

CLOUD COMPUTING AND STORED COMMUNICATIONS: ANOTHER LOOK AT *QUON V. ARCH WIRELESS*

David S. Barnhill

I. INTRODUCTION

“[N]othing is better worthy of legal protection than private life, or, in other words, the right of every man to keep his affairs to himself, and to decide for himself to what extent they shall be the subject of public observation and discussion.”¹

As I write this Note, each draft is uploaded to a server on a network run by Dropbox, an internet-based service that syncs files across multiple computers, so that I can access drafts from any computer. When I email this Note for comments and suggestions from my Gmail account, copies of the emails will be saved on Google’s servers. When the Note is complete, I will upload it to a networked storage system run by Amazon so that other people with sufficient account privileges may access it.

This real-world example of cloud computing raises important Fourth Amendment issues.² Average Americans regularly use web-based email and online storage systems to interact and communicate in the cloud. Which of these communications, if any, does the Fourth Amendment protect from unreasonable search and seizure? To put it another way, when do people have a reasonable expectation of privacy in data stored in the cloud?

In the recent *Quon v. Arch Wireless Operating Co.*³ decision, the Ninth Circuit held that there was a reasonable expectation of privacy in the contents of text messages. The Ninth Circuit broke with Supreme Court

© 2010 David S. Barnhill.

1. Edward L. Godkin, *Libel and Its Legal Remedy*, 12 J. SOC. SCI. 69, 80 (1880).

2. The National Institute of Standards and Technology provides the following definition of cloud computing: “Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.” Peter Mell and Tim Grance, *The NIST Definition of Cloud Computing*, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, INFORMATION TECHNOLOGY LABORATORY (October 7, 2009), <http://csrc.nist.gov/groups/SNS/cloud-computing>. For more discussion on the definition of cloud computing, see Section IV.A, *infra*.

3. 529 F.3d 892, 905 (9th Cir. 2008) [hereinafter *Quon Circuit*], *cert. granted sub nom.* City of Ontario v. Quon, 2009 WL 1146443 (U.S. Dec. 14, 2009) (No. 08-1332).

precedent that held information voluntarily revealed to third parties loses all privacy protection (the business records cases).⁴

The decision in *Quon* is also notable because the protected text messages were sent from an employer-issued pager and the Ninth Circuit held that the “operational realities” of the workplace indicated that Quon’s messages would be private, even though his employer’s policy was that all pager communications would be subject to inspection.⁵ The court further ruled that Quon’s employer, the Ontario Police Department, violated his Fourth Amendment rights because the audit of his text messages constituted an excessively intrusive and therefore unreasonable search.⁶

The Supreme Court granted certiorari, so it will decide whether the Ninth Circuit correctly found a reasonable expectation of privacy in the content of the text messages and correctly weighed the “operational realities” of the workplace to find that the search performed was excessively intrusive.⁷ This is an opportunity for the Court to speak directly on the privacy protections available for electronic communications delivered through third parties. By extending Fourth Amendment protections to text messages, the Supreme Court could recognize the growing importance of email and texting as a means of private communication and update privacy protections to accommodate current technology just as it did with telephones in the 1967 decision *Katz v. United States*.⁸ Additionally, the Court will likely attempt to give greater guidance to courts in analyzing the “operational realities” of a particular workplace.⁹ Because the current analysis of the Fourth Amendment in the workplace is case-specific, general guidance is desirable to

4. See *Smith v. Maryland*, 442 U.S. 735 (1979) (holding that because dialed telephone numbers are voluntarily revealed to the phone company, the plaintiff did not have any reasonable expectation in the privacy in the numbers dialed); *United States v. Miller*, 425 U.S. 435 (1976) (holding that the plaintiff had no reasonable expectation of privacy in bank records that contained only information voluntarily given to the bank for use in their normal course of business); *Couch v. United States*, 409 U.S. 322 (1973) (holding that there was no reasonable expectation of privacy in tax records produced by an accountant where the plaintiff challenged a summons directing her accountant to produce her tax records).

5. *Quon Circuit*, 529 F.3d at 907.

6. *Id.* at 909 (“[The search] was excessively intrusive in light of the noninvestigatory object of the search, and because Appellants had a reasonable expectation of privacy in those messages, the search violated their Fourth Amendment rights.”).

7. See Brief of Petitioners at i, *City of Ontario v. Quon*, No. 08-1332 (U.S. Feb. 5, 2010) (listing the questions presented to the Court).

8. *Katz v. United States*, 389 U.S. 347 (1967) (holding that electronically recording a phone call made from a phone booth violated the Fourth Amendment even though no physical intrusion occurred).

9. Brief of Petitioners at i, *City of Ontario*, No. 08-1332 (listing the questions presented to the Court).

provide more certainty for employers to establish effective workplace policies without incurring liability for violating an employee's privacy protections.

The Note begins by discussing the Supreme Court Fourth Amendment precedent in Part I. Part II recounts the factual and procedural background of *Quon*, focusing on the Fourth Amendment and the workplace. Part III surveys cloud computing technology, including the motivations and concerns related to its use, and Fourth Amendment protections to cloud data. The Note concludes by proposing a method for analyzing privacy in cloud computing in the workplace.

II. THE FOURTH AMENDMENT

The Fourth Amendment to the Constitution provides in part: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."¹⁰ The protection against unreasonable search and seizure in the Fourth Amendment applies only to state action, including government employers like those in *Quon*.¹¹

This section describes the Supreme Court's Fourth Amendment jurisprudence, tracing its evolution and current status in the context of both electronic communication and the workplace. It particularly focuses on the third-party doctrine as it is applied in the business records cases because of its relevance to the discussion of Fourth Amendment protections for cloud data.¹² The business records cases raised the possibility that emails and data stored on remote servers were "wholly without Fourth Amendment protection" because "individuals have no protected privacy interest in personal information and records voluntarily disclosed to businesses."¹³

A. *KATZ V. UNITED STATES*

The modern view of the Fourth Amendment must start with the Supreme Court's decision in *Katz v. United States*. In *Katz*, the Court held that the government performed an unlawful search in violation of the Fourth

10. U.S. CONST. amend. IV.

11. *See* O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("Searches and seizures by government employers or supervisors of the private property of their employees, therefore, are subject to the restraints of the Fourth Amendment."); *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921) ("The Fourth Amendment gives protection against unlawful searches and seizures, and . . . its protection applies to governmental action.").

12. *See* Section IV.C, *infra*.

13. Dierdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1558 (2004).

Amendment when it electronically listened to and recorded Katz's telephone conversation while he was in a phone booth.¹⁴ This was a departure from previous Fourth Amendment jurisprudence limiting illegal searches to physical intrusions;¹⁵ the Court stated that "the Fourth Amendment protects people—and not simply 'areas.'"¹⁶ The Court recognized that Fourth Amendment protection for the telephone was necessary because "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."¹⁷

The Court's holding opened the door to broader privacy protection. Justice Harlan's concurring opinion particularly focused the Court's modern Fourth Amendment jurisprudence on people rather than property by articulating the need for a reasonable expectation of privacy.¹⁸ Justice Harlan's concurrence identified two requirements to claim Fourth Amendment protection. First, a person must "exhibit[] an actual (subjective) expectation of privacy," and second, "the expectation [must] be one that society is prepared to recognize as 'reasonable.'"¹⁹ The first requirement is subjective, the second is objective. Following Supreme Court guidance, the Ninth Circuit has traditionally focused on the objective requirement, stating "the touchstone of the Fourth Amendment is reasonableness."²⁰

B. THE FOURTH AMENDMENT IN THE WORKPLACE, *O'CONNOR V. ORTEGA*

Applying the reasonableness standard, the Supreme Court defined the scope of Fourth Amendment protection in the workplace in *O'Connor v. Ortega*.²¹ In *Ortega*, state hospital officials searched the office of a physician in

14. 389 U.S. 347, 352 (1967) ("One who occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.>").

15. *Id.* at 352–53 ("[T]he absence of [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry, for that Amendment was thought to limit only searches and seizures of tangible property.") (citing *Goldman v. United States* 316 U.S. 129, 134–36 (1942); *Olmstead v. United States*, 277 U.S. 438, 457, 464, 466 (1928)).

16. *Id.* at 353.

17. *Id.* at 352.

18. Robert S. Steere, *Keeping "Private Email" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U. L. REV. 231, 241 (1998) ("[T]he language found in Justice Harlan's concurring opinion [has] emerged as the foundation for the 'reasonable expectation of privacy' test that exists today.>").

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

20. *Quon Circuit*, 529 F.3d 892, 903 (9th Cir. 2008) (quoting *United States v. Kriesel*, 508 F.3d 941, 947 (9th Cir. 2007)); see *Illinois v. McArthur*, 531 U.S. 326, 330 (2001) ("[The Fourth Amendment's] central requirement is one of reasonableness.>").

21. 480 U.S. 709 (1987).

conjunction with a sexual harassment investigation.²² The hospital fired the physician, who subsequently filed suit claiming that the hospital violated his Fourth Amendment rights.²³ The Supreme Court, in a plurality opinion, held that the physician had a reasonable expectation of privacy in his workplace and remanded to determine whether the hospital's search was reasonable.²⁴

The first issue presented in *Ortega* was whether a public employee had a reasonable expectation of privacy “in his office, desk, and file cabinets at his place of work.”²⁵ Assuming that the public employee established a reasonable expectation of privacy, the second issue concerned the “appropriate Fourth Amendment standard for a search conducted by a public employer.”²⁶ Justice O'Connor, writing for the plurality, presented a contextual approach that weighed the privacy interests of the public employees against the interests of the employers in efficiently and effectively managing the workplace.²⁷

1. *Reasonable Expectation of Privacy of Employees*

The threshold question in *Ortega* asks whether a public employee has a reasonable expectation of privacy in the physical location or item of interest.²⁸ The expectation of privacy must be one that society is willing to accept and is not nullified because a person works for the government.²⁹

But not all workplaces are equal. Once a court determines that there is a reasonable expectation of privacy in the location or item of interest, the inquiry must proceed on a fact-specific basis because, as the *Ortega* Court recognized, the “operational realities” vary from workplace to workplace.³⁰ Some of the “operational realities” of a workplace affecting an employee's reasonable expectation of privacy include the employer's regulations and policies related to privacy and whether they are actively enforced.³¹ In *Ortega*, the Court found that the physician had a reasonable expectation of privacy in his desk and file cabinets considering the following factors: he did not share his desk, he kept personal material in his office, and the hospital had not

22. *Id.* at 712–13.

23. *Id.* at 714.

24. *Id.* at 728–29.

25. *Id.* at 712.

26. *Id.*

27. *Id.* at 719–20.

28. *Id.* at 715.

29. *Id.* at 716–17.

30. *Id.* at 718.

31. *Id.* at 719.

established any policy discouraging employees from storing personal items in their offices.³²

This analysis did not satisfy Justice Scalia, however, who argued in a concurring opinion for a clearer rule: “I would object to the formulation of a standard so devoid of content that it produces rather than eliminates uncertainty in this field.”³³

32. *Id.* at 718–19.

33. *Id.* at 730 (Scalia, J., concurring). One way to analyze this statement is to look at the application of the standard as applied by the various circuits. Circuit courts applying *Ortega* have recognized several factors as important. *See* *United States v. Taketa*, 923 F.2d 665, 671 (9th Cir. 1991) (holding that an employee who used a coworker’s office where that coworker was granted exclusive use of the office, does not have a reasonable expectation of privacy); *Am. Postal Workers Union, Columbus Areal Local AFL-CIO v. U.S. Postal Serv.*, 871 F.2d 556, 59–60 (6th Cir. 1989) (ruling that a waiver of privacy rights and notice to the employees as provided in collective bargaining agreement were enough to defeat an expectation of privacy even when employers had never previously searched the area in question); *Schowengerdt v. Gen. Dynamics Corp.*, 823 F.2d 1328, 1335 (9th Cir. 1987) (concluding that the employee enjoyed a reasonable expectation of privacy in areas where he had exclusive use unless he was on notice from the employer that searches could be performed); *McGregor v. Greer*, 748 F. Supp. 881, 888 (D.D.C. 1990) (deciding that public access to an employee’s office, employer privacy policies, and history of searches by the employer are questions of fact to determine whether the employee had a reasonable expectation of privacy). Much of the analysis has turned on whether an employer has an anti-privacy policy. *Compare* *United States v. Ziegler*, 456 F.3d 1138, 1146 (9th Cir. 2006), *superseded by* *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007) (holding no objectively reasonable expectation of privacy existed where the employee’s workplace computer was routinely monitored and the employer’s privacy policy provided sufficient notice of such monitoring), *and* *Biby v. Bd. of Regents, of the Univ. of Neb.*, 419 F.3d 845, 850–51 (8th Cir. 2005) (holding employment policy saying the employer could search employee computer enough to defeat a reasonable expectation of privacy), *and* *United States v. Thorn*, 375 F.3d 679, 683 (8th Cir. 2004) (holding that a policy reserving the right to audit computer use and a prohibition against downloading sexual images overcomes employee’s privacy rights), *and* *United States v. Angevine*, 281 F.3d 1130, 1134 (10th Cir. 2002) (stating because computer-use policy reserved the right to randomly audit internet use and to monitor specific individuals suspected of misusing computers, the employee is on notice, and therefore the expectation of privacy is unreasonable), *and* *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (“Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy. . . .”), *and* *United States v. Simons*, 206 F.3d 392, 398 (4th Cir. 2000) (declaring that the company’s Internet use policy gave sufficient notice to the employee to render any expectation of privacy unreasonable), *and* *Am. Postal Workers Union*, 871 F.2d at 560 (holding no reasonable expectation of privacy in light of the clearly expressed provisions permitting random and unannounced locker inspections), *and* *McGregor*, 748 F. Supp. at 888 (holding that where the policy regarding privacy is unclear an employee may have a reasonable expectation of privacy), *with* *Leventhal v. Knapek*, 266 F.3d 64, 74 (2d Cir. 2001) (stating that because employer did not practice routine searches of workplace computers and did not have a general privacy policy, the employee had a reasonable expectation of privacy in contents of their work computer); *see also* *United States v. Slanina*, 283 F.3d 670, 677 (5th Cir. 2002)

2. Reasonable Search by Employers

If the employee's expectation of privacy was reasonable, then the employer must demonstrate that the search was reasonable "under all the circumstances" to avoid violating the Fourth Amendment.³⁴ Because an employer may desire to search an employee's workplace for various work-related reasons (as opposed to criminal investigations), and because law enforcement is generally not involved in investigations into workplace misfeasance, the traditional requirement that the employer have probable cause before a search can be performed could prove too onerous.

Therefore, the plurality in *Ortega* concluded "that the 'special needs, beyond the normal need for law enforcement[,] make the . . . probable-cause requirement impracticable[]' for legitimate work-related, noninvestigatory intrusions as well as investigations of work-related misconduct."³⁵ Thus, when balancing employees' privacy interests with the employers' special needs to manage the workplace, a standard of reasonableness will not permit arbitrary intrusions upon the former nor "unduly burden" the latter.³⁶ The Court in *Ortega* did not rule on the search performed by the hospital and remanded the case to determine if it was reasonable.³⁷

C. THE THIRD-PARTY DOCTRINE AND THE BUSINESS RECORDS CASES

The third-party doctrine states that even where a person has a reasonable expectation of privacy in a particular item, once he voluntarily gives that item to a third party he surrenders his Fourth Amendment rights.³⁸ The Court applied this doctrine in a trio of cases that have become known as the business records cases.³⁹

In *Couch v. United States*, the Court held that there was no reasonable expectation of privacy in tax records produced by an accountant. The plaintiff challenged a summons directing her accountant, an independent contractor, to produce her tax records as a violation of her Fourth

("[G]iven the absence of a city policy placing [the employee] on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that [the employee's] expectation of privacy was reasonable.").

34. *Ortega*, 480 U.S. at 725–26.

35. *Id.* at 725 (quoting *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring)).

36. *Id.*

37. *Id.* at 729.

38. *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

39. *See* *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976); *Couch v. United States*, 409 U.S. 322 (1973).

Amendment rights.⁴⁰ The IRS attempted to get plaintiff's tax records after noticing that there was a "substantial understatement of gross income" related to the plaintiff's restaurant.⁴¹ The Court held that the plaintiff's reasonable expectation of privacy vanished once she gave the records to the accountant, knowing that much of the information would be revealed in tax documents.⁴²

In *United States v. Miller*, the Court held that the plaintiff had no reasonable expectation of privacy in bank records arising from the normal course of business. The plaintiff was convicted of possessing an unregistered still and defrauding the government of various taxes.⁴³ Before the case was tried, the plaintiff attempted to prevent his bank records from being produced.⁴⁴ The Court found that the records contained only information voluntarily given to the bank for use in their normal course of business, thus destroying any reasonable expectation of privacy the plaintiff had in the records.⁴⁵

In *Smith v. Maryland*, the Court held that the disclosure of telephone numbers to the phone company when dialing prevented plaintiff from having a reasonable expectation of privacy in the numbers dialed. The plaintiff was arrested for robbery after the police discovered that he continued to call and harass the robbery victim.⁴⁶ Investigators discovered this after installing a pen register, a device to record phone numbers, on the plaintiff's phone line.⁴⁷ The plaintiff claimed that the Fourth Amendment protected against discovery of the phone numbers he dialed.⁴⁸ The Court disagreed, holding that because the phone company necessarily inspected the phone numbers to complete the telephone call and bill the plaintiff, he had no reasonable expectation of privacy in the telephone numbers he dialed.⁴⁹ The Court found that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."⁵⁰

40. *Couch*, 409 U.S. at 323.

41. *Id.* at 324.

42. *Id.* at 335–36.

43. *Miller*, 425 U.S. at 436.

44. *Id.*

45. *Id.* at 442–43.

46. *Smith v. Maryland*, 442 U.S. 735, 738 (1979).

47. *Id.* at 737.

48. *Id.* at 737–38.

49. *Id.* at 742.

50. *Id.* at 741 (emphasis in original).

III. *QUON V. ARCH WIRELESS*

The Ninth Circuit in *Quon v. Arch Wireless* held that a person has a reasonable expectation of privacy in the content of text messages sent via, and stored with, third parties. The court also addressed whether certain practices in the workplace defeated that reasonable expectation. Section III.A explores the facts of the case. Section III.B follows with a discussion of the decision in the district court. The decision in the Ninth Circuit is presented in Section III.C. Section III.D discusses the denial for a rehearing en banc.

A. FACTS OF THE CASE

Sergeant Jeff Quon of the Ontario Police Department (OPD), husband to Jerilyn Quon of the OPD, had an affair with OPD dispatcher April Florio.⁵¹ Sergeant Quon routinely sent personal, sexually explicit text messages from his work-issued pager to both his wife and his mistress.⁵² He also sent personal text messages to Sergeant Steve Trujillo, a fellow member of the SWAT team at the OPD.⁵³ The Chief of Police of the OPD discovered that Quon was using his pager for personal purposes when he audited transcripts of Quon's text messages.⁵⁴

The City of Ontario contracted with Arch Wireless Operating Company in October of 2001 to provide two-way, alphanumeric pagers to the City's employees.⁵⁵ In the contract, Arch Wireless stipulated a limit of 25,000 characters per month for each pager and an extra fee for each character exceeding that limit.⁵⁶ The City issued pagers to the OPD SWAT team because of OPD's "refusal to pay overtime or stand-by pay to officers who must be available for SWAT call-outs."⁵⁷

The pagers sent a text message by first sending the message via a radio-frequency (RF) transmission from the pager to a receiving station.⁵⁸ The receiving station then relayed the message either via satellite or wired transmission to a computer network owned by Arch Wireless.⁵⁹ The computer network stored the message for up to seventy-two hours, until the

51. *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1122 (C.D. Cal. 2006) [hereinafter *Quon District*].

52. *Id.* at 1126.

53. *Id.*

54. *Id.* at 1126–27.

55. *Id.* at 1122–23.

56. *Id.* at 1123.

57. *Quon v. Arch Wireless*, 554 F.3d 769, 770 (9th Cir. 2009) [hereinafter *Quon En Banc*].

58. *Quon District*, 445 F. Supp. 2d at 1123.

59. *Id.*

recipient pager was ready to receive the message.⁶⁰ Arch Wireless also archived a copy of the message on their servers.⁶¹ When the recipient pager became ready to receive the message, Arch Wireless sent the message to the transmission station closest to the recipient pager where the station then sent the message via an RF transmission to the pager.⁶²

The OPD declared that the use of the pagers was covered by the City's "Computer Usage, Internet and Email Policy" (Policy).⁶³ The Policy stated that the City "reserves the right to monitor and log all [email use], with or without notice" and that the "[u]sers should have no expectation of privacy . . . when using these resources."⁶⁴ The Policy also stated that all information produced using the City's resources was considered property of the City, and consequently, employees should not use the City's email or Internet for personal communication.⁶⁵ Finally, the Policy stated that "[t]he use of inappropriate, . . . obscene, suggestive, . . . or harassing language in the email system will not be tolerated."⁶⁶

Sergeants Quon and Trujillo, members of the OPD SWAT team, reviewed and signed this Policy in 2000 but were not issued pagers until late 2001 or early 2002.⁶⁷ The OPD issued the pagers to members of the SWAT team "to enable better coordination and a more rapid and effective response to emergencies by providing nearly instantaneous situational awareness to the team as to the other members [sic] whereabouts."⁶⁸ On April 18, 2002, Quon attended a meeting where Lieutenant Steven Duke (Duke), the pager administrator, informed all present that: "two-way pagers are considered email messages. This means that messages would fall under the City's policy as public information and eligible for auditing."⁶⁹ Quon declared that he "vaguely recalled attending the meeting" and that he did not recall Duke extending the Policy to text messages.⁷⁰ Both he and Trujillo, however, subsequently received a memorandum reiterating what Duke had said in the meeting: the OPD considered text messages as email communications covered by the City's Policy.⁷¹

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.* at 1124.

67. *Quon Circuit*, 529 F.3d 892, 895–96 (9th Cir. 2008).

68. *Quon District*, 445 F. Supp. 2d at 1123.

69. *Id.* at 1124.

70. *Quon Circuit*, 529 F.3d at 896 (internal quotations removed).

71. *Quon District*, 445 F. Supp. 2d at 1124.

Despite the statements made in that April meeting, Duke implemented an informal policy regarding the use of the pagers that contravened the City's Policy.⁷² As the pager administrator, Duke informed personnel (including Quon) that messages would only be audited if an officer exceeded his monthly character limit and disputed the charges claiming that the messages were work-related.⁷³ If an officer paid the overage charges himself, the messages would not be audited.⁷⁴ Quon exceeded his limit three or four times, but paid the charges each time without incident.⁷⁵

In August of 2002, however, Duke grew weary of collecting the overage charges from the officers and informed Chief Lloyd Scharf of the problem.⁷⁶ Chief Scharf told Duke to audit the messages to see if they were work-related to determine if the character limit should be increased. Chief Scharf ordered Duke to review the transcripts of Quon's sent messages over a two-month period.⁷⁷

The transcripts of Quon's text-messages over the two-month period covered forty-six pages and of the 450 text-messages sent, only fifty-seven were for business-related purposes.⁷⁸ After reading Duke's report on the matter, Chief Scharf and Quon's supervisor reviewed the contents of the messages.⁷⁹ Subsequently, the matter was turned over to Internal Affairs to investigate Quon's alleged misconduct.⁸⁰ When asked why Chief Scharf and the Internal Affairs officer read all of Quon's messages, the Internal Affairs officer stated: "Sgt. Quon was asked and indicated that he could not state how much time he spent on the pager during work hours. Therefore, reviewing and redacting the transcripts was the only reasonable method to obtain this information."⁸¹

72. *Id.*

73. *Id.*

74. *Id.*

75. *Quon Circuit*, 529 F.3d at 897.

76. *Quon District*, 445 F. Supp. 2d at 1125.

77. *Id.* at 1125–26. Chief Scharf requested that Duke review the text message transcripts of the two officers with the most severe overages, not specifying any particular officer. *Id.* at 1125. Quon satisfied this criteria. *Id.*

78. *Quon En Banc*, 554 F.3d 769, 775 (9th Cir. 2009).

79. *Quon District*, 445 F. Supp. 2d at 1126.

80. *Id.* at 1127 ("Chief Scharf thereafter made a determination that Quon's pager was being misused in that too much duty time was used for personal pages not associated with duty on duty time.").

81. Aff. Of Patrick McMahon at ¶ 4, *Quon v. Arch Wireless, Inc.*, 445 F. Supp. 2d 1116 (C.D. Cal. June 30, 2006) (No. ED CV 03-199 SGL), 2006 WL 4791055.

B. THE DISTRICT COURT DECISION

Quon and several others filed suit against the City of Ontario and the Ontario Police Department in the Central District of California alleging, *inter alia*, violations of their Fourth Amendment rights.⁸² After a jury determined the purpose of the police department's search into the content of Quon's text messages, the district court found all defendants free from liability for the search.⁸³

Relying on *Ortega*, the court held that the City's search was not unreasonable notwithstanding the plaintiffs' reasonable expectation of privacy in the content of the text messages based on the informal policy instituted by Duke.⁸⁴ The court concluded that the intent of the search determined its reasonableness—if the intent was to uncover misconduct then it was unreasonable, but if the intent was to determine the efficacy of the character limit then it was reasonable.⁸⁵ A jury decided that the purpose of the search was to determine the efficacy of the character limit.⁸⁶ Thus, the court returned a verdict in favor of the defendants.⁸⁷

The court held that Quon (and the rest of the plaintiffs by extension) had a reasonable expectation of privacy in the content of the text messages.⁸⁸ Applying the first prong of the *Ortega* test, the court stated that if the City's formal Policy (as applied to text messages) was the only factor considered, Quon would have no reasonable expectation of privacy.⁸⁹ However, the court held that Duke's informal policy of not auditing text messages if overage charges were paid "eroded any attempt on defendants' part to lessen the expectation of privacy its employees had in the use of the pagers issued to

82. *Quon District*, 445 F. Supp. 2d at 1128. Jeff and Jerilyn Quon, April Florio, Steve Trujillo, and Doreen Klein filed claims against Arch Wireless, the City of Ontario, Chief of Police Lloyd Scharf, and Sergeant Glenn were for violating the Stored Communications Act, the Fourth Amendment, the California Constitution, C.P.C. § 629.86, invasion of privacy and defamation. The government defendants (all defendants except Arch) were granted summary judgment on the SCA claims because they provide no service (no cause of action under § 2702) and the investigation was not a criminal one (no cause of action under § 2703). *Id.* at 1129. Likewise, Arch was granted summary judgment on the Fourth Amendment (and related California Constitution claims) because these claims are preempted by the allowances in the SCA. *Id.* at 1138. The claims for invasion of privacy and defamation along with violations of C.P.C. § 629.86 will not be discussed in this Note. Also, Doreen Klein was not part of the appeal to the Ninth Circuit, so this Note will not discuss her case.

83. *Id.* at 1138, 1149.

84. *Id.* at 1149.

85. *Id.* at 1146.

86. *Quon Circuit*, 529 F.3d 892, 908 (9th Cir. 2008).

87. *Id.*

88. *Quon District*, 445 F. Supp. 2d at 1141–43.

89. *Id.* at 1140.

them; indeed, [Duke's] actions could be said to have *encouraged* employees to use the pagers for personal matters."⁹⁰

To determine the reasonableness of a search, a court must decide whether the search was justified at its inception and whether it was "reasonably related in scope to the circumstances which justified the interference in the first place."⁹¹ Regarding the reasonableness of the search performed, the court reasoned that "[t]he dispute in question concerns the actual *purpose* or *objective* Chief Scharf sought to achieve in having Duke perform the audit of Quon's pager."⁹² If Scharf ordered the search to determine the efficacy of the character limit, then the search was reasonable at its inception.⁹³ Otherwise, if it were designed to uncover misconduct the search would be unreasonable at its inception.⁹⁴ The court declared if a jury found that the true purpose of the audit was to determine the percentage of text messages that were work-related, then it would be reasonable in scope.⁹⁵ The court concluded "if the purpose for the audit was to determine the efficacy of the existing character limits to ensure that officers were not paying hidden work-related costs, then the Court finds that no constitutional violation occurred."⁹⁶

C. THE NINTH CIRCUIT'S DECISION

Quon appealed the case to the Ninth Circuit where the court reversed the district court's decision. It held that OPD's search was unreasonable in scope.⁹⁷ The Ninth Circuit agreed with the district court that Quon and the other appellants had a reasonable expectation of privacy in the content of their text messages, but the court disagreed as to the scope of the search ruling, finding that the search was excessively intrusive and violated the appellants' Fourth Amendment rights.⁹⁸

90. *Id.* at 1142 (emphasis original).

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

92. *Quon District*, 445 F. Supp. 2d at 1144 (emphasis original).

93. *Id.* at 1146.

94. *Id.* at 1144. The court stated that the applicable misconduct was "play[ing] games [on] City time" according to the defendants. *Id.* Since Duke's informal policy allowed officers to use the pagers for personal use, the misconduct at issue here did not exist and hence could not be uncovered by the search making the search unreasonable at its inception. *Id.*

95. *Id.* at 1145.

96. *Id.* at 1146.

97. *Quon Circuit*, 529 F.3d 892, 910–11 (9th Cir. 2008). The court affirmed the district court's holding that the search was reasonable at its inception. *Id.* at 908. The claims against Arch Wireless for violating the Stored Communications Act will not be discussed in this Note.

98. *Id.* at 909.

1. *Fourth Amendment Protection for Text Messages*

The Ninth Circuit held that the search in question violated their Fourth Amendment rights because Quon and the other appellants had a reasonable expectation of privacy in the content of the text messages and the scope of the search conducted by the OPD was unreasonable.⁹⁹

The Ninth Circuit has declared that the “touchstone of the Fourth Amendment is reasonableness,” both in the expectation of privacy and the search in question.¹⁰⁰ Because the extent of Fourth Amendment protection for modern electronic communication is an “open question,” the Ninth Circuit looked to comparable communications for guidance on the privacy expectations.¹⁰¹ In addition, employment circumstances often affect whether an expectation of privacy is reasonable.¹⁰² To evaluate the reasonableness of a search, the court must determine whether it is “justified at its inception” and whether it is “reasonably related in scope to circumstances which justified interference in the first place.”¹⁰³

a) Reasonable Expectation of Privacy

In determining whether the Appellants had a reasonable expectation of privacy in stored text messages, the Ninth Circuit looked to other technologies for guidance.¹⁰⁴ First, the Ninth Circuit looked to cases involving phones and determined that tapping a telephone violates a reasonable expectation of privacy while a device that records phone numbers dialed does not because it does not capture the contents of the communication.¹⁰⁵ Next, the court reviewed cases involving letters where the Supreme Court and the Ninth Circuit determined that there is a reasonable expectation of privacy as to the contents but not the address.¹⁰⁶ Finally, the

99. *Id.*

100. *United States v. Kriesel*, 508 F.3d 941, 947 (9th Cir. 2007).

101. *Quon Circuit*, 529 F.3d at 904.

102. *O'Connor v. Ortega*, 480 U.S. 709, 718 (1987).

103. *Id.* at 726.

104. *Quon Circuit*, 529 F.3d at 904–06. For a critique on this method of analysis, see Amanda Yellon, Comment, *The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications*, 4 J. BUS. & TECH. L. 411 (2009).

105. *Quon Circuit*, 529 F.3d at 904 (looking to previous Supreme Court cases, *Smith v. Maryland*, 442 U.S. 735 (1979) and *Katz v. United States*, 389 U.S. 347 (1967), for guidance regarding Fourth Amendment protection for electronic communication). For more discussion on *Smith* and *Katz*, see Part II, *supra*.

106. *Quon Circuit*, 529 F.3d at 905 (looking to previous Supreme Court and Ninth Circuit cases, *United States v. Jacobsen*, 466 U.S. 109, 114 (1984), *United States v. Hernandez*, 313 F.3d 1206, 1209–10 (9th Cir. 2002), and *United States v. Choate*, 576 F.2d 165, 174 (9th Cir. 1978), about the privacy of letters).

court drew upon its email privacy jurisprudence that ruled that there is no privacy in the information indicating the sender and recipient of emails.¹⁰⁷ The court concluded that the privacy interests in letters and email were identical,¹⁰⁸ and extended that protection to text messages by declaring “no meaningful difference between . . . emails . . . and the text messages at issue here.”¹⁰⁹ For the recipients of text messages, the Ninth Circuit held that as a matter of law there is a reasonable expectation of privacy that the content of the messages will not be revealed without the sender’s consent.¹¹⁰

For the sender of the text messages in this case, Quon, the Ninth Circuit ruled that the informal policy of the Department, stating that text messages would not be audited if the officers paid their overage charges, rendered the expectation of privacy reasonable.¹¹¹ The court affirmed the district court’s finding that if the OPD followed the formal Policy of the City there would be no reasonable expectation of privacy for the employees.¹¹² However, because the informal policy instituted by Duke was the “operational reality” of the OPD and because officers relied on the informal rather than the formal policy, Quon had a reasonable expectation of privacy in the contents of his messages.¹¹³

b) Reasonableness of the Search

The court in *Quon* found that when the OPD audited Quon’s text messages they violated the appellants’ Fourth Amendment rights.¹¹⁴ The court affirmed the finding of the jury, that Chief Scharf’s purpose in searching Quon’s text messages was to determine the efficacy of the character limit, and consequently held the search reasonable at its inception.¹¹⁵ However, the court determined that the scope of the search intruded upon the Appellants’ reasonable expectation of privacy in such a

107. *Id.* (reviewing a Ninth Circuit opinion, *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008), about the privacy of email). The Court points out that there has been no ruling as to whether there is a reasonable expectation of privacy in the content of emails. *Id.*

108. *Id.* (citing *Forrester*, 512 F.3d at 511).

109. *Id.*

110. *Id.* This ruling applied to Appellants Jerilyn Quon, Steve Trujillo, and April Florio, the recipients of Jeff Quon’s text messages. *Id.* at 905 n.6. Jeff Quon’s reasonable expectations were additionally affected by the OPD’s policies. *Id.*

111. *Id.* at 907.

112. *Id.*

113. *Id.*

114. *Id.* at 909.

115. *Id.* at 908.

manner as to be deemed unreasonable as a matter of law in light of the non-investigatory purpose of the search.¹¹⁶

D. PETITION FOR REHEARING EN BANC DENIED

Judge Ikuta wrote a vigorous dissent to the denial of the petition for rehearing the case en banc, criticizing the panel's decision regarding the Fourth Amendment and accusing them of ignoring Supreme Court precedent.¹¹⁷ Judge Wardlaw, the author of the Ninth Circuit's opinion, wrote a concurrence to the denial of hearing demonstrating that the decision comported with the Court's prior rulings.¹¹⁸

The dissent criticized the Ninth Circuit's ruling that the OPD violated the Fourth Amendment when it audited Quon's messages for two reasons. First, the dissent asserted that a finding of a reasonable expectation of privacy in messages sent with company pagers undermined the rule set forth in *Ortega* and "hobbles government employers."¹¹⁹ Second, the dissent argued the opinion in *Quon* failed to follow Supreme Court precedent and seven other Circuits regarding the reasonableness of searches.¹²⁰

As to the first point, the dissent argued that finding a reasonable expectation of privacy in the content of the text messages ignored the operational realities of the workplace. The dissent pointed to several factors militating against a reasonable expectation of privacy in the text messages, such as: (1) the written and oral policy of the City communicated to Quon, (2) the issuance of the pager Quon for SWAT-related work, (3) the lack of privacy expectations in the content of SWAT-related communications, and (4) the diminished expectation of any privacy under the California Public Records Act.¹²¹ The dissent insisted that ignoring these operational realities and allowing one man's informal policy to override all other factors "departs from the practical approach of *O'Connor* and effectively precludes a public employer from undertaking investigations reasonably necessary to conduct its business."¹²²

Additionally, Judge Ikuta declared that the court erred in holding that the OPD's search was excessively intrusive.¹²³ The dissent argued that the court

116. *Id.* at 909 (reasoning that the search was excessively intrusive in light of the purpose of the search, noting a "host of simple ways" to achieve the same goal).

117. *Quon En Banc*, 554 F.3d 769, 774–79 (9th Cir. 2009).

118. *Id.* at 769–74.

119. *Id.* at 774.

120. *Id.*

121. *Id.* at 776.

122. *Id.* at 777.

123. *Id.*

relied on a test from *Schowengerdt v. General Dynamics Corp.*, the “least intrusive means” test, that the Supreme Court has superseded three times and that was no longer considered good law.¹²⁴ The dissent explained that to determine the reasonableness of the search, the court erroneously looked at what the OPD could have done rather than analyzing what it actually did.¹²⁵ Again, the dissent suggested this result would unfairly burden government employers and restrict their ability to reasonably monitor their workplace.¹²⁶

Judge Wardlaw began the concurring opinion by saying that “[n]o poet ever interpreted nature as freely as Judge Ikuta interprets the record on this appeal.”¹²⁷ The concurrence declared that the court’s decision in *Quon* follows *Ortega* and that the dissent misconstrues several key facts,¹²⁸ including: (1) there was no official policy regarding the pagers, (2) Quon did not recall Duke extending the City’s computer policy to the pagers, (3) Duke’s informal policy carried “a great deal of weight” as the administrator of the pagers, (4) Quon’s reliance on the informal policy was reasonable, (5) the practices of the OPD were consistent with the informal policy, and (6) both the District Court and Ninth Circuit panel found that Quon had a reasonable expectation of privacy in the messages.¹²⁹

Judge Wardlaw then explained how the court followed the Supreme Court’s rule in *Ortega*, rebutting the dissent’s claim that the panel applied the superseded “least intrusive means” test. The concurrence emphasized that the rule in *Ortega* dictates that a court must consider the operational realities of the particular workplace and determine reasonableness “under all the circumstances.”¹³⁰ The alternate methods the court discussed in the opinion were to illustrate that the method adopted by the OPD was unreasonable in light of the purpose of the search.¹³¹ The concurrence concluded that the dissent’s fact-blind interpretation of the law would “strip[] public employees of all rights to privacy regardless of the *actual* operational realities of each workplace,” and “create a far broader rule than Supreme Court precedent allows.”¹³²

124. *Id.*; see *Schowengerdt v. Gen. Dynamics Corp.*, 823 F.2d 1328 (9th Cir. 1987) (holding that a search was unreasonable where less intrusive means were feasible that could accomplish the purpose of the search).

125. *Id.* at 778.

126. *Id.* at 779.

127. *Id.* at 769.

128. *Id.* at 769–70.

129. *Id.* at 770–71.

130. *Id.* at 772 (citing *O’Connor v. Ortega*, 480 U.S. 709, 725–26 (1987)).

131. *Id.* at 773.

132. *Id.* at 774 (emphasis in original).

IV. THE INTERSECTION OF STORED COMMUNICATIONS, THE WORKPLACE, AND THE CLOUD

Quon confronts the problem of privacy in stored electronic communications and the workplace's effect on it. Similar problems in a workplace setting in the near future will likely involve cloud computing.¹³³ What can *Quon* teach us about the inevitable conflicts that will arise when privacy in data stored in the cloud is breached? This Part will focus on the expectation of privacy in data for personal use and in a workplace setting to see to what degree the decision in *Quon* affects Fourth Amendment protections for data that is migrating to the cloud.¹³⁴

A. DEFINING CLOUD COMPUTING

Attempting to define cloud computing can prove to be as elusive as attempting to capture a genuine cloud with one's hands.¹³⁵ Many scholars' attempts to define cloud computing have not yielded a universally agreed-upon definition.¹³⁶ The working definition of cloud computing as provided by the National Institute of Standards and Technology will serve as a starting point: "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service

133. See, e.g., *Clash of the Clouds*, THE ECONOMIST, Oct 15th 2009, available at http://www.economist.com/displaystory.cfm?story_id=14637206 (arguing that cloud computing is pushing computing power to central hubs, contrary to previous trends in the industry); Posting of Erick Schonfeld to TechCrunch, "IBM's Blue Cloud Is Web Computing By Another Name," <http://techcrunch.com/2007/11/15/> (Nov. 15, 2007) (defining cloud computing as massive server farms are used for online storage and applications by companies such as Amazon, Google, Yahoo, and IBM).

134. For an interesting take on this, see David A. Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2205–06 (2009) ("Despite the shift in Internet usage, users expect their information to be treated the same on this virtual cloud as it would be if it were stored on their own computer, phone, or iPod.").

135. For an explanation of the origin of the term cloud and its association with the Internet, see Jessie Holliday Scanlon and Brad Wieners, *The Internet Cloud*, THE INDUSTRY STANDARD, July 9, 1999, <http://www.thestandard.com/article/0,1902,5466,00.html?page=0,0>.

136. See, e.g., Posting of Jeremy Geelan to Virtualization Journal, "Twenty one experts define cloud computing," <http://virtualization.sys-con.com/node/612375> (Jan. 24, 2009, 06:15 EST) (presenting twenty-one experts' definitions of cloud computing); Eric Knorr & Galen Gruman, *What Cloud Computing Really Means*, INFOWORLD, April 7, 2008, http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality_1.html (presenting a description of the term cloud and examples of what cloud computing entails).

provider interaction.”¹³⁷ This Part will attempt to present a general overview of the cloud computing model as previously defined that is accessible yet sufficiently detailed to motivate the discussions regarding privacy presented in Section IV.C.

First, it is helpful to identify the three primary actors involved in cloud computing: the Service Users (SUs), the Service Providers (SPs), and the Infrastructure Providers (IPs). SPs provide software services available to SUs.¹³⁸ SP services are made available to SUs through the Internet via interfaces designed for the particular service.¹³⁹ SUs employ client applications that run on SUs’ devices, such as a laptop, PDA, or cellular phone. These client applications may be specific to an SP’s service, like an online backup service running on a computer, or may be a general web browser, like Mozilla Firefox or Internet Explorer. The infrastructure is provided to the SPs by other entities, IPs.¹⁴⁰ IPs provide and maintain the computing resources that allow SPs to scale their services flexibly and reduce their costs.¹⁴¹

The next step is to identify the cloud service models. The cloud services can be grouped into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).¹⁴² SaaS is the most familiar to most internet users, and web-based email falls into this category. SaaS provides users applications through the Internet that behave as the provider intends and over which users have little control outside of configuration settings.¹⁴³ PaaS is a platform for application development that gives customers tools and a computing environment to develop and run their own applications. The PaaS company provides the platform on remote servers to run these applications, and the customers need not maintain the

137. Mell, *supra* note 2; cf. Luis M. Vaquero et al., *A Break in the Clouds: Toward a Cloud Definition*, ACM SIGCOMM COMPUTER COMMUNICATION REVIEW, Volume 39, Issue 1, at 51 (January 2009), ISSN:0146-4833, available at <http://portal.acm.org/citation.cfm?id=1496091.1496100> (“Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization.”).

138. See Vaquero, *supra* note 137, at 50.

139. *Id.*

140. *Id.*

141. *Id.*

142. See Mell, *supra* note 2; Vaquero, *supra* note 137, at 51.

143. See Mell, *supra* note 2; Vaquero, *supra* note 137, at 51. Examples of SaaS include online office applications (e.g., Google Docs), email applications (e.g., Hotmail), Flickr (online photo storage), and Pixlr (online photo editor).

underlying software infrastructure that allows the applications to function.¹⁴⁴ IaaS companies provide the hardware infrastructure (such as servers and storage) for a customer to use remotely, allowing the customer to install and maintain whatever operating system, software, and applications they desire.¹⁴⁵

The final step in this overview is to identify how these clouds are deployed. The three main deployment models are private clouds, public clouds, and hybrid clouds.¹⁴⁶ A private cloud is one where the cloud infrastructure is uniquely provided to a single customer.¹⁴⁷ A public cloud is one provided to the general public.¹⁴⁸ A hybrid cloud mixes private and public clouds, maintaining them as unique entities but tying the clouds together with technology allowing for data and application portability between them.¹⁴⁹

To illustrate how these categories interact, I will provide a hypothetical example. Imagine that Company A designed a web application that allows users to upload a number of photographs to create a collage. Company A pays Company B to provide a suitable number of web servers and storage so that internet users may access Company A's application. Company A installs the necessary operating systems and software libraries on Company B's servers so that Company A's application is functional and available on the Internet. In this scenario, Company A is providing Software as a Service and acts as Service Provider to any internet user making a collage with their application, the internet users being the Service Users. For these Service Users, the collage application is in a public cloud. Company B provides Infrastructure as a Service to Company A, so Company B is the Infrastructure Provider. If Company B provides the servers and storage only for Company A, the infrastructure is a private cloud, but if this service is open to the public it is a public cloud.

B. MOTIVATIONS AND CONSIDERATIONS WHEN MOVING TO THE CLOUD

Many motivations exist for migrating to cloud-based services. Consumers benefit when ad-supported applications in the cloud are free and viable options to costly non-cloud software. In addition, possible customers need

144. See Mell, *supra* note 2; Vaquero, *supra* note 137, at 51. Examples of PaaS include Google Apps Engine, BungeeConnect, and Yahoo! Pipes.

145. See Mell, *supra* note 2; Vaquero, *supra* note 137, at 51. Examples of IaaS are Amazon Web Services and Flexiscale.

146. See Mell, *supra* note 2.

147. *Id.*

148. *Id.*

149. *Id.*

not install resource intensive applications on their computers because the hardware in the cloud provides the computing power and storage. All that the potential customer needs is a simple client application or a web browser and an internet connection. Many cloud-based services are available to any device that can connect to the Internet, which provides increased mobility and freedom from device tie-in. Finally, data stored in the cloud serves as a useful backup for important information that could be lost due to hardware failures.

Significant economic benefits exist for migrating to the cloud for businesses as well. As a practical matter for businesses, providing a service that does not require a customer to have a particular operating system or minimum hardware capabilities broadens a company's possible consumer base. In addition, as server-side storage and processing power costs decline relative to those of client-side storage and processing, a business realizes an economic advantage from moving their data and processing to the cloud.¹⁵⁰

However, these may not be the most compelling economic reasons to migrate to cloud computing because they ultimately waste resources.¹⁵¹ In the cloud, multiple copies of data may be stored and bandwidth is needed to interact with the various applications and to access the online storage.¹⁵² Ed Felten, in a post on the blog Freedom to Tinker, presents an alternative economic motivation:

Why, then, are we moving into the cloud? The key issue is the cost of management. Thus far we focused only on *computing* resources such as storage, computation, and data transfer; but the cost of managing all of this – making sure the right software version is installed, that data is backed up, that spam filters are updated, and so on – is a significant part of the picture. Indeed, as the cost of computing resources, on both client and server sides, continues to fall rapidly, management becomes a bigger and bigger fraction of the total cost. And so we move toward an approach that minimizes management cost, even if that approach is relatively wasteful of computing resources. The key is not that we're moving computation from client to server, but that we're moving management to the server, where a team of experts can manage matters for many users.¹⁵³

150. Posting of Ed Felten to Freedom to Tinker, "What Economic Forces Drive Cloud Computing?" <http://www.freedom-to-tinker.com/blog/felten/what-economic-forces-drive-cloud-computing> (July 23, 2009, 12:39).

151. *Id.*

152. *Id.*

153. *Id.* (emphasis in original).

Thus, the move to the cloud may present many advantages. But before a person or company chooses to migrate to the cloud, they should consider the privacy implications of such a move.

C. CLOUD COMPUTING, PRIVACY, AND THE WORKPLACE

The Ninth Circuit in *Quon* held that the sender and recipients of text messages had a reasonable expectation of privacy in the content of their messages, even where the service provider had access to the contents of those messages.¹⁵⁴ The court reached this conclusion by analogizing text messages to phone calls, letters, and emails.¹⁵⁵ Only after finding a reasonable expectation of privacy in the content of the text messages did the court proceed to consider the employee's workplace environment to determine whether that environment rendered the expectation unreasonable.¹⁵⁶ The analysis in *Quon* guides the discussion in this Section. Privacy in the cloud first hinges on whether there exists a reasonable expectation of privacy in the content of certain data, and then whether a public employee's expectation may be rendered unreasonable by various workplace practices and policies.¹⁵⁷

1. Reasonable Expectation of Privacy in the Cloud

The first step is to determine whether there is a reasonable expectation of privacy in the data stored in the cloud. Because of the nature of cloud computing, data must be stored with third parties. Thus, courts must consider the broad implications of Fourth Amendment doctrine that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" to the cloud.¹⁵⁸

Two recent cases illustrate the current divergence over whether the third-party doctrine applies to cloud-based email services.¹⁵⁹ A district court judge

154. See Section III.C, *supra*.

155. *Quon Circuit*, 529 F.3d 892, 904–05 (9th Cir. 2008). Note, however, that the court recognized that there was no case explicitly holding that there is a reasonable expectation of privacy in the content of emails, but they cited a case where the Ninth Circuit declared that the privacy interests in letters and emails were identical. *Id.* at 905.

156. *Id.* at 906.

157. Fourth Amendment conflicts between employers and employees in the workplace necessarily require that the employer be a public employer. *Burdeau v. McDowell*, 256 U.S. 465, 475 (1921). States may have privacy laws affecting private sector employees in a similar fashion, see e.g., Laura B. Pincus & Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers*, 33 AM. BUS. L.J. 51 (1995) ("As the Constitution applies only to state action, private sector employees must rely on common law protections or state statutory protection, both of which vary wildly from state to state.").

158. *Smith v. Maryland*, 422 U.S. 735, 743–44 (1979).

159. For a discussion of the third-party doctrine, see *supra* Section II.C.

in Oregon wrote about the privacy of email stored in the cloud in *In re United States*, a case deciding whether the government must notify an individual when they have obtained a search warrant for their personal email account.¹⁶⁰ He explained that Google's Privacy Policy indicated that Google can access any information stored on their servers and will share such information about its subscribers when it has a "good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to . . . satisfy any applicable law, regulation, legal process or enforceable governmental request."¹⁶¹ The court looked to the Supreme Court's third-party doctrine to inform their opinion on the privacy of email in the cloud.¹⁶² Apparently contradicting the Ninth Circuit's decision in *Quon*, the District Court of Oregon reasoned that:

[S]ubscribers are, or should be, aware that their personal information and the contents of their online communications are accessible to the ISP and its employees and can be shared with the government under the appropriate circumstances. Much of the reluctance to apply traditional notions of third party disclosure to the email context seems to stem from a fundamental misunderstanding of the lack of privacy we all have in our emails. Some people seem to think that they are as private as letters, phone calls, or journal entries. The blunt fact is, they are not.¹⁶³

The court stated that email that is stored on a remote computer with a third party has no Fourth Amendment protection. This statement cannot be squared with the holding in *Quon* that there is a reasonable expectation of privacy in the content of text messages even though the service provider can access that information.¹⁶⁴ However, the court did not hold that email was per se without Fourth Amendment protection. It assumed without deciding that email was protected, but the language cited above indicates a lack of unanimity whether there is any constitutional protection for email stored in the cloud.¹⁶⁵

In a similar case involving a Bear Stearns hedge fund manager prosecuted for securities fraud, the state attempted to enter the manager's personal email

160. *In re United States*, Nos. 08-9131-MC, 089147-MC, 2009 WL 3416240, at *3-4 (D. Or. June 23, 2009).

161. *Id.* at *13 (quoting Google Privacy Policy, <http://www.google.com/privacypolicy.html> (last visited May 13, 2009)).

162. *Id.* at *11-13.

163. *Id.* at *15.

164. *Quon* Circuit, 529 F.3d at 905.

165. *See In re United States*, 2009 WL 3416240 at *12.

sent via Gmail into evidence.¹⁶⁶ The defendant successfully moved to suppress the evidence, and the court in *United States v. Cioffi* stated that the defendant had a reasonable expectation of privacy in the contents of his personal email account.¹⁶⁷

This case is also interesting because it highlights some of the privacy pitfalls inherent in cloud computing. The defendant had deleted his Gmail account before the government served Google with the search warrant.¹⁶⁸ Google originally responded to the search warrant by stating that the emails were gone because the defendant had deleted the account.¹⁶⁹ “On the eve of trial,” however, Google located a version of the defendant’s account as it existed nearly two years prior to the date of the warrant and promptly sent the contents to the government.¹⁷⁰ This illustrates the concern that once data is in the cloud, a person loses the ability to completely control access to it.¹⁷¹

As described in Section III.A., data that is stored in the cloud comprises more than simple communications like text messages or emails. The possible information stored with third parties in the cloud includes personal identification data, photos, videos, recordings, documents, software source and object code, and financial information. Furthermore, the Supreme Court has stated that information voluntarily revealed to third parties loses privacy protection, the third-party doctrine.¹⁷² Thus the question becomes whether

166. *United States v. Cioffi*, No. 08-CR-415, 2009 WL 3738314, at *1 (E.D.N.Y. Nov. 2, 2009).

167. *Id.* at *3 n.7, *12 (“The government does not dispute that [the defendant] had a reasonable expectation of privacy in the contents of his personal email account.”).

168. *Id.* at *2.

169. *Id.*

170. *Id.*

171. See Alan Weissberger, *ACLU Northern CA: Cloud Computing—Storm Warning for Privacy?* VIODI (February 13, 2009), <http://viodi.com/2009/02/13/aclu-northern-ca-cloud-computing-storm-warning-for-privacy/>, stating:

Once this information is located in one or more databases “in the cloud”, it may be accessed and used in ways that individuals never envisioned or intended, and with little oversight. . . . And with the lengthy data retention periods and ineffective deletion procedures of many companies, we may find it very difficult to remove their data once it is uploaded.

Id.; see also Brian Kane & Brett T. Delange, *A Tale of Two Internets: Web 2.0 Slices, Dices, and is Privacy Resistant*, 45 IDAHO L. REV. 317, 346 (2009) (“But the stark reality is that users have to understand that each piece of their lives uploaded onto the Internet becomes a lost piece of privacy.”).

172. See David A. Couillard, *supra* note 134 at 2207–08 (“However, when the object of a search—tangible or not—is voluntarily turned over to a third party, the Supreme Court has held that a person loses their reasonable expectation of privacy in that object.”); Orin S. Kerr, *supra* note 38 at 563 (indicating that Supreme Court precedent holds that information

the reasoning that the Ninth Circuit employed in *Quon*, concluding that text messages and emails are protected under the Fourth Amendment, renders the third-party doctrine inapplicable to information stored in a cloud.¹⁷³

As explained in Section I.C., the three principal cases espousing the third-party doctrine in the context of tangible communications are *Smith*, *Couch*, and *Miller*, also known as the business records cases.¹⁷⁴ The common thread in these cases is that the information was revealed to a third party to accomplish a task commissioned by the revealer.¹⁷⁵ Thus, the third party necessarily used the communicated information, and it is the third party's active use that exhausted any reasonable expectation of privacy in the communication.¹⁷⁶ Privacy law should distinguish between cloud-based communications that convey information to the service provider (or infrastructure provider) for the provider's use and those that convey information to the provider for mere reception and storage.¹⁷⁷ There is a reasonable expectation of privacy in the latter, and the cloud service

voluntarily revealed to third parties eliminates Fourth Amendment protection for that information). For more information on the third-party doctrine, see *supra* Section II.C.

173. That this information may be "communicated" only to the person who put the information in the cloud in the first place does not alter this analysis. If a person stores data in the cloud that only he or she uses, it does not cease to be a communication in this analysis. One of the primary emails of concern in *Cioffi* was an email the defendant sent to himself containing a running diary of some thoughts, and the fact that it was sent to himself and to no one else did not alter the conclusion that there was a reasonable expectation of privacy in the content of the communication. See *Cioffi*, 2009 WL 3738314 at *2–3.

174. *Smith v. Maryland*, 442 U.S. 735 (1979) (concluding that there was no reasonable expectation of privacy in the telephone numbers a person dialed); *United States v. Miller*, 425 U.S. 435 (1976) (stating that there was no reasonable expectation of privacy in financial records turned over to a bank); *Couch v. United States*, 409 U.S. 322 (1973) (holding that tax records given to an accountant were not protected by the Fourth Amendment because they were given to a third party). See *supra* Section II.C.

175. For a more lengthy discussion of various forms of communication, such as telegrams, and their Fourth Amendment protections, see Alexander Scolnick, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 *FORDHAM L. REV.* 349 (2009).

176. See Alyssa H. DaCunha, Note, *TXTS R SAFE 4 2DAY: Quon v. Arch Wireless and the Fourth Amendment Applied to Text Messages*, 17 *GEO. MASON L. REV.* 295, 326–27 (2009) ("The significant factor distinguishing the business records cases from a case such as *Quon* is that, unlike stored text messages, each of the documents at issue in the business records cases was of 'independent interest' to the business that received the documents from the individual.").

177. For an alternate approach considering four different models of Fourth Amendment, see R. Bruce Wells, Comment, *The Fog of Cloud Computing: Fourth Amendment Issues Raised by the Blurring of Online and Offline Content*, 12 *U. PA. J. CONST. L.* 223, 237–39 (2009).

provider's ability to review the information should not diminish this expectation.¹⁷⁸

2. *Cloud Computing Privacy in the Public Sector Workplace*

Turning to cloud computing in the public sector employment context, another factor must enter into the equation in calculating privacy expectations in cloud data. The “operational realities” of the workplace may diminish an expectation of privacy in data stored with third parties to the point of making it unreasonable. This is a fact-intensive inquiry dependent on the specific details of each public sector workplace, but *Quon* provides a sample analysis.¹⁷⁹ The Supreme Court has the opportunity to provide further guidance when it reviews *Quon*, which will provide a clearer framework for privacy policies in the workplace.¹⁸⁰

In *Quon*, the OPD issued pagers to SWAT officers and paid for the base contract, but officers paid for the overages they incurred.¹⁸¹ The City had a policy that governed the use of the pagers, but the administrator of the pagers instituted a practice that contravened it.¹⁸² These factual scenarios are subject to a myriad of variations in different public employment contexts, and it may not be clear from the outset how a court would decide a particular situation. With the disagreement over how to weight each factor in the analysis, the Supreme Court will have the opportunity to help employers and employees by providing some clarity.¹⁸³

The guidance from *Quon* directs public sector employers to take affirmative steps to control employee conduct. From an employer's perspective, the lesson to be learned from *Quon* is to be ever-vigilant in overseeing privacy policies because courts may find them nullified due to lack of enforcement or contrary policies informally introduced by management.¹⁸⁴ Employers migrating to cloud computing must establish business practices that control data, including which employees can access

178. A result that would be consistent with the holding of *Quon*. See *Quon* Circuit, 529 F.3d 892, 905–06 (9th Cir. 2008).

179. See *Id.* at 906–07.

180. See Brief of Petitioners at i, *City of Ontario v. Quon*, No. 08-1332 (U.S. Feb. 5, 2010) (listing the questions presented to the Court).

181. *Id.* at 895, 897.

182. *Id.* at 897.

183. See Brief of Petitioners at i, *City of Ontario v. Quon*, No. 08-1332 (U.S. Feb. 5, 2010) (listing the questions presented to the Court). Compare *Quon En Banc*, 554 F.3d 769, 770–71 (9th Cir. 2009) (concurring opinion) with *Id.* at 776–77 (dissenting opinion).

184. See *Quon* Circuit, 529 F.3d at 907.

the cloud computing service, procedures for removing employee access, and policies regarding personal use of cloud resources.

For the courts, the analysis of privacy interests in the public sector workplace should not differ in principle from the analysis to determine whether there is a reasonable expectation of privacy in the first place. For data stored with third parties, once the court establishes that an employee has a subjective expectation of privacy, the court should proceed to analyze the workplace environment to decide whether the expectation is objectively reasonable. This is accomplished by inquiring whether the public sector employer has access to the employee's data, notwithstanding the third party's ability to access the data. An employer can demonstrate access by showing that its policies and monitoring practices establish an open door for investigating an employee's data stored in the cloud. In this way, the employer is analogous to a third party and the analysis proceeds along the lines of the third-party doctrine, requiring a court to decide whether the communication is directed to the third party or provided to them (the employer in this case) to accomplish an agreed upon task. In the employment context, the agreed upon task is the efficient and effective monitoring of the workplace. Any data stored in the cloud that affects how an employer manages the workplace would then lose any privacy protection. Data that does not fall in this category, such as personal email sent from a work email account as permitted by the public sector employer, would enjoy Fourth Amendment protection.¹⁸⁵

Analyzing the facts in *Quon* using the proposed framework, the result would remain largely unchanged with one exception. The informal policy would serve to eliminate the OPD as a possible third party with access to Quon's text messages because it destroys the employer's access to the text messages. Quon would then have an objectively reasonable expectation of privacy in the contents of his messages even after considering the "operational realities" of the workplace.

V. CONCLUSION

When the Supreme Court reviews *Quon* it will be in a similar position as it was when it decided *Katz*. Prior to *Katz*, Fourth Amendment jurisprudence did not indicate that there was a reasonable expectation of privacy in

185. See Scolnik, *supra* note 175, at 393–97. Of course, even where there is a reasonable expectation of privacy, an employer may show that the search was reasonable and would not run afoul of the Fourth Amendment or similar state-provided privacy protections. See *Quon* Circuit, 529 F.3d at 906.

telephone calls because there was no physical intrusion, but the Supreme Court held that a caller who entered a phone booth had a reasonable expectation that the contents of his telephone call would not be “broadcast to the world.”¹⁸⁶ The Court recognized that the Fourth Amendment should provide protection for telephone conversations because “[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.”¹⁸⁷ By granting certiorari in *Quon*, the Supreme Court is poised to reinforce *Katz*’s interpretation of the Constitution by recognizing that text messaging and email have also come to play a “vital role” in private communication. Failing to recognize a reasonable expectation of privacy in communications such as text messages and emails stored with third parties would be a step backwards in Fourth Amendment jurisprudence. Affirming the Ninth Circuit’s holding in *Quon* will bring Fourth Amendment protection into the twenty-first century and protect the information that will inevitably migrate to the cloud.

The Supreme Court could also provide more guidance for courts in analyzing privacy for electronic communication in the workplace. By extending the third-party doctrine and its logical implications to the employment context, the Supreme Court could provide more certainty for employers rather than allowing for various, but undefined, “operational realities” to affect a court’s analysis.

186. *Katz v. United States*, 389 U.S. 347, 352 (1967).

187. *Id.*