 438, 464–65 (1928).

67. *Terry v. Ohio*, 392 U.S. 1, 19–20 (1968).

68. *See, e.g., id.*

69. *Id.* at 4–7.

70. *Id.* at 6.

71. *Id.* at 7.

72. *Id.* at 30–31.

73. *Id.* at 21 (quoting *Camara v. Municipal Court*, 387 U.S. 523, 536–37 (1967)).

committed and that evidence will be found if the search is allowed.⁷⁴ Where a warrant supported by probable cause is not a realistic option (such as when a police officer must react to an immediately unfolding situation), the same reasonableness requirement still exists.⁷⁵ Reasonableness is not to be confused with good faith; it requires that a reasonable person, with a neutral and objective view of the facts available before the search, would approve of the action.⁷⁶ In *Terry*, the police officer's search was justified by the legitimate concern that the suspicious men would be armed and would therefore pose a threat to his safety—the search was reasonable in inception.⁷⁷ Furthermore, his search was only a pat down of the suspects' outer clothing.⁷⁸ Thus he “confined his search strictly to what was minimally necessary to learn whether the men were armed”—the search was reasonable in scope.⁷⁹

When courts apply the Fourth Amendment outside of the police context, the analysis is somewhat modified.⁸⁰ In *New Jersey v. T.L.O.*, the Court addressed the reasonableness of searching a high school freshman suspected of smoking in the school bathroom.⁸¹ Although the principal was not expected to follow the procedure that a police officer would be compelled to follow, the Court reiterated that the reasonableness of a search is judged by its purpose and scope; both must be found reasonable after balancing the need of the search against the interest being invaded.⁸² Here, the search's purpose at inception needed to be based on “reasonable grounds for suspecting that the search [would] turn up evidence that the student has violated . . . the law or the rules of the school.”⁸³ Similarly, the search's scope would be reasonable so long as the search conducted was “reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student and the nature of the infraction.”⁸⁴ This language emphasizes the unique factors of the school setting that influence the reasonableness of a search.

74. *E.g.*, *Illinois v. Gates*, 462 U.S. 213, 238–39 (1983) (discussing the totality of the circumstances standard for probable cause).

75. *Terry*, 392 U.S. at 21–22.

76. *Id.*

77. *Id.* at 28.

78. *Id.* at 30.

79. *Id.*

80. *New Jersey v. T.L.O.*, 469 U.S. 325, 340 (1985).

81. *Id.* at 328–29.

82. *Id.* at 341–42.

83. *Id.* (internal quotes and citation omitted).

84. *Id.* at 342.

D. GOVERNMENT EMPLOYEE PRIVACY UNDER THE FOURTH AMENDMENT

The Fourth Amendment's application to government employees is similarly tailored to accommodate the workplace setting. The policies and practices of the workplace are given great weight in assessing an employee's reasonable expectation of privacy. Both the purpose and the scope of a search are considered. The Court addressed public workplace privacy in *O'Connor v. Ortega*.⁸⁵ Dr. Magno Ortega, a long time psychiatrist at Napa State Hospital, was suspected of improperly coercing contributions from residents at the hospital to purchase an Apple II computer, and was placed on administrative leave while staff conducted an investigation.⁸⁶ There was no policy permitting an employee's office to be entered or searched without consent.⁸⁷ The hospital staff, however, searched Dr. Ortega's office; taking and reviewing personal correspondence with a former resident, billing documents, and other personal property.⁸⁸ Some of the seized material from his office became evidence against him in his administrative proceedings. The Court, in a 5–4 decision, remanded the case because the trial record did not adequately establish the purpose of the search and other facts relevant to the search's reasonableness.⁸⁹

The *O'Connor* Court produced three opinions discussing the correct application of the Fourth Amendment to government workplaces. Justice O'Connor wrote for a four Justice plurality that a public employee's reasonable expectation of privacy at work is to be considered in light of the "operational realities" of the office environment, taking into account "actual office practices and procedures, or . . . legitimate regulation [of the workplace]."⁹⁰ Where the office's reasonable policies and practices make it clear that an individual cannot expect privacy, the Fourth Amendment (apparently) cannot prevent its invasion.⁹¹ The plurality also held the warrant requirement unduly burdensome for employers and used language very

85. 480 U.S. 709 (1987). It is worth noting that this case's history continued for another eleven years after the Court remanded the case. The Court found that summary judgment was premature given the factual dispute about the purpose of the search. Dr. Ortega eventually prevailed. *Ortega v. O'Connor*, 146 F.3d 1149 (9th Cir. 1998) (affirming a jury award of over \$400,000).

86. *O'Connor*, 480 U.S. at 712.

87. *Id.* at 713.

88. *Id.*

89. *Id.* at 729; *id.* (Scalia, J., concurring).

90. *Id.* at 717.

91. *Id.*

similar to *New Jersey v. T.L.O.* to define the reasonableness of a search.⁹² An employer search is reasonable at inception if the employer had “reasonable grounds for suspecting that the search will turn up evidence that the employee is guilty of work-related misconduct, or that the search [was] necessary for a noninvestigatory work-related purpose such as to retrieve a needed file.”⁹³ An employer search is reasonable in scope where “the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct].”⁹⁴

Justice Scalia concurred in the remand of the case but espoused a different analytic approach.⁹⁵ He agreed with the plurality that the warrant requirement was per se impractical in the employer context (giving this holding the force of law).⁹⁶ However he was harshly critical of the “operational realities” approach taken by Justice O’Connor.⁹⁷ In his view, the accessibility of one’s office should never excuse unreasonable searches.⁹⁸ His approach would essentially forego the preliminary inquiry into the reasonable expectation of privacy, and focus analysis on the reasonableness of the search.⁹⁹ The fact that an employer, and not a police officer, conducts the search has an impact on this stage of Scalia’s analysis. “The government, like any other employer, needs frequent and convenient access to its desks, offices, and file cabinets for work-related purposes.”¹⁰⁰ His view is that “searches of the sort that are regarded as reasonable and normal in the private-employer context . . . do not violate the Fourth Amendment.”¹⁰¹

92. *Id.* at 722–23. Recall that the Court in *T.L.O.* defined a reasonable search as one when there are reasonable grounds for suspecting that the search will turn up evidence that the student has violated or is violating either the law or the rules of the school [and] when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the age and sex of the student . . .

New Jersey v. T.L.O., 469 U.S. 325, 342 (1985).

93. *O’Connor*, 480 U.S. at 726.

94. *Id.* (quoting *T.L.O.*, 469 U.S. at 342) (alterations in original).

95. *Id.* at 729 (Scalia, J., concurring)

96. *Id.* at 732 (Scalia, J., concurring)

97. *Id.* at 730 (Scalia, J., concurring) (“I . . . object to the formulation of a standard so devoid of content that it produces rather than eliminates uncertainty in this field.”).

98. *Id.*

99. *Id.* at 731–32 (Scalia, J., concurring) (“[O]ffices of government employees . . . are covered by Fourth Amendment protections as a general matter. . . . The case turns, therefore, on . . . whether the governmental intrusion was reasonable.”).

100. *Id.* at 732 (Scalia, J., concurring).

101. *Id.*

Finally, Justice Blackmun wrote a lengthy dissent signed by three other justices. This plurality believed that Dr. Ortega's Fourth Amendment rights had been violated and that a probable cause warrant was not unreasonable to require in this case.¹⁰² Therefore, because a warrant was required, but not obtained, Blackmun would have ruled in Dr. Ortega's favor. Setting this point aside, he also strongly objected to the Court's development of a legal standard in a case where important facts remained unsettled. Blackmun, like Scalia, was troubled that the Court had announced a fact sensitive standard absent "sustained consideration of a particular factual situation."¹⁰³ Unlike Scalia, however, Blackmun's concern was that "the standard that emerges makes reasonable almost any workplace search by a public employer"¹⁰⁴ by setting the bar of an employee's expectation of privacy too low. The modern employee's private life necessarily intersects with the workplace in a variety of ways that Blackmun believed the plurality failed to acknowledge.¹⁰⁵ He also strongly objected to the O'Connor plurality's purported balancing of the employer and employee interests in their discussion of the reasonableness of the search. In his view, they failed to appreciate the weight of the employee's interests in protection from invasive and surprising employer searches, and deferred instead to a legitimate, but vague, notion of the employer's need to address and investigate misconduct in an efficient manner.¹⁰⁶ In Blackmun's view, without more specific facts to tether its determination, the Court erred in announcing a general standard for reasonable searches.¹⁰⁷

Thus, the analytic framework for public employer Fourth Amendment claims is not as settled as the tidy accounting suggested *supra* Section I.A.¹⁰⁸

102. *Id.* (Blackmun, J., dissenting).

103. *Id.* at 733 (Blackmun, J., dissenting).

104. *Id.* at 734 (Blackmun, J., dissenting).

105. *Id.* at 740 (Blackmun, J., dissenting) ("[T]he plurality's remark that the 'employee may avoid exposing personal belongings at work by simply leaving them at home,' *ante*, at 725, reveals on the part of the Members of the plurality a certain insensitivity to the 'operational realities of the workplace,' *ante*, at 717, they so value"). Justice Blackmun's point is all the more relevant today. As *Quon's* facts illustrate perfectly, technology continues to blur the line between the workplace and the home. See *Ontario v. Quon*, 130 S. Ct. 2619, 2629–30 (2010) ("The mixed personal and professional use of company-provided devices is an essential tool for transacting business in the information age."); Brief of Elec. Frontier Found. et al. as Amici Curiae in Support of Respondents at 3, *Quon*, 130 S. Ct. 2619 (No. 08–1332), 2010 WL 1063463, at *3.

106. See *O'Connor*, 480 U.S. at 738–40 (Blackmun, J., dissenting).

107. *Id.* at 733 (Blackmun, J., dissenting).

108. When no opinion is supported by a majority of the Court, the holding decided on the narrowest grounds is said to be controlling. *Marks v. United States*, 430 U.S. 188, 193 (1977). Justice Scalia and Orin Kerr have both balked at the task of subjecting this plurality

Still, although a definitive analytic framework for assessing government employer violations of the Fourth Amendment has not been reached by the Supreme Court, many courts—and both parties in the *Quon* case¹⁰⁹—adopt the approach espoused by the *O'Connor* plurality when assessing a public employee's reasonable expectation of privacy.¹¹⁰

As for the standard for reasonable searches of public employees under the Fourth Amendment, the *O'Connor* plurality largely duplicates the standard announced in *T.L.O.* Since *O'Connor*, the Court has followed this approach, emphasizing that the government's interest in conducting searches is to be balanced against an employee's interest in workplace privacy when considering the purpose and scope of the search.¹¹¹ In both *Skinner v. Railway Labor Executives Association*¹¹² and *National Treasury Employees Union v. Von Raab*,¹¹³ the Court upheld drug-screening regulations for railway employees and certain employees of the U.S. Customs Service. Both programs involved government-imposed mandatory submission of blood or urine samples for testing employees.¹¹⁴ The Court agreed with a unanimous body of appellate court opinions that such tests implicated a reasonable expectation of privacy, leaving little to discuss on the application of the Fourth Amendment.¹¹⁵ The cases focused on the reasonableness of these mandatory drug screenings. In *Skinner*, the “risks of injury to others that even a momentary lapse of attention”¹¹⁶ by a railroad employee represent won out against the “limited threats” to employee privacy posed by the tests. Similarly, in *Von Raab*, the Custom Service's important role as “the first line of defense against [drug trafficking,] one of the greatest problems affecting the health and welfare of our population,”¹¹⁷ and the need to “ensur[e] that front-line interdiction personnel are physically fit, and have unimpeachable integrity and

opinion to a *Marks* analysis. *Quon*, 130 S. Ct. at 2634 n. * (2010) (Scalia, J., concurring); Orin Kerr, *Will the Supreme Court Rethink Public Employee Privacy Rights in Quon?*, THE 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/> (“It's somewhat hard to subject the *O'Connor* opinions to a *Marks* analysis. . . . The question makes my head hurt.”).

109. *Quon*, 130 S. Ct. at 2628.

110. E.g., Kerr, *supra* note 108; see also KATHLEEN MCKENNA, PROSKAUER ON PRIVACY § 9:4.2[B] (Kristen J. Mathews, ed. 2010).

111. See *Skinner v. Ry. Labor Executives Ass'n*, 489 U.S. 602 (1989); *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989).

112. 489 U.S. 602.

113. 489 U.S. 656.

114. *Id.* at 660–61; *Skinner*, 489 U.S. at 609.

115. See *Von Raab*, 489 U.S. at 665 (citing *Skinner*, 489 U.S. at 616–18).

116. *Skinner*, 489 U.S. at 628.

117. *Von Raab*, 489 U.S. at 668.

judgment”¹¹⁸ outweighed “the diminished expectation of privacy [drug enforcement officers have] in respect to the intrusions occasioned by a urine test.”¹¹⁹ Both cases placed a strong emphasis on the importance of balancing the public interests against the privacy invasions at issue.

In *Skinner*, the railway employees challenging the tests suggested a number of less intrusive alternatives, including the possibility that impaired employees would be detected without any testing at all.¹²⁰ The Court expressly rejected this approach to challenging the reasonableness of government activity: “We have repeatedly stated, . . . that the reasonableness of any particular government activity does not necessarily or invariably turn on the existence of alternative less intrusive means.”¹²¹ The question was not whether the drug testing was the best balance of government and employee interests, but whether it was a permissible one.

II. ONTARIO V. QUON: FACTS AND COMMENTARY

In addition to summarizing the facts and disposition of the case at the district court, Ninth Circuit, and Supreme Court, this Part includes some critical analysis of the Court’s opinion. The Supreme Court in *Ontario v. Quon* held that the review of the full text of a SWAT officer’s text messages on an employer provided device did not violate the Fourth Amendment because it was reasonable under the circumstances.¹²² This Part will discuss, however, that the unanimous opinion¹²³ fails to articulate why the search at issue was reasonable, skirts the issue of the Fourth Amendment’s application to the facts of the case, and provides little instructive guidance for the disposition of future cases.

A. THE FACTS OF *ONTARIO V. QUON*

In the Fall of 2001, the City of Ontario Police Department (Department) supplied alphanumeric pagers to members of the SWAT—including Sergeant Jeff Quon—to facilitate emergency communication.¹²⁴ Arch Wireless, a company with experience providing mobile communication services to government and corporate clients, provided over one hundred pagers to the

118. *Id.* at 670.

119. *Id.* at 672.

120. *Skinner*, 489 U.S. at 619 n.9.

121. *Id.* (internal quotation marks, brackets and citations omitted).

122. *Ontario v. Quon*, 130 S. Ct. 2619, 2631 (2010).

123. Justice Scalia signed onto all but Part III.A of the opinion. *Id.* at 2634 (Scalia, J., concurring).

124. *Id.* at 2625.

Department.¹²⁵ Eighteen months prior to receiving his pager, Quon signed a statement acknowledging the City's Computer Usage, Internet, and E-Mail Policy that "reserve[d] the [Department's] right to monitor and log all network activity including e-mail and Internet use, with or without notice."¹²⁶ On its face, this policy did not plainly apply to the new pagers.¹²⁷ However, in April of 2002, the Department clarified at a meeting Quon attended that text messages on the Department's pagers were considered email and were not private.¹²⁸

Shortly after receiving the pager, Quon began to exceed his monthly character allowance and incur overage charges.¹²⁹ Lieutenant Duke, the officer responsible for the pager contract, approached Quon about the excess charges.¹³⁰ Duke made it clear that the messages could be audited, but said "it was not his intent to audit" the messages.¹³¹ He said that as long as Quon paid for the overage fees, the messages would not be audited.¹³² Quon agreed to pay the fees. His understanding was that Duke had informally agreed not to review his messages if he paid the overage fees that accrued.¹³³

The overages continued, and Quon continued to pay the fees.¹³⁴ But by August of 2002, Duke told Ontario Police Chief Lloyd Scharf that he had grown "tired of being a bill collector."¹³⁵ He also mentioned the regular

125. Transcript of Deposition of Jackie Deavers at 12, *Quon v. Arch Wireless*, 445 F. Supp. 2d 1116 (C.D. Cal. 2006) (No. EDCV 03-0199 RT(SGLx)), 2004 WL 5389367.

126. *Quon*, 130 S. Ct. at 2625 (citation omitted).

127. *Id.*

128. *Quon*, 445 F. Supp. 2d at 1124.

129. *Id.*

130. *Id.*

131. *Quon*, 130 S. Ct. at 2625. The full story is recounted by the district court: "As Lieutenant Duke explained in his deposition: '[W]hat I told Quon was that he had to pay for his overage, that I did not want to determine if the overage was personal or business unless they wanted me to, because if they said, 'It's all business, I'm not paying for it,' then I would do an audit to confirm that. And I didn't want to get into the bill collecting thing, so he needed to pay for his personal messages so we didn't—pay for the overage so we didn't do the audit.'" *Quon*, 445 F. Supp. 2d at 1125.

132. *Quon*, 445 F. Supp. 2d at 1124.

133. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 897 (9th Cir. 2008).

134. *Quon*, 445 F. Supp. 2d at 1125.

135. The Supreme Court mistakenly reports that this meeting took place in October of 2002. Compare *Quon*, 130 S. Ct. at 2626 ("At a meeting in October . . ."), with *Quon*, 529 F.3d at 897 ("In August 2002 . . . Lieutenant Duke then let it be known . . ."), and *Quon*, 445 F. Supp. 2d at 1125 ("[I]n August, 2002, [Duke] made it known at a meeting with . . . Scharf . . ."), and Transcript of Deposition of Jackie Deavers, *supra* note 125, at 8 (confirming that transcripts were delivered to the department on the 10th of October and that the request occurred sometime around September).

overcharges of two officers, including Quon.¹³⁶ In response, Scharf asked Duke to review the transcripts of messages sent by these two officers for the months of August and September.¹³⁷ Duke requested and received these transcripts from Arch Wireless.¹³⁸ An internal review of the transcripts revealed that in the month of August, about 88% of messages sent or received by Quon while on duty (nearly 400 messages total) were not work related.¹³⁹ These personal messages included explicit sexual conversations with Quon's wife and with his mistress.¹⁴⁰ Quon was then disciplined for misusing his pager because "too much duty time was used for personal pages not associated with duty on duty time."¹⁴¹

As a public employee, Quon and several of the people he had messaged objected to the Department's actions. They brought suit against the City and Police Department for violation of their Fourth Amendment rights to privacy and against Arch Wireless for violation of the Stored Communications Act (SCA).¹⁴² To succeed on the Fourth Amendment claim, they needed to show a reasonable expectation of privacy and that the review of the full text of the messages was an unreasonable search or seizure under the circumstances.¹⁴³

136. *Quon*, 130 S. Ct. at 2626.

137. *Quon*, 445 F. Supp. 2d at 1125–26.

138. *Id.* at 1126.

139. *Quon*, 130 S. Ct. at 2625 (noting that only 57 of 456 messages sent and received on duty in August were work related).

140. *Id.* at 2626.

141. *Quon*, 445 F. Supp. 2d at 1127 (citation omitted).

142. Although this claim is not the focus of this Note, the SCA claim is briefly discussed by the Supreme Court's resolution of the Fourth Amendment Claim. Briefly, the SCA protects certain types of privacy breaches in electronic communications and makes two distinctions relevant to this case. The first is between subscribers and addressees. The second is between electronic communication services (ECS) and remote computing services (RCS). An ECS can lawfully release information to an addressee or intended recipient. 18 U.S.C. § 2702(b)(1), (b)(3) (2006). An RCS can lawfully release information to an addressee, intended recipient, or to a subscriber. *Id.* § 2702(b)(3). In this case, Quon and the other plaintiffs were addressees and the City was a subscriber. Therefore the classification of Arch Wireless as an ECS or RCS would resolve the case. The District Court found that such a classification was not "all or nothing," but that the subscriber exception applied to the retrieval of text transcripts. *Quon*, 445 F. Supp. 2d at 1137. The Ninth Circuit reversed, holding that Arch Wireless was an ECS. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 902 (9th Cir. 2008), *cert. denied*, 130 S.Ct. 1011 (2009).

143. *See supra* Section I.A.

B. THE DISTRICT COURT OPINION

The district court held that Quon had a reasonable expectation of privacy in his text messages.¹⁴⁴ This holding turned on Lieutenant Duke's informal policy of permitting officers to essentially buy back their privacy by paying for overages. Duke's policy of "turning a blind eye" to the Police Department's official privacy policy so long as overage payments were made, "could [even] be said to have *encouraged* employees to use the pagers for personal matters."¹⁴⁵ The court also discussed the Department's ownership of the pager, noting that "[e]xpectations of privacy are not tied up by reference to property law."¹⁴⁶ Here, Duke's policy on the use of the City's equipment canceled out any effect that the City's ownership of the pagers may have had on the analysis.¹⁴⁷

In order to decide the reasonableness of the search, the court administered a jury trial to determine the purpose of the department's audit.¹⁴⁸ If the audit of Quon's texts was "meant to ferret out [his] misconduct," the search was unreasonable given Lieutenant Duke's informal policy permitting (or even encouraging) personal use of the pagers. On the other hand, if the audit was a noninvestigatory effort to determine "the utility or efficacy of the existing monthly character limits" the police department had contracted for, it was reasonable in inception.¹⁴⁹ The plaintiffs argued that the search could still be held unreasonable in scope because less intrusive means of determining the adequacy of the character limits were available, but the court rejected this suggestion because it found their suggestions ineffective given the Department's purpose.¹⁵⁰ The jury's determination as to the purpose of the search would completely resolve the Fourth Amendment claim.¹⁵¹

144. *Quon*, 445 F. Supp. 2d at 1141.

145. *Id.* at 1142 (emphasis in original).

146. *Id.* at 1141 (citing *Katz*, 389 U.S. at 352).

147. *Id.* at 1142.

148. *Id.* at 1144.

149. *Id.*

150. *Id.* at 1145–46 ("[T]he only way to accurately and definitively determine whether . . . the monthly character limits [were adequate] was by looking at the actual text-messages . . .").

151. It is interesting to note that the district court's ruling, although entirely defensible, put the Department in the somewhat paradoxical situation of arguing that the purpose of its searches was for bureaucratic, noninvestigatory, and somewhat unremarkable. In contrast, *Von Raab* and *Skinner* both focused on the vital importance of the searches at issue in order to declare them reasonable. *Skinner v. Ry. Labor Executives Ass'n*, 489 U.S. 602 (1989);

Notwithstanding the court's skepticism to the contrary,¹⁵² the jury determined that the search was undertaken to assess the adequacy of the character limit. The court accordingly ruled that the search was reasonable in its inception and its scope, and entered judgment for the defendants.¹⁵³

C. THE NINTH CIRCUIT OPINION

At the Ninth Circuit, the panel reversed the district court. They agreed that Quon had a reasonable expectation of privacy in his texts and held that, given its noninvestigatory purpose, the search was unreasonable in its scope. In this reversal, the court noted a number of less intrusive alternatives that the police department could have used to determine whether a higher character limit was necessary.¹⁵⁴ When the defendants moved for rehearing en banc, a heated dispute over this bit of analysis erupted between Judge Wardlaw, the author of the panel opinion, and Judge Ikuta.¹⁵⁵

Judge Wardlaw's vigorous concurrence in the denial for rehearing en banc begins, "No poet ever interpreted nature as freely as Judge Ikuta interprets the record on this appeal."¹⁵⁶ Although the disputed points of law and fact are too numerous to catalog here, a key dispute between the two judges centered on whether reviewing the content of Quon's messages was reasonable in scope. Judge Ikuta's dissent asserts that Wardlaw's opinion reasoned that because less intrusive means were available, the search was unreasonable.¹⁵⁷ Wardlaw, however, directly disavows reliance on the "less

Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656 (1989). For further discussion of these cases see *supra* Section I.D.

152. The court expressed its doubt about the purpose of the Department's search: Defendants next argue that the scope of the search was reasonable because . . . "the purpose of the search was simple to determine whether or not the character limit was to be increased, as had been previously done. In order to make such a determination, the messages had to be reviewed to determine what percent were business versus personal." (Defs' Mot. J. Pleadings at 8). While the Court may not find this convincing in light of much of the deposition testimony it has reviewed, the Court does find that, *if* a jury were to find that this was in fact the purpose for the audit, the audit would both be justified at its inception and would be reasonable in its scope.

Quon, 445 F. Supp. 2d at 1145 (emphasis in original).

153. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 899 (9th Cir. 2008) (describing *Quon's* disposition at the district court following the jury trial).

154. *Quon*, 529 F.3d at 909.

155. *See Quon v. Arch Wireless Operating Co.*, 554 F.3d 769 (9th Cir. 2008) (en banc).

156. *Id.* at 769 (Wardlaw, J., concurring).

157. *Id.* at 774 (Ikuta, J., dissenting).

intrusive means test.”¹⁵⁸ This argument would eventually play the dispositive role in the Supreme Court’s decision.¹⁵⁹

The portion of the panel’s opinion purportedly employing the less intrusive means test begins by discussing the district court ruling. “The district court,” Wardlaw noted, “determined that there were no less-intrusive means [and that] the only way to accurately and definitively determine whether [the monthly character limit was sufficiently high] was by looking at the actual text-messages used by the officers who exceeded the character limits.”¹⁶⁰ Responding to the district court’s analysis, Wardlaw continued, “[w]e disagree,”¹⁶¹ and went on to list a number of alternatives:

[T]he Department could have warned Quon that for the month of September he was forbidden from using his pager for personal communications, and that the contents of all of his messages would be reviewed to ensure the pager was used only for work-related purposes during that time frame. Alternatively, if the Department wanted to review past usage, it could have asked Quon to count the characters himself, or asked him to redact personal messages and grant permission to the Department to review the redacted transcript. . . . These are just a few of the ways in which the Department could have conducted a search that was reasonable in scope.¹⁶²

Wardlaw then concluded that “in light of [its] non-investigatory object . . . the search violated [Quon’s] Fourth Amendment rights.”¹⁶³ When pressed by Judge Ikuta’s dissent, Wardlaw vigorously defended her analysis, explaining that “[w]e mentioned other ways the [Department] could have verified the efficacy of the 25,000-character limit merely to illustrate our conclusion that the search was ‘excessively intrusive’ under *O’Connor*, when measured against the purpose of the search as found by the jury.”¹⁶⁴ Wardlaw’s point was that the recitation of less intrusive means in her opinion

158. *Id.* at 772 (Wardlaw, J., concurring).

159. *Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) (explaining that “[t]he Court of Appeals erred” and that “[e]ven 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”).

160. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 908–09 (9th Cir. 2008) (quoting *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1146 (C.D. Cal. 2006)).

161. *Id.* at 909.

162. *Id.*

163. *Id.*

164. *Id.*

was a response to the district opinion, not the basis for her conclusion. The search was excessive because Quon's privacy interest outweighed the Department's interest in determining the suitability of its character limit.

D. THE SUPREME COURT OPINION

The Supreme Court granted certiorari to address three issues: (1) whether the less intrusive means test decried by Judge Ikuta had been applied, (2) whether Quon had a reasonable expectation of privacy in his messages, and (3) whether the individuals Quon was texting with had a reasonable expectation of privacy.¹⁶⁵ There are two noteworthy aspects of the Court's decision. First, with no acknowledgement of Wardlaw's assertion to the contrary, the Court found that the Ninth Circuit had improperly analyzed the reasonableness of the search. The Court determined that reviewing Quon's messages was reasonable under the circumstances.¹⁶⁶ Second, because the audit of Quon's texts was permissible under the Fourth Amendment, the issue of his (and his friend's) reasonable expectation of privacy was not reached. The Court noted that the evolving norms of communication technology, particularly in the workplace, counseled against a premature statement of whether the expectation of privacy in messages like Quon's should receive constitutional protection.¹⁶⁷

1. *Less Intrusive Means*

In its analysis of the Ninth Circuit's ruling, the Court did not mention Judge Wardlaw's explanation in her denial of rehearing en banc concurrence. Quon's brief recites Judge Wardlaw's explanation and sums up the grounds for the Ninth Circuit's conclusion: "Reviewing all of the text-messages is an excessive manner in which to determine if the City needed to increase its character allotment."¹⁶⁸ The Court, however, recited the less intrusive alternatives that Judge Wardlaw's opinion mentioned and summarily concluded that the approach taken by the Ninth Circuit was an inappropriate application of the less intrusive means test, and that the search was reasonable in scope.¹⁶⁹

Where did this leave the requirement that the search be reasonable in scope? The Court was particularly concerned that the post hoc judicial reasoning employed by the less intrusive means test would permit courts to

165. Brief of Petitioners at i, *Ontario v. Quon*, 130 S. Ct. 2619 (2010) (No. 08-1332).

166. *Ontario v. Quon*, 130 S. Ct. 2619, 2632–33 (2010).

167. *Id.* at 2629.

168. Brief of Respondents at 59, *Quon*, 130 S. Ct. 2619 (No. 08-1332).

169. *Quon*, 130 S. Ct. at 2632 (emphasis added).

find any search unreasonable.¹⁷⁰ As the *Quon* Court noted, the *O'Connor* plurality opinion called for an analysis of whether “the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of the circumstances giving rise to the search.”¹⁷¹ It is difficult, however, to imagine such an analysis that does not at least consider what alternative means of achieving the objective were available. Indeed, its own analysis contains dicta of post hoc judicial reasoning of *more* intrusive means that the Department might have reasonably resorted to.¹⁷² During oral arguments, the Justices pressed Quon’s counsel on whether the search was reasonable or not. The discussion quickly became one about the less intrusive alternatives and their adequacy; the Justices seemed unimpressed with the alternatives mentioned, but did not press the point that less intrusive means were inappropriate to consider during the discussion.¹⁷³ It is clear from the Court’s opinion, however, that the availability of less intrusive alternatives does not resolve the matter of a search’s reasonableness.

The Court’s assertion that less intrusive means do not render a search unreasonable does not explain why the government interest underlying the search in *Quon* outweighed Quon’s interest in privacy. Judge Wardlaw and Quon agreed that the availability of alternatives were not decisive. Their belief that the search was not reasonable seems grounded in the intuition that a purpose as bureaucratic, unassuming, and noninvestigatory as confirming character limits ought not to justify the full text review of what were predictably personal text messages. Furthermore, over a hundred pagers were distributed by the City,¹⁷⁴ but only two officers had their transcripts audited. If the character limit were truly inadequate, it seems unlikely that only these two officers would be exceeding their limits. At the risk of providing yet

170. *Id.* at 2632 (quoting *United States v. Martinez-Fuerte*, 428 U.S. 543, 557 n.12 (1976)).

171. *Id.* at 2630 (quoting *O'Connor v. Ortega*, 480 U.S. 709, 725–26 (1987)).

172. *Id.* at 2631 (“OPD requested transcripts for only the months of August and September 2002. While it may have been reasonable for OPD to review transcripts of all the months in which Quon exceeded his allowance . . .”).

173. Transcript of Oral Argument, *supra* note 65, at 35 (Justice Breyer: “I don’t see why these four things are so obviously more reasonable than what they did.”). In defense of Quon’s position, simply clarifying to Quon that future overages would result in automatic review and that extensive personal use would no longer be tolerated (one of the options mentioned by Quon’s counsel) would have spared Duke the role of “bill collector” that he had “grown tired of,” and provided an answer as to whether or not the limit was adequate. This option would have been about as “expedient and efficient” as ordering the transcripts (which took at least a month to be ordered) and would have avoided the violation of the SCA (as found by the Ninth Circuit).

174. Transcript of Deposition of Jackie Deavers, *supra* note 125, at 12.

another less intrusive means of assessing the character limit, some analysis of the number of overage charges throughout the department might have resolved the matter. Further still, Duke's informal policy was predicated on the offer to review the transcripts if the officers insisted that the texts were business related. The fact that Quon had paid the overage fees was essentially an admission that they were not. Thus reviewing the transcripts to determine if the character limit was adequate was unnecessary; Quon would have demanded a review if he felt the limit was inadequate.

Previous Fourth Amendment cases upholding government searches have focused on the important government interest promoted by allowing the search.¹⁷⁵ The *Quon* Court's opinion evinces the concern expressed in *O'Connor* that "government offices could not function if every employment decision became a constitutional matter."¹⁷⁶ The *Quon* Court's analysis, however, is more a repudiation of the less intrusive means test than a lengthy discussion of the important interests promoted by finding this sort of search reasonable. The Court might have, for instance, compared Quon's role as a SWAT officer to the railway employees or Customs agents in *Skinner* and *Von Raab* where the employees' unique role in public safety subjects them to a higher degree of regulation.¹⁷⁷ However, the jury's determination that the search was conducted for a noninvestigatory and administrative purpose limited the significance of Quon's important public role. The competing interests to balance, given the purpose of the search, was the department's need to determine its character limits' adequacy and Quon's (perhaps limited) expectation of privacy, formed on the basis of Duke's arrangement with him.

With this balance in mind, the Court held that "reviewing the transcripts was reasonable because it was an *efficient and expedient* way to determine whether Quon's overages were the result of work-related messaging or personal use."¹⁷⁸ Although previous decisions have mentioned efficiency

175. *See, e.g., Skinner v. Ry. Labor Executives Ass'n*, 489 U.S. 602, 621 (1989) ("This governmental interest in ensuring the safety of the traveling public and of the employees themselves plainly justifies . . . the exercise of supervision to assure that the restrictions [on alcohol and drugs] are in fact observed.") (citation omitted); *Nat'l Treasury Employees Union v. Von Raab*, 489 U.S. 656, 668 (1989) ("[T]he Government's need to discover such latent or hidden conditions . . . is sufficiently compelling to justify the intrusion on privacy . . ."). For further discussion, see *supra* Section I.D.

176. *O'Connor v. Ortega*, 480 U.S. 709, 722 (1987) (quoting *Connick v. Myers*, 461 U.S. 138, 143 (1983)).

177. *See, Skinner*, 489 U.S. at 628; *Von Raab*, 489 U.S. at 671–72.

178. *Ontario v. Quon*, 130 S. Ct. 2619, 2631 (2010) (emphasis added).

concerns,¹⁷⁹ the Court's choice of words suggests that the requirement that a search be reasonable in scope has few, if any, teeth when applied to noninvestigatory searches. At least in the government employer context, most if not all searches that would satisfy the other elements of a Fourth Amendment claim will be both "efficient and expedient."¹⁸⁰ The Fourth Amendment rights of public employees apparently depend primarily on whether their expectation of privacy is reasonable and whether the employer's purpose in searching is reasonable. By chastising the Ninth Circuit's approach at length, the Court limits the chance that future courts will spill much ink discussing a search's reasonableness in scope by considering the alternative means that would fulfill the same purpose.

2. *Reasonable Expectation of Privacy*

The Court avoided a ruling on Quon's reasonable expectation of privacy, holding instead that even if an expectation of privacy did exist, the search was still constitutionally permissible.¹⁸¹ However, this holding was in part predicated upon the Court's qualifications about the extent of Quon's reasonable expectation of privacy.¹⁸² Even assuming the department's official computer privacy policy, public disclosure requirements, and Quon's especially public line of work did not tip the scales against Quon's reasonable expectation of privacy, they still operated as factors minimizing the unreasonableness of the search.¹⁸³

In its opinion, the Ninth Circuit noted the importance of privacy expectations in modern forms of communication,¹⁸⁴ and analogized the case to its recent jurisprudence on emails to find that Quon and the people he sent and received messages with had a reasonable expectation of privacy in

179. *See Von Raab*, 489 U.S. at 665–66. Judge Ikuta's dissent also notes that "[s]even other circuits have . . . explicitly rejected a less intrusive means inquiry." *Quon v. Arch Wireless*, 554 F.3d 769, 778 (9th Cir. 2009) (en banc) (J., Ikuta, dissenting); *e.g.*, *Davenport v. Causey*, 521 F.3d 544, 552 (6th Cir. 2008) ("The Fourth Amendment does not require officers to use the best technique available as long as their method is reasonable under the circumstances.").

180. *Quon*, 130 S. Ct. at 2631.

181. *Id.* at 2624.

182. *Id.* at 2631 ("[T]he extent of an expectation is relevant to assessing whether the search was too intrusive.").

183. *Id.*

184. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904 (9th Cir. 2008) ("The recently minted standard of electronic communication . . . opens a new frontier in Fourth Amendment jurisprudence that has been little explored. . . . Do users of text messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text messages . . . ?").

their messages.¹⁸⁵ The Ninth Circuit agreed with the district court's conclusion that Duke's informal policy gave Quon a reasonable expectation of privacy in his messages.¹⁸⁶ Before the Supreme Court published their opinion, some commentators¹⁸⁷ anticipated the Court would be cautious in determining what reasonable expectation of privacy individuals have in text messages sent on employer-provided devices.¹⁸⁸

Exercising the restraint that some expected, the Court remained officially agnostic on Quon's expectation of privacy. It did offer "instructive" discussion of what would have mattered had it been inclined to rule on the matter and been convinced that the *O'Connor* analysis of the workplace's "operational realities" was the appropriate one.¹⁸⁹ The Court would have needed to weigh Lieutenant Duke's informal policy of collecting overages, his authority to effect a change in policy, and other potential justifications for reviewing the messages.¹⁹⁰ In addition to the particulars of the Police Department's policies and regulations, evolving "workplace norms" with respect to cell phone and text message communication would also shape an employee's privacy expectations.¹⁹¹

3. Justice Scalia's Concurrence

Justice Scalia joined most of the majority opinion, but wrote separately to defend his concurrence in *O'Connor*.¹⁹² He still believes the "operational realities" rubric is "standardless and unsupported."¹⁹³ In his view the Fourth Amendment applies in most cases of public employer work-related searches, but only demands that government employers behave as private employers would be expected to.¹⁹⁴ Scalia also expresses his dissatisfaction with the Court's "instructive" dicta on the relevant factors of the operational realities

185. *Id.* at 906–08.

186. *Id.* at 904.

187. See, e.g., Lyle Denniston, *A Pager as an Open Book*, SCOTUSBLOG (Apr. 19, 2010, 4:02 PM), <http://www.scotusblog.com/?p=18860>. But see David S. Barnhill, Note, *Cloud Computing and Stored Communications: Another Look at Quon v. Arch Wireless*, 25 BERKELEY TECH. L.J. 621, 648 (2010) ("The Supreme Court could also provide more guidance for courts in analyzing privacy for electronic communication in the workplace [when it decides *Quon*].").

188. *Quon*, 130 S. Ct. at 2629–30; see also Brief for Electronic Frontier Foundation, *et al.*, *supra* note 105, at 5.

189. *Quon*, 130 S. Ct. at 2629.

190. *Id.*

191. *Id.* at 2630.

192. *Id.* at 2634 (Scalia, J., concurring).

193. *Id.*

194. *Id.* at 2628, 2634.

test. In addition to being unnecessary to resolve the issues before them, the suggestion that the reasonable expectation of privacy test requires “evaluating whether a given gadget is a ‘necessary instrumen[t] for self-expression, even self-identification [and how] the law’s treatment of [workplace norms has] evolve[d]” is proof positive that the reasonable expectation of privacy test cannot yield objective answers.¹⁹⁵ In his dissatisfaction with the Court’s treatment of the Fourth Amendment, Justice Scalia is not alone.¹⁹⁶

III. ANALYSIS

Privacy is a notoriously amorphous concept. Efforts to define it often begin with a laundry list of complaints about the inherent murkiness of the concept and the range of inconsistent standards and factors that judges use before rules for a particular circumstance are settled.¹⁹⁷ Fourth Amendment jurisprudence is particularly damaged by the vagueness surrounding the concept of privacy. What expectations of privacy society finds reasonable is “the central mystery of Fourth Amendment law.”¹⁹⁸ As Justice Scalia and many others have pointed out, expectations of privacy that society is prepared to consider reasonable “bear an uncanny resemblance to those expectations of privacy that [the Supreme Court] considers reasonable.”¹⁹⁹ *Quon* is only the most recent example of this. The Court has long resisted calls to pin down a single test or formulation to define when and how the Fourth Amendment limits government collection of information. Instead, their approach has been to address the question on a case-by-case basis and permit much of the uncertainty surrounding the Fourth Amendment’s application to persist.

Although caution in the pronouncement of Constitutional protections is appropriate, the Court’s reticence to discuss the Fourth Amendment’s application to new technology is misplaced. This Part reviews three perspectives on privacy protection and the Fourth Amendment that each provide a helpful lens through which to consider the deficits of the Court’s

195. *Id.* at 2635 (Scalia, J., concurring) (quoting the majority).

196. *See, e.g., infra* Sections III.A, III.B.

197. *See, e.g.,* Ruth Gavinson, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 421–22 (1980) (noting scholarly disagreement about the distinctiveness and utility of the concept of privacy); Solove, *Conceptualizing, supra* note 64, at 1088 (“Time and again philosophers, legal theorists, and jurists have lamented the great difficulty in reaching a satisfying conception of privacy.”).

198. Orin Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 504 (2007) [hereinafter Kerr, *Four Models*].

199. *Minnesota v. Carter*, 525 U.S. 83, 97 (1998) (Scalia, J., concurring).

current approach to the Fourth Amendment. The first two authors—Orin Kerr and Daniel Solove—were chosen because they represent two highly regarded and contrasting scholarly views on the application of the Fourth Amendment. The third article, *Privacy 3.0* by Andrew Serwin, places the concept of privacy in a historical context and presents a promising approach to reasonably sorting out the benefits and dangers that new technology presents to private life.

Sections III.A and III.B present the views of Orin Kerr and Daniel Solove, and consider how some of their recent comments on Fourth Amendment jurisprudence apply to the Quon case. A recent article by Kerr organizes the different factors the court draws from when applying the Fourth Amendment. He identifies four models of analysis that courts consider when determining the reasonable expectation of privacy and encourages courts to explicitly acknowledge the use of these distinct approaches. Solove recently published a framework laying out a fundamentally different “pragmatic approach” to Fourth Amendment claims. His approach challenges courts to develop a more comprehensive regulation of government privacy invasion by applying the Fourth Amendment to a broader array of situations than the reasonable expectation of privacy test currently allows for. Section III.C explains how Andrew Serwin’s concept of privacy in the twenty-first century could be drawn on to inform the broader Fourth Amendment privacy protection that Solove calls for. Finally, Section III.D briefly synthesizes and critiques the three authors’ perspectives and discusses how each author’s observations support the conclusion that the Fourth Amendment’s application to information gathering, particularly when it involves new technology, should reflect a proportional protection of information based on its sensitivity.

A. ORRIN KERR’S FOUR MODELS OF FOURTH AMENDMENT ANALYSIS

Scholars widely disparage the unpredictable and inconsistent results the reasonable expectation of privacy test produces, but Orin Kerr takes a different view of Fourth Amendment jurisprudence.²⁰⁰ To him, the array (or disarray) of different approaches to the reasonable expectation of privacy test serves an important purpose. He believes that no single test can adequately distinguish the types of government searches that require Fourth

200. Kerr does acknowledge that the confusion stems from a genuine incoherence in the case law. Kerr, *Four Models*, *supra* note 198, at 505 (“Supreme Court opinions cannot even agree on *what kind of test it is*. . . . The cases are all over the map, and the Justices have declined to resolve the confusion.”).

Amendment scrutiny from those that do not. Rather than pin down one specific and imperfect definition, Kerr believes that the Supreme Court emphasizes certain tests (or models) in different circumstances.²⁰¹ Doing this provides guidance to lower courts about the important factors to consider when deciding to apply the Fourth Amendment without denying courts the flexibility to limit Constitutional protection, especially application of the harsh exclusionary rule, in future cases.²⁰² Kerr argues that application of his four distinct models to Fourth Amendment cases would relieve much of the perceived uncertainty and confusion surrounding the Fourth Amendment.²⁰³

1. *The Four Models*

The first three models that courts draw from to define one's reasonable expectation of privacy use proxies to determine which government practices merit Constitutional regulation.²⁰⁴ They are the probabilistic model, the private facts model, and the positive law model.²⁰⁵ The fourth model addresses the same question directly and is labeled the policy model.²⁰⁶ The probabilistic model is descriptive: it considers the odds that a piece of gathered information would have been revealed in the ordinary course of social practices and norms.²⁰⁷ The private facts model focuses on the character of the collected information rather than the character of the search and determines whether the information is sensitive enough to merit constitutional protection.²⁰⁸ The positive law model considers the legality of the government's information collecting activity. If laws were not broken in the collection of the information, a reasonable expectation of privacy from the information collecting activity does not exist. Government information gathering that violates a law also violates a reasonable expectation of privacy.²⁰⁹ The policy model considers directly whether the information collecting activity in question should be subject to the warrant requirement or not.²¹⁰ The analysis, roughly speaking, looks to balance the threat the activity poses to civil liberties and the burden of regulating the activity on

201. *Id.* at 507.

202. *Id.* at 507, 527.

203. *Id.* at 548–49.

204. *Id.* at 525.

205. *Id.* at 506.

206. *Id.*

207. *Id.* at 508–09.

208. *Id.* at 512–13.

209. *Id.* at 516.

210. *Id.* at 519.

government investigations to determine whether the conduct triggers the Fourth Amendment.²¹¹

Two dichotomies clarify the relationship of these four models to one another. Two of the models focus on normative determinations (private facts and policy), and two focus on descriptive determinations (probabilistic and positive law).²¹² Two of the models focus on what Kerr calls “micro-scale” determinations—determinations based on the particular facts of a case.²¹³ The other two focus on “macro-scale” determinations—determinations based on the courts assessment of a “broader category of cases.”²¹⁴ Kerr summarizes these relations in the table reproduced below:²¹⁵

Table 1: Relationship of the Four Models of Fourth Amendment Analysis

	<i>Micro-Scale</i>	<i>Macro-Scale</i>
<i>Descriptive</i>	Positive Law	Probabilistic
<i>Normative</i>	Private Facts	Policy

These four models are mixed and matched by the courts with little to no acknowledgement of when one model should be used or another discounted.²¹⁶ To make matters worse, the Court will explicitly reject a model in one case, and continue to embrace it in another, again with no acknowledgement of the apparent conflict.²¹⁷ The answer to this mystery, Kerr claims, is that the Court emphasizes or rejects the models in different contexts based on each model’s ability to accurately identify when the Fourth Amendment should apply.²¹⁸ Thus, many of the cases involving new technologies emphasize the private facts model,²¹⁹ many cases involving

211. *Id.*

212. *Id.* at 523.

213. *Id.*

214. *Id.*

215. *Id.* at 524.

216. *Id.* at 524–25 (“[T]he models usually are used as general tools rather than clear and specific doctrinal tests.”).

217. *Id.* at 511, 514, 518, 521–22. Compare, e.g., *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (finding no reasonable expectation of privacy in aerial observation of a fenced backyard given the prevalence of private and commercial flights), with *Illinois v. Caballes*, 543 U.S. 405, 410 (2005) (denying that the probability that police would become aware of drugs in defendant’s trunk during a routine traffic stop had any bearing on his reasonable expectation of privacy), and *United States v. Jacobsen*, 466 U.S. 109, 122 (1984) (“The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.”).

218. Kerr, *Four Models*, *supra* note 198, at 507.

219. *Id.* at 543.

group settings (including government employers) emphasize the probabilistic model,²²⁰ cases relating to physical access or entry to the defendant's property often employ the positive law model,²²¹ and the policy model is most often used when the other models cannot provide a clear or sensible result.²²² Kerr is clear that these models and their emphasis or rejection in different circumstances do not reflect firm (or even conscious) decisions made by the Court. Kerr's point is that these models are emphasized and rejected in somewhat predictable ways, and that greater awareness and clarity about how and when the various models should be applied in the Court's opinions would provide better guidance to lower courts.²²³

2. *The Four Models and Quon*

The *Quon* Court's treatment of the reasonable expectation of privacy test maps well onto Kerr's assessment of the Court's emphasis of certain models in certain contexts.²²⁴ In the government employer context, the probabilistic model is largely embodied by the *O'Connor* plurality's "operational realities" inquiry. The operational realities "test" applies the social norms that the probabilistic model looks to in the specific context of the workplace, looking to "actual office practices and procedures, or . . . legitimate regulation."²²⁵ The Court's "instructive"²²⁶ dicta on *Quon*'s reasonable expectation of privacy begin with this version of the probabilistic model, looking towards a descriptive assessment of the odds that *Quon*'s messages would be viewed. Here, this probability can be assessed by considering whether Lieutenant "Duke's statements could be taken as announcing a change in OPD policy, [and] whether a review of messages sent on police pagers . . . might be justified for other reasons, including performance evaluations, litigation concerning the lawfulness of police actions, and perhaps compliance with state open records laws."²²⁷ The factors mentioned by the Court increase the probability that the text messages *Quon* sent would be reviewed at some point. However, the Court fails to mention one factor that arguably decreases this probability: the police did not have direct access to the transcripts. The transcripts were not stored on city equipment; the request to retrieve them

220. *Id.* at 544.

221. *Id.*

222. *Id.* at 545.

223. *Id.* at 548.

224. *Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010).

225. *O'Connor v. Ortega*, 480 U.S. 709, 717 (1987).

226. *Quon*, 130 S. Ct. at 2629.

227. *Id.*

took over a month to complete and was eventually found to violate the SCA.²²⁸

As Kerr's article predicts, the Court also gives a nod to the private facts model when discussing new communication technology. "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."²²⁹ Because it is not yet clear "what society considers proper behavior"²³⁰ with respect to employer-provided texting devices, the Court admits that it "would have difficulty predicting . . . the degree to which society will be prepared to recognize those expectations as reasonable."²³¹ In other words, a reasonable expectation of privacy analysis in this case would require a determination of how private (or sensitive) the text messages sent on an employer-provided pager were. The difficult question of how private this form of information should be is precisely what Serwin aims to address in his ongoing project to separate different types of information into four tiers of sensitivity.²³²

Consideration of the Stored Communication Act (SCA) is conspicuously absent from the factors the Court points to in deciding Quon's expectation of privacy.²³³ The Ninth Circuit found that Arch Wireless violated the SCA in turning over the transcripts of Quon's texts.²³⁴ Further, in his brief, Quon argued that the undisturbed finding that Arch Wireless violated the SCA

228. *Id.* at 2626.

229. *Id.* at 2629. Kerr has called for this sort of caution in the past, arguing that legislative protection of privacy with respect to new technology is preferable. Kerr, *Constitutional Myths*, *supra* note 59, at 808 ("Courts should recognize their institutional limitations and remain cautious until the relevant technology and its applications stabilize."). Daniel Solove's responds directly to Kerr's call, claiming that "[t]he courts have taken too narrow a view of the Fourth Amendment with regard to many issues . . ." Daniel Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 *FORDHAM L. REV.* 747, 774 (2005) [hereinafter Solove, *Fourth Amendment Codification*]. Forcing courts into "[d]iscussions about whether certain new technologies fit into the labyrinthine framework of electronic surveillance [statutes misses the point.] Principles should guide technology, not vice versa." *Id.* at 773.

230. *Quon*, 130 S. Ct. at 2629.

231. *Id.* at 2630.

232. Andrew Serwin, *Privacy 3.0 Survey*, PRIVACY & SECURITY SOURCE (Oct. 5, 2010), <http://www.privacysecuritysource.com/privacy-30-survey/> ("The next step in the work is to define the types of data that fall into each category . . ."); *see also infra* Section III.C.

233. The SCA is only discussed in regards to the reasonableness of the search. *See Quon*, 130 S. Ct. at 2632.

234. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900–03 (9th Cir. 2008), *cert. denied*, 130 S. Ct. 1011 (2009).

weighed in favor of his reasonable expectation of privacy.²³⁵ The City responded that, in addition to being wrong, the Ninth Circuit's determination that federal law was violated cannot establish an expectation of privacy where the violation "depends on the application of complex statutory provisions that the employee and those sending messages to the employee did not even know and could not control."²³⁶ Furthermore, regardless of the purported violation of the SCA, the Department could also have reclaimed its pager and viewed the messages stored on the device's memory.²³⁷ Still, the Court's decision to forego discussion of the SCA's bearing on a reasonable expectation of privacy illustrates Kerr's point that certain factors or models, in this case the positive law model, are often ignored by the Court in unpredictable ways. The fact that both sides spend several pages of their briefs discussing the SCA and other laws regulating the use of Quon's messages²³⁸ reflects the uncertainty as to what models the Court will ultimately hang their decision on.

Kerr's four model description of Fourth Amendment jurisprudence provides a helpful framework for *Quon's* discussion of the reasonable expectation of privacy. It also appears to be a promisingly accurate categorization of the puzzling landscape of Fourth Amendment cases. His analysis skillfully brings a semblance of order to the chaos of the Court's doctrine, and his proposal—an acknowledgement of the four models and explanation of when each is appropriate—is a more modest retooling of Fourth Amendment doctrine than Solove's proposal.

B. DANIEL SOLOVE'S PRAGMATIC APPROACH TO THE FOURTH AMENDMENT

Solove's most recent article on the Fourth Amendment argues that the reasonable expectation of privacy test should be discarded altogether in favor of a more practical approach. For years, Solove has been a strong voice in the chorus of derision that the Fourth Amendment receives from the legal academy.²³⁹ In the past, he critiqued the Court for often having the wrong

235. Brief of Respondents, *supra* note 168, at 48–49. Quon also mentioned state-based privacy protections that were violated by the Department's actions. *Id.* at 49 n.8.

236. Reply Brief of Petitioners at 14, *Quon*, 130 S. Ct. 2619 (No. 08–1332).

237. See Brief for the United States as Amicus Curiae Supporting Reversal at 29, *Quon*, 130 S. Ct. 2619 (No. 08–1332), 2010 WL 565206, at *29.

238. See Brief of Respondents, *supra* note 168, at 42–50; Brief of Petitioners, *supra* note 165, at 35–45.

239. See, e.g., Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002); Solove, *Fourth Amendment Codification*, *supra* 229;

answers when it came to assessing the reasonable expectation of privacy.²⁴⁰ Now, Solove criticizes the Court for asking the wrong questions all along.²⁴¹ Rather than focus on the unwieldy reasonable expectation of privacy, “courts should directly address how to regulate government information gathering” in the most sensible way.²⁴²

1. *Solove’s Proposal*

At a basic level, Solove identifies two questions in any Fourth Amendment claim. The first is whether the Fourth Amendment applies to the government activity at issue.²⁴³ The second is how the Fourth Amendment restricts the government activity at issue.²⁴⁴ The current Fourth Amendment approach is dominated by the first basic question,²⁴⁵ what Solove terms the “coverage question,” in the form of the reasonable expectation of privacy test.²⁴⁶ Instead of conditioning Fourth Amendment protection on the “unstable”²⁴⁷ theory of an “objective” expectation of privacy, the Fourth Amendment should regulate any “government information gathering activity [that] creates problems of reasonable significance”²⁴⁸ Accordingly, Solove believes that the second question, or the “procedure question,” should be the central question addressed by courts considering a Fourth Amendment claim.²⁴⁹

Solove takes issue with the reasonable expectation of privacy test on two grounds. First, he argues that the test purports some empirical measure of “what society is prepared to recognize” while, in reality, it is plain that it is the intuitions of the judges deciding a case, and analogies to prior cases, that

Daniel J. Solove, *“I’ve Got Nothing to Hide” and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

240. Daniel Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1512 (2010) [hereinafter Solove, *Fourth Amendment Pragmatism*]; see also Solove, *Fourth Amendment Codification*, *supra* 229, at 773.

241. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1512.

242. *Id.* at 1515. In one sense, Solove’s proposal is to use what Kerr calls the Policy model to decide not just *if* but *how* the Fourth Amendment applies.

243. *Id.* at 1514.

244. *Id.*

245. Even *Quon*, which doctrinally turned on the second question (the reasonableness of the search) was dominated by consideration of Quon’s reasonable expectation of privacy and its limits.

246. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1514.

247. *Id.* at 1512 (quoting Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002)).

248. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1514.

249. *Id.*

guide the analysis.²⁵⁰ Solove finds that troubling enough, but an accurate measure of society's privacy expectations is quite elusive.²⁵¹ Resorting to surveys of public opinion would be equally problematic. Although surveys suggest that public intuitions about privacy differ markedly from the Court's doctrine,²⁵² data on people's actual behavior suggests that they are often "willing to trade privacy for convenience" ²⁵³ Even behavioral data is a limited measure of people's preferences, as "[p]eople often fail to understand the implications of their behavior."²⁵⁴

The second flaw Solove identifies offers an even more focused critique of the current framework: "[l]ooking at expectations is the wrong inquiry."²⁵⁵ The law of privacy, Solove argues, should shape expectations, not vice versa.²⁵⁶ Employers, police officers, litigants, and the general public look to statements of the Court when forming their expectations on privacy.²⁵⁷ If the Court were more consistent and clear about the protection of privacy and its limits in our society, both the searchers and the searched would benefit. The general public would benefit from a clearer understanding of what privacy they could expect. Government officials conducting various types of searches would also have a better sense of the limits of permissible searching and how

250. *Id.* at 1521.

251. *Id.* at 1522–23. The *Quon* court certainly acknowledged as much. *Ontario v. Quon*, 130 S. Ct. 2619, 2629 (2010) ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

252. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1522; Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at 'Understandings Recognized and Permitted by Society'*, 42 DUKE L.J. 727, 774 (1993) (discussing data that "would suggest the Supreme Court's conclusions about the scope of the Fourth Amendment are often not in tune with commonly held attitudes about police investigative techniques").

253. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1522 (quoting Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality: A Survey*, in *PRIVACY AND TECHNOLOGIES OF IDENTITY: A CROSS-DISCIPLINARY CONVERSATION* 15, 16 (Katherine J. Strandburg & Daniela Stan Raicu eds., 2006)).

254. *Id.* at 1523.

255. *Id.* at 1524.

256. *Cf.* *United States v. White*, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumption of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.").

257. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1524; *see also* Andrew Serwin, *Quon v. Arch Wireless—A Partial Answer*, SAN DIEGO SOURCE (June 22, 2010), http://www.sddt.com/commentary/article.cfm?sourcecode=20100622tb&commentary_id=136# (drawing inferences from the *Quon* decision about best practices for employer monitoring of electronic communication).

to frame privacy policies that respected these limits. Without clarity on the meaning and scope of privacy protection, expectations of privacy tend to erode.²⁵⁸ Solove's indictment of the expectation of privacy test is convincing, yet his alternative path forward is less clear.

Solove's answer to the "procedure" question—the question of *how* the Fourth Amendment should apply—is related to Kerr's characterization of the policy model.²⁵⁹ For Kerr, the policy model asks *if* the Fourth Amendment should regulate a certain set of investigative practices.²⁶⁰ Solove's approach adds consideration of *how* the regulation should operate. Kerr finds the policy model inadequate because lower courts will inject too much uncertainty into the policy model's application.²⁶¹ Solove responds that the current test, if it can be called a test, is similarly unstable and that many areas of law require a difficult balancing of interests.²⁶² Kerr would prefer to let Congress provide more specific privacy protections where the Fourth Amendment's protections are found lacking.²⁶³ Solove believes that courts are equipped to balance these interests in an appropriate and consistent manner. Solove argues that deferring to congressional action or the lack thereof is inadequate to protect privacy in the context of rapidly evolving technology.²⁶⁴

Solove asserts that, as a practical matter, the Fourth Amendment operates as "the central regulatory system for government information gathering."²⁶⁵ Analytic gamesmanship over a one-size-fits-all statement about where the Fourth Amendment applies—the reasonable expectation of privacy—or what enforcement mechanisms should be used—often the relatively severe exclusionary rule—has pushed the Court to carve up the application of Fourth Amendment in incoherent and unhelpful ways.

258. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1525; *see also* United States v. Pineda-Moreno, 617 F.3d 1120, 1126–27 (9th Cir. 2010) (Reinhardt, J., dissenting) (listing cases that "gradually but deliberately reduced the protections of the Fourth Amendment").

259. Compare Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1514 ("How should the Fourth Amendment regulate this form of government information gathering?"), with Kerr, *Four Models*, *supra* note 198, at 519 ("[S]hould a particular set of police practices be regulated by the warrant requirement?"). Of course, Kerr's policy model is still couched in the coverage question of whether or not the Fourth Amendment applies at all. Still, the similarities are noted by Solove. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1534.

260. Kerr, *Four Models*, *supra* note 198, at 519.

261. *Id.* at 536.

262. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1534.

263. Kerr, *Constitutional Myths*, *supra* note 59, at 858–59.

264. Solove, *Fourth Amendment Codification*, *supra* 229, at 747–48.

265. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1529.

Although the Fourth Amendment can certainly be used as a guide to evaluate statutes, Solove believes that courts and policy makers must often develop rules where no statute exists.²⁶⁶

Solove acknowledges the concern that this approach requires courts to usurp the legislative role of Congress by enshrining whatever the Court's preferred rules are in the single sentence of the Fourth Amendment.²⁶⁷ Where the legislature has spoken, the Court's only role is to review "whether [the statutes] meets the basic principles of the Fourth Amendment."²⁶⁸ He also notes that, in reality, Congress has not made the active regulation of government information gathering a priority.²⁶⁹ Where Courts do create their own rules—filling gaps that the statutes have not addressed—the legislatures would still have some latitude to step in and pass regulations clarifying the specifics of what forms of government information gathering are reasonable. Only patently unreasonable statutes, which violated the basic principles enshrined in the Fourth Amendment, would be the rightful targets of Constitutional objection.

2. *Application of Solove's Proposal to Quon*

How might Solove's pragmatic approach apply to *Quon*? Solove plainly states that he wants to expand the scope of the Fourth Amendment (and increase the flexibility of its enforcement mechanisms). "The Fourth Amendment," Solove writes, "should regulate government information gathering whenever it causes problems of reasonable significance."²⁷⁰ These problems, such as government invasions of privacy, and inhibition of free speech and association "are of a constitutional magnitude, for they are fundamental to the scope of the government's power . . ."²⁷¹ Although the constitutional magnitude of the *Quon* facts is, perhaps, less compelling than

266. Kerr argues that, with respect to new technologies, statutes are better suited to fill gaps when it remains unclear what the Fourth Amendment does and does not cover. Kerr, *Constitutional Myths*, *supra* note 59, at 869 ("The technologies exist, . . . [b]ut no one really knows how the Fourth Amendment applies to them.").

267. Similar concerns were mentioned by the Solicitor General during the *Quon* oral argument, and Justice Roberts responded by wondering whether "more flexib[ility] in determining what is reasonable because we are dealing with evolving technology" is appropriate. Transcript of Oral Argument, *supra* note 65, at 22–23. As noted above, Kerr and Solove have debated whether courts or legislators are better suited to set rules regarding privacy. See Kerr, *Constitutional Myths*, *supra* note 59; Solove, *Fourth Amendment Codification*, *supra* note 229.

268. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1537.

269. *Id.* at 1536.

270. *Id.* at 1528.

271. *Id.*

some more heavy handed exercises of state power, the search does raise problems of reasonable significance.

The increasingly blurred line between the workplace and the home, noted in Justice Blackmun's dissent in *O'Connor*, illustrates why the employee privacy at issue in *Quon* is a "problem[] of reasonable significance"²⁷² that the Fourth Amendment should cover. The Department required Quon to carry his pager with him at all times and had an informal policy that allowed him to use it for private communications.²⁷³ Although they could have insisted that it be used only for business, they did not.²⁷⁴ The review of Quon's messages resulted in the release of particularly private content, which was completely foreseeable given Quon's willingness to pay for the messages to remain private.²⁷⁵ The Department's somewhat dubious need to confirm the adequacy of their character limit, as found by the jury, does little to balance out this foreseeable revelation of Quon's personal information.

The procedure question asks how the Fourth Amendment should regulate the information gathering activity at issue.²⁷⁶ Although the current Fourth Amendment framework is a fact sensitive inquiry, it is essentially a series of yes-or-no questions: is there a reasonable expectation of privacy? Is a warrant required? Solove thinks a more flexible approach would result in a more balanced application of the Fourth Amendment's protections. Solove provides several questions that the court might consider in addressing the matter: "Is this information gathering activity one that government should perform frequently? Rarely? Early on in an investigation? Only as a last resort? In particular cases involving only those suspected of crimes? En masse to the entire population?"²⁷⁷ Auditing the full text of employee messages is an inappropriate way to determine the adequacy of word limits for the employer's devices. Certainly employers require the authority to monitor their employees, and to set a low bar for their expectation for privacy at work and on work equipment, but where they have not plainly done so, the employee's privacy interest in their communications outweighs the non-investigatory purpose that the Department argued had driven the audit. Using Solove's more flexible approach, the Court could push future

272. *Id.*

273. *Ontario v. Quon*, 130 S. Ct. 2619, 2625 (2010).

274. *Id.*

275. *Id.* at 2626; *cf.* *Katz v. United States*, 389 U.S. 347, 351 (1967) ("[W]hat [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

276. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1514.

277. *Id.* at 1529.

public employers to set and enforce clearer guidance about the use of communication equipment and to limit the review of personal messages where possible.

The parties' treatment of the various public disclosure laws, state privacy laws, and the SCA in the *Quon* case are another good example of how Solove's approach could alter the analysis. In the briefs and at oral argument,²⁷⁸ the City argued that the SCA was too complex and technical a statute to have any bearing on Quon's expectation of privacy. His ignorance of the SCA and of how a court would apply it, they argued, negated any influence it might have on his privacy expectation.²⁷⁹ Under Solove's pragmatic approach, Quon's lack of understanding of these laws and their effect on his expectations would be irrelevant; the laws would be instructive indications that people desired a certain type of information gathering activity to be regulated in certain ways.

Another insight Solove offers in his somewhat brief discussion of the tough procedure question is that clearer regulation and oversight can avoid many of the problems created by information gathering in the first place. "[O]versight and regulation can . . . minimize many problems created by [a form of information] gathering" by clarifying expectations for the potential searchers and those that will be subject to their searches.²⁸⁰ In the *Quon* case, it is plain enough that whatever the purpose or motivation of the search, concern for Quon's privacy did not enter Lieutenant Duke or Chief Scharff's mind.²⁸¹

With a clearer statement from the Court about the propriety of such searches, similar circumstances in the future could likely be avoided. Employers are free to shape the privacy expectations of their employees in reasonable ways. There is no doubt that Quon's text messages were not off limits for review under any circumstance. The point for the Ninth Circuit and for Solove is that Scharff and Duke should have appreciated Quon's privacy interest in a way they did not. For instance, if Duke was "tired of being a bill collector" he could simply choose to end his informal practice of allowing officers to go over the limit and pay him the extra fee. If the motivation was in fact directed at seeing what Quon had been up to while on

278. Transcript of Oral Argument, *supra* note 65, at 17; Reply Brief for the Petitioners, *supra* note 236, at 9.

279. When pressed, Quon's attorney made a similar argument with respect to the California Public Records Act. Transcript of Oral Argument, *supra* note 65, at 45.

280. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 1530.

281. See *Quon v. Arch Wireless*, 445 F. Supp. 2d 1116, 1126 (C.D. Cal. 2006).

duty, a simple clarification that he was to refrain from excessive pager use, especially while on duty, would have put Quon on notice that he should stop or limit his texting.

C. ANDREW SERWIN'S PRIVACY 3.0

In *Privacy 3.0*, Andrew Serwin traces the development of privacy theory over the last century and argues that a new framework to understand the significance of privacy is necessary. Privacy 1.0 is embodied in Warren and Brandeis' seminal *The Right to Privacy*—"the right to be let alone."²⁸² Privacy 2.0 is marked by Prosser's organization of the common law development of privacy protection into four distinct torts: intrusion, public disclosure of private facts, false light publicity, and appropriation.²⁸³ Serwin argues that this twentieth century understanding of privacy, as a right of protection against a particular form of harm, is ill suited to address the privacy issues of today.²⁸⁴

Instead, privacy is best understood today through the principle of proportionality. This principle aims to strike a balance between the costs and benefits of different types of information being disseminated. As Serwin explains, proportionality "places higher restrictions and access barriers on truly sensitive information that . . . has great capacity to damage individuals and society, while simultaneously permitting . . . access to those having a legitimate need to know certain information, particularly when that information is less sensitive."²⁸⁵

1. *The Principle of Proportionality*

Serwin proposes four tiers of information sensitivity to guide analysis of privacy protection. The tiers are (1) highly sensitive information,²⁸⁶ (2) sensitive information,²⁸⁷ (3) slightly sensitive information,²⁸⁸ and (4) non-

282. Warren & Brandeis, *supra* note 1.

283. Serwin, *supra* note 5, at 882–83; Prosser, *supra* note 29.

284. Serwin, *supra* note 5, 878–79.

285. *Id.* at 876.

286. As explained below, precise determinations regarding what kinds of information belong in what tier of sensitivity are based on a number of factors. Serwin still provides several examples of what would likely be considered highly sensitive information including, e.g., genetic information, sexual history, religious affiliation, images or video of conduct in private areas. *Id.* at 902–03.

287. *E.g.*, "content of wire or electronic communication, video rental and television programming preferences, financial information, consumer's purchasing preferences, Social Security numbers." *Id.* at 904.

288. *E.g.*, "connection records from telephone companies or ISPs (but not the content of the communication), financial information regarding consumer debts, information

sensitive information.²⁸⁹ Several factors guide the classification of information into each of these tiers. These factors include how much the information reveals what would otherwise be unknown, the societal and personal impact of disclosure, the utility of sharing the information, the risks of unauthorized access posed by limited authorized sharing of the information, whether the information can lead to access to other types of information, and the steps taken to protect the privacy of the information.²⁹⁰

Serwin's discussion is directed at privacy protection in the private sector, but his insights into the past and future of privacy's place in our legal and social institutions provides a helpful perspective.²⁹¹ Further, although Serwin does not discuss the Fourth Amendment directly, many Fourth Amendment scholars share Serwin's concern that information privacy is often lost in the judicial shuffle of one's reasonable expectation of privacy. For example, as noted in Section III.B.1, *supra*, Solove believes that people's desire for protection from government information gathering—not privacy expectations—should inform the application of the Fourth Amendment. Although he does not use Serwin's vocabulary, the answer Solove identifies is very similar to the principle of proportionality.²⁹²

Serwin's discussion of privacy as proportionality goes directly to the heart of what sort of privacy protection "society is [or should be] prepared to recognize as reasonable."²⁹³ The privacy interest protected by the Fourth Amendment—recognized in *Katz* and puzzled over ever since—could incorporate Serwin's discussion of proportionality. That is, the sensitivity of the type of information being gathered, shared, or considered for protection

disclosed on an employer's computer network, images captured in a public space, addresses of websites visited, IP addresses, To/From addresses from emails." *Id.* at 905.

289. *E.g.*, "a person's name, email address, telephone number, and address." *Id.* at 905–06.

290. *Id.* at 901 (explaining these factors and arguing that sorting information into tiers of sensitivity will provide greater clarity for the application of and adherence to existing law).

291. Also, although the Fourth Amendment does not apply to private employers, Serwin notes elsewhere that "many [private] employee privacy issues still devolve into an examination of whether the employee had a reasonable expectation of privacy . . . similar to that under the Fourth Amendment." ANDREW B. SERWIN, INFORMATION SECURITY AND PRIVACY: A PRACTICAL GUIDE TO FEDERAL, STATE AND INTERNATIONAL LAW § 15:1 (2008).

292. Solove, *Fourth Amendment Pragmatism*, *supra* note 240, at 19–20 ("We must assess the value of the information gathering activity and consider it in light of the importance of ameliorating the problems it causes.").

293. *Katz v. United States*, 389 U.S. 347, 361 (Harlan, J., concurring).

should play a more prominent role in assessing the reasonableness of a search under the Fourth Amendment.²⁹⁴

2. Privacy 3.0 and Quon

Quon plainly represents a close case; there is room to argue whether the information collected was sensitive or slightly sensitive based on Serwin's discussion of these two tiers. Sensitive information, or Tier II information, includes "the content of wire or electronic communications"²⁹⁵ and would be subject to more rigorous collection, retention, and use restrictions. If Quon's texts qualify as Tier II information, the Department's actions with respect to that information become subject to more scrutiny.²⁹⁶ Slightly sensitive information, or Tier III information, would include "information disclosed on an employer's computer network"²⁹⁷ and could typically be "gathered without consent or notice."²⁹⁸ If Quon's texts were Tier III information because of the employer privacy policy, the Department is probably acting reasonably by reviewing his transcripts. The debate would still center on the effect of Duke's informal practice of letting officers pay their overages, but the issue would be focused on whether the invasion of Quon's privacy was, on balance, appropriate or not.

D. COMPARING THE THREE APPROACHES: THE FUTURE OF PRIVACY AND THE FOURTH AMENDMENT

Elements from each of the perspectives reviewed contribute to the conclusion that the Fourth Amendment should develop to protect against searches of sensitive information in a more predictable and consistent manner. As Kerr observes, the sensitivity of information (i.e., the private facts model) is already sometimes, but not always, used to determine reasonable expectations of privacy.²⁹⁹ Solove argues that the Fourth Amendment's focus on privacy expectations should be abandoned for a more flexible approach.³⁰⁰ Finally, Serwin believes that an emerging principle of proportionality will (and should) guide the concept of modern information

294. The danger of hindsight playing too prominent a role in the analysis of information's sensitivity is real. One response, however, is that Serwin's tiers of sensitivity focus on gauging the sensitivity of broader categories of information (e.g., electronic communication), not particular instances of information.

295. Serwin, *supra* note 5, at 904.

296. *Id.*

297. *Id.* at 905.

298. *Id.*

299. *See supra* Section III.A.1.

300. *See supra* Section III.B.1.

privacy: identifying categories of more sensitive information and providing them with greater protection.³⁰¹

While Kerr encourages the Court to make privacy jurisprudence more systematic by being more explicit in choosing amongst the analytic models it already uses, he understates the normative failings of the law's current "structure." The problem with the expectation of privacy test is not simply that courts look to an unpredictable array of factors when considering it. The problem is that judges applying it to particular cases often craft rules narrowing privacy protection where it should be protected. More importantly, while social expectations certainly operate to shape the law, the law also can operate to shape societal expectations. Solove believes that courts should take a more active role in shaping society's expectations.

Solove's promotion of a more pragmatic Fourth Amendment is light on specific details about application, but presents an intriguing perspective on the failures of focusing on reasonable expectations of privacy. Though the two are importantly linked, Solove argues that expectations of privacy should not be conflated with actual privacy. That is, perfunctory notices that privacy is not to be expected in the public workplace should not thwart one's desire for reasonable protection against government invasion. Instead of focusing on "reasonable expectations," privacy protection should focus on setting expectations by identifying and limiting access to information society values as sensitive. Serwin's *Privacy 3.0* explores an understanding of privacy modeled on these values.

Serwin's tiers of privacy protection would not instantly provide clear rules with which to apply the Fourth Amendment, but they can focus and improve our vocabulary of privacy. Debate about the sensitivity of information, and the protection afforded to certain types of information would, generally, be much clearer than the current muddle of reasonable privacy expectations. With an improved vocabulary comes a stronger appreciation for the importance of privacy protection. As Solove recently observed, "Privacy is a concept in disarray. . . . [A]bstract incantations of the importance of 'privacy' do not fare well when pitted against more concretely stated countervailing interests."³⁰² The current disarray in privacy is disruptive because it limits agreement on acceptable behavior when it comes to collecting information. The appreciation for what type of information is sensitive moves the conversation past whether a particular incident created a

301. See *supra* Section III.C.1.

302. Daniel Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 477-78 (2006).

particular harm and on to the point that the value of privacy protection goes beyond recourse for the harm of an invasion. A focus on protecting sensitive information from unreasonable search, and not on whether the search upset privacy expectations, would better protect the security—and the freedom that flows from it—that the Fourth Amendment is meant to protect.

Since the Court decided *Quon*, two cases have yielded noteworthy developments in the Constitutional protection of sensitive information. In *NASA v. Nelson*,³⁰³ the Supreme Court continued its delicate approach to Constitutional protection of privacy. Without directly affirming the existence of any Constitutional protection of “information privacy,”³⁰⁴ the Court held that a mandatory questionnaire asking government contractors about drug use did not violate any such right.³⁰⁵ In *U.S. v. Warshak*,³⁰⁶ the Sixth Circuit acknowledged a reasonable expectation of privacy in email communication, noting that “[a]s some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise.”³⁰⁷ The *Warshak* opinion has been hailed as a major development in Fourth Amendment law,³⁰⁸ but its vitality on appeal and its persuasiveness to other Circuits remains to be seen.

IV. CONCLUSION

Quon is a deeply unsatisfying opinion; it provides an unconvincing rebuke to the Ninth Circuit’s conclusion that Quon’s employer’s search was unreasonable and skirts the question of whether a reasonable expectation of privacy exists in electronic communications in the workplace—an issue of increasing relevance. Although the Court appreciates the danger of limiting a technology’s usefulness by protecting too much privacy, it does a poor job of

303. 562 U.S. ___, 131 S. Ct. 746 (2011).

304. “Information privacy” in this context refers “broadly to a constitutional privacy interest in avoiding disclosure of personal matters.” *Id.* at 751 (citing “two cases decided more than 30 years ago . . .”: *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977)). The *NASA* court does not discuss the Fourth Amendment in any detail; indeed, it does not even cite to the *Quon* opinion.

305. *Id.* at 751.

306. 631 F.3d 266 (6th Cir. 2010).

307. *Id.* at 286.

308. Paul Ohm, *Court Rules Email Protected by Fourth Amendment*, FREEDOM TO TINKER (Dec. 14, 2010, 3:02 PM), <http://www.freedom-to-tinker.com/blog/paul/court-rules-email-protected-fourth-amendment/> (“[*Warshak* is] the opinion privacy activists and many legal scholars . . . have been waiting and calling for, for more than a decade.”).

striking a balance with the danger of protecting too little. Both too much protection and too little protection of privacy are legitimate concerns. Going forward, courts should assess privacy protection (including Fourth Amendment protection) through the lens of proportionality that Serwin discusses.

Quon only serves to punctuate the need for a clearer articulation of Fourth Amendment's protection of privacy. Whether through Solove's dramatic revision to the Fourth Amendment or Kerr's more modest restructuring, the need for a clearer picture of the Amendment's scope has nearly universal recognition in legal academia. As technology pushes more personal information into electronic space, and as employers provide and expect less separation between professional and personal time, the need for clarity—from the Court or from Congress—grows more pressing. Without a stronger statement about the Constitutional protection of information privacy, the stealthy encroachments of the digital age will become commonplace, and the moving target of privacy—along with the liberty and security it affords—will move further and further from the mark.