

2009

Quon v. Arch Wireless: The Ninth Circuit Correctly Assess Fourth Amendment Privacy Interests in Workplace Text-Messaging

Marvin A. Liang

Follow this and additional works at: <https://scholar.smu.edu/scitech>

Recommended Citation

Marvin A. Liang, *Quon v. Arch Wireless: The Ninth Circuit Correctly Assess Fourth Amendment Privacy Interests in Workplace Text-Messaging*, 12 SMU SCI. & TECH. L. REV. 231 (2009)
<https://scholar.smu.edu/scitech/vol12/iss3/4>

This Article is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit <http://digitalrepository.smu.edu>.

Quon v. Arch Wireless: The Ninth Circuit Correctly Assesses Fourth Amendment Privacy Interests in Workplace Text-Messaging

*Marvin A. Liang**

A. INTRODUCTION

Wireless providers process over seventy-five billion text-messages every month in the United States.¹ Text-messaging is often used for personal communication, but its ability to transmit information with instantaneous speed has also created an ideal medium in business settings.² Due to the sheer volume of these daily transmissions, text-messaging creates problems of regulation, security, and privacy for both employers and employees.³

Recently, the United States Court of Appeals for the Ninth Circuit decided *Quon v. Arch Wireless Operating Co.* on first impression and addressed issues of the Stored Communications Act (hereinafter SCA) and the Fourth Amendment right to be protected against unreasonable searches and seizures regarding the content of employees' text-messages on devices issued by an employer.⁴ The court's ruling protected the employee's right to a reasonable expectation of privacy with respect to the content of his transmitted text-messages.⁵ Nevertheless, the opinion is narrowly tailored to the facts of the case, and the court's rationale provides precedent that calls for a careful examination to prevent future abuse in this area.

* Marvin A. Liang is a May 2010 candidate for Juris Doctor at Southern Methodist University Dedman School of Law. He graduated from the University of Texas at Austin with a Bachelor of Arts in the Plan II Honors Program and a minor in Biology.

1. CTIA – The Wireless Association, Wireless Quick Facts, <http://www.ctia.org/content/index.cfm/AID/10323> (data current as of June 2008) (last visited Sept. 25, 2009).
2. Text-messaging is also known as SMS, or Short Message Service. *Util. Consumers' Action Network v. Sprint Solutions, Inc.*, No. C07-2231RJB, 2008 U.S. Dist. LEXIS 53075, at *12 n.7 (S.D. Cal. July 10, 2008). Text-messaging “enables short messages of generally no more than 140-160 characters in length to be sent and transmitted from a cell phone. Unlike [standard, one-way] paging, but similar to e-mail, short messages are stored and forwarded at SMS centers, which means a person can retrieve messages later if the person is not immediately available to receive them.” *Id.* at *12-13 n.7.
3. See William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 EMP. RTS. & EMP. POL'Y J. 49, 50 (2008).
4. See *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892 (9th Cir. 2008).
5. *Id.* at 909.

B. FACTUAL BACKGROUND

On October 24, 2001, Arch Wireless contracted with the City of Ontario, California (hereinafter City) to provide wireless text-messaging services. Arch Wireless provided alphanumeric pagers to the City, which distributed the devices to their employees, including Sergeants Jeff Quon and Steve Trujillo.

Although the City did not have an official policy for text-messaging, it did have a general "Computer Usage, Internet and E-mail Policy" (hereinafter Policy), providing that employees were to use City-owned electronic systems and associated equipment for official business purposes only.⁶ Additionally, the Policy stated that "[a]ccess to the Internet and the e-mail system is NOT confidential; and information produced either in hard copy or electronic form is considered City property."⁷

In 2000, prior to receiving their pagers, Quon and Trujillo signed an "Employee Acknowledgment," which contained language similar to that of the general technology-use Policy of the Ontario Police Department (hereinafter "Department").⁸ In 2002, Quon attended a Department meeting where a senior officer informed the employees that messages on the new pagers would be considered e-mail and would therefore fall under the City's policies for monitoring and auditing.

Although the City did not have an official policy governing the use of the pagers, the contract with Arch Wireless allowed 25,000 characters of use per month for each device before a penalty overage fee would apply. Furthermore, the City's informal policy was that Lieutenant Steve Duke would merely collect overage fees from an employee in violation of excessive pager use rather than conduct an audit of the messages. This happened "three or four times" with Officer Quon, and in each of those instances, Quon paid the City for the extra charges.⁹

In August 2002, Duke became 'tired of being a bill collector' so Chief Lloyd Scharf ordered a review of the text-message transcripts 'to determine if the messages were exclusively work related, which would require an increase in the number of characters officers were permitted, as had occurred in the past, or if they were using the pagers for personal matters.'¹⁰

Since the City officials were unable to directly access the messages, they contacted Arch Wireless, who delivered transcripts of the messages to the Department for auditing. Pursuant to its investigation, the Department discovered that many messages on Quon's pager were "personal in nature

6. *Id.*

7. *Id.* at 896 (emphasis in original).

8. *Id.*

9. *Id.* at 897.

10. *Id.*

and often sexually explicit.”¹¹ The court also noted that the text-messages “were directed to and received from, among others, the other Appellants.”¹²

C. DESCRIPTION OF PLAINTIFF’S CLAIM

The City employees initially filed suit in the United States District Court for the Central District of California in 2004, naming Arch Wireless, the City, city officials, and the Department as the defendants.¹³ The employees alleged violations of 18 U.S.C. section 2702 of the Stored Communications Act (SCA) and California Penal Code section 629.86, as well as an invasion of privacy violating Article I, Section 1 of the California constitution.

D. PROCEDURAL AND SUBSTANTIVE HISTORY

The trial court held that Arch Wireless did not violate the SCA because the company acted as a “remote computing service” (hereinafter RCS) rather than an “electronic communication service” (hereinafter ECS) under SCA section 2702(a).¹⁴ Therefore, the company committed no injury when it released the transcripts of the text-messages to the City. The trial court also held that the government defendants did not violate the Fourth Amendment of the United States Constitution, which prohibits unreasonable searches and seizures. The court reasoned that a plaintiff must show a reasonable expectation of privacy in his text-messages and show that the government’s search and seizure was unreasonable under the circumstances to prevail on a Fourth Amendment claim.¹⁵ The district court looked to Lieutenant Duke’s informal policy of not auditing pagers if the employee would pay the overage fees and held, as a matter of law, that the employees had a reasonable expectation of privacy regarding their text-messages.¹⁶ Looking at the issue of reasonableness, the district court held a jury trial to examine if Chief Scharaf’s intent was to uncover misconduct or to determine the suitability of the 25,000 character limit for each pager.¹⁷ Since the jury found that Chief Scharaf’s intent

11. *Id.* at 898.

12. *Id.*

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

14. *Id.* at 1129.

15. *Id.* at 1139; *see O’Connor v. Ortega*, 480 U.S. 709, 725-26 (1987) (stating that “public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances.”).

16. *Quon*, 445 F. Supp. 2d at 1144.

17. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 899 (9th Cir. 2008).

was to determine the efficacy of the character limit, the court absolved all of the government defendants of liability for the text-message search.¹⁸

In December 2006, plaintiffs filed a Federal Rule of Civil Procedure 59(e) motion to amend or alter the judgment and a 59(a) motion for new trial.¹⁹ The district court denied each of these motions, and the plaintiffs appealed to the United States Court of Appeals for the Ninth Circuit.²⁰

E. COURT OF APPEAL HOLDING AND OVERVIEW OF RATIONALE

The Ninth Circuit first examined the SCA claim and disagreed with the district court that Arch Wireless acted as an RCS for the City.²¹ Therefore, since Arch Wireless was providing an “electronic communication service” for the City, the company violated the SCA when it knowingly released the text-message transcripts to the City.²² Since the court of appeals agreed with the Appellants, it held that the district court erred to grant summary judgment in favor of Arch Wireless.²³ The court of appeals then turned to the Fourth Amendment claim and held that the text-message search violated the plaintiffs’ Fourth Amendment rights as well as their privacy rights under the California constitution.²⁴ The search was found to be unreasonable because the Department could have used alternative and less intrusive ways to conduct its investigation.²⁵ Finally, the Ninth Circuit held that the law entitled Chief Scharf to qualified immunity, but the California constitution did not afford statutory-immunity protection to either the City or the Department.²⁶

F. COURT’S RATIONALE

The court began its analysis by examining section 2702 of the SCA, which governs liability for both ECS and RCS providers.²⁷ According to the SCA’s plain language, an ECS is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communica-

18. *Id.*

19. *Quon v. Arch Wireless Operating Co.*, 2006 WL 4791384 (C.D. Cal. Dec. 7, 2006).

20. *See Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 899 (9th Cir. 2008).

21. *Id.* at 900.

22. *Id.* at 903.

23. *Id.* at 900.

24. *Id.*

25. *Id.* at 909.

26. *Id.* at 910.

27. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008).

tions.”²⁸ The court stated that, on its face, this definition seemed to describe the text-messaging services Arch Wireless provided to the City.²⁹

On the other hand, an RCS is defined in the SCA as “the provision to the public of computer storage or processing services by means of an electronic communications system.”³⁰ The court noted that Arch Wireless did not provide “computer storage” to the city, nor did it provide any “processing services.”³¹

To bolster these interpretations, the court turned to the legislative history of the SCA.³² A 1986 Senate report clarifies “data communication” to include services involving cellular phones and paging devices.³³ In the same report, “storage” is analogized to when “physicians and hospitals maintain medical files in offsite data banks.”³⁴ “Processing information” is comparable to when “businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services.”³⁵ The Ninth Circuit noted that neither of these examples, which illustrate functions of an RCS, is accurate in describing the services that Arch Wireless provided as a company.³⁶

To dispose of any remaining notion that Arch Wireless is not an ECS, the court cited its own decision in *Theofel v. Farey Jones*.³⁷ In that case, NetGate was an e-mail service provider, undisputedly an ECS, which retained e-mails on its servers for “backup protection.”³⁸ The court notes that Arch Wireless and NetGate supplied closely analogous services.³⁹ Both companies provided a means to transmit electronic communication from one user to another, and both companies maintained a copy of delivered messages on their server.⁴⁰ The court held that the similarities between the

28. 18 U.S.C. § 2510(15) (2006).

29. *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 901 (9th Cir. 2008).

30. 18 U.S.C. § 2711(2) (2006).

31. *Quon*, 529 F.3d at 901.

32. *Id.*

33. S. Rep. No. 99-541, at 2-3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556 (listing data communication providers to include “large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices”).

34. *Id.*

35. *Id.* at 10-11.

36. *Quon*, 529 F.3d at 902.

37. *See Theofel v. Farey-Jones*, 359 F.3d 1066, 1070 (9th Cir. 2004).

38. *See id.* at 1075.

39. *Quon*, 529 F.3d at 902.

40. *Id.*

companies in business function and operation support categorizing Arch Wireless as an ECS.⁴¹

As a result of analyzing the plain language of the SCA, legislative history of the SCA, and federal case law, the Ninth Circuit held that Arch Wireless was an ECS.⁴² Although both an ECS and RCS can release private information to “an addressee or intended recipient of such communication, only an RCS can release such information with the lawful consent of the subscriber.”⁴³ It is undisputed that the City was only a subscriber and not an addressee or intended recipient, so Arch Wireless violated the SCA when it knowingly turned over the transcripts of text-messages to the City.⁴⁴ Consequently, the district court erred when it granted summary judgment in favor of Arch Wireless and determined that judgment in favor of Appellants was appropriate as a matter of law.⁴⁵

The court then turned to Appellant’s Fourth Amendment claim to examine if “users of text-messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text-messages stored on the service provider’s network.”⁴⁶ The court answered this question in the affirmative⁴⁷ after examining the “totality of the circumstances to determine whether a search is reasonable.”⁴⁸

Since Quon signed the Department’s general computer usage policy, he should not have an expectation of privacy regarding his pager transmissions.⁴⁹ However, the “operational reality” at the Department created a different situation.⁵⁰ Lieutenant Duke had made it clear that he would not audit pagers as long as an employee would pay the overage charges, and Quon had exceeded his usage “three or four times” without an audit after paying the extra fees.⁵¹ The court looked to the fact that Duke was “in charge of the

41. *Id.* at 903.

42. *Id.*

43. *Id.* at 900; *see* 18 U.S.C. §§ 2702(b)(1)-(3) (West 2006).

44. *See Quon*, 529 F.3d at 903.

45. *Id.*

46. *Id.*

47. *Id.*

48. *United States v. Kriesel*, 508 F.3d 941, 947 (9th Cir. 2007) (stating that “the touchstone of the Fourth Amendment is reasonableness.”).

49. *See Quon*, 529 F.3d at 906; *see Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002) (stating that a company destroyed any reasonable expectation of privacy for its employee when the company announced that it “could inspect the laptops that it furnished for the use of its employees.”).

50. *Quon*, 529 F.3d at 907.

51. *Id.*

paggers, and it was reasonable for Quon to rely on the policy—formal or informal—that Lieutenant Duke established and enforced.”⁵²

The court then examined whether the text-message search itself was reasonable and held that it was not.⁵³ Regarding the scope of a search, the court stated, “[i]f less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceed[s] that necessary for the government’s legitimate purposes,” a search is unreasonable and violates Fourth Amendment privacy rights.⁵⁴ The Ninth Circuit disagreed with the lower court’s statement that less-intrusive alternatives to verify why Quon exceeded his allotted monthly pager usage did not exist.⁵⁵

The court turned to the issue of whether Chief Scharf should be granted qualified immunity, even if the court concluded that he violated Appellant’s Fourth Amendment privacy rights.⁵⁶ Using a two-step inquiry,⁵⁷ the Ninth Circuit held that the Chief was entitled to qualified immunity because “at the time of the search, there was no clearly established law regarding whether users of text-messages that are archived, however temporarily, by the service provider have a reasonable expectation of privacy in those messages.”⁵⁸

52. *Id.*

53. *Id.* at 908.

54. *Id.*; *Schowengerdt v. Gen. Dynamics Corp.*, 823 F.2d 1328, 1336 (9th Cir. 1987).

55. *Quon*, 529 F.3d at 909 (stating that “the 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.”).

56. *Id.*

57. *Saucier v. Katz*, 533 U.S. 194, 201 (2001) (explaining that the first part of the test is to view the facts in the light most favorable to the party asserting injury to see if the officer’s conduct violates a constitutional right, and if so, then the second part of the test asks for a determination of whether the right was clearly established.); *see also Pearson v. Callahan*, 129 S.Ct. 808 (2009) (reconsidering the Saucier procedure, and holding that, “while the sequence set forth therein is often appropriate, it should no longer be regarded as mandatory in all cases” but stating that, “Saucier was correct in noting that the two-step procedure promotes the development of constitutional precedent and is especially valuable for questions that do not frequently arise in cases in which a qualified immunity defense is unavailable”).

58. *Quon*, 529 F.3d at 910.

Finally, the court dismissed the City and the Department's claim of statutory immunity from liability.⁵⁹ Lieutenant Duke's informal policy allowed officers to use the Department pagers for personal use and exceed the monthly character allotment as long as excess charges were paid.⁶⁰ Keeping this in mind, the court stated that Quon could not have committed any misconduct, which would be a prerequisite to initiate a formal proceeding.⁶¹ The Ninth Circuit then held that the City and Department could not be entitled to statutory immunity in the absence of a proceeding.⁶²

G. CRITIQUE OF THE COURT'S APPROACH

In recent years, a rapid increase to use new technology in the workplace has created concerns of diminished personal privacy rights.⁶³ Generally, case law has centered on claims and issues related to e-mail, but this Ninth Circuit holding in *Quon v. Arch Wireless* has brought text-messaging to the forefront of discussion. As a case of first-impression, the Ninth Circuit's holding can be instructive as to where the law is headed. However, the opinion is also tailored to the specific facts and issues of the case, so a thorough analysis of the Ninth Circuit's reasoning is important for the future scenarios that may be closely analogous to this decision.

1. Stored Communications Act

The Ninth Circuit correctly decided the first issue that Arch Wireless violated the SCA. The text-messaging company provided a service that allowed users the ability to send or receive electronic communications, which fits the plain-meaning definition of an ECS.⁶⁴ Furthermore, the legislative history clearly demonstrates that Congress intended to address specific privacy issues in electronic communication with little ambiguity when it drafted the SCA.⁶⁵ Although the Senate Report was issued in 1986, the basic principles mentioned have remained the same, and the Report's explicit definitions

59. *Id.*

60. *Id.*

61. *Id.*

62. *Id.*; CAL. GOV'T CODE § 821.6 (2006) (stating that "[a] public employee is not liable for injury caused by his instituting or prosecuting any judicial or administrative proceeding within the scope of his employment, even if he acts maliciously and without probable cause.").

63. See generally Herbert, *supra* note 3 at 49.

64. See 18 U.S.C. § 2510(15) (2006) (stating that an ECS is "any service which provides to users thereof the ability to send or receive wire or electronic communications.").

65. See Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209-1212 (2004).

and examples allow Arch Wireless to properly be characterized as an ECS.⁶⁶ The Senate Report was also helpful to dismiss Arch Wireless' claim that its company was an RCS.⁶⁷

H. FOURTH AMENDMENT CLAIMS

The Ninth Circuit was also correct in holding that “users of text-messaging services such as those provided by Arch Wireless have a reasonable expectation of privacy in their text-messages stored on the service provider’s network.”⁶⁸ Although Quon had signed the Department’s electronic-use Policy, the court properly applied the reasonableness standard to the Fourth Amendment analysis, holding that the operational reality at the Department cleared Quon of liability.⁶⁹

The Ninth Circuit also correctly held that the text-message search itself was unreasonable. A search is unreasonable if less intrusive means are feasible, and the court listed several alternatives that could have been employed to verify the efficacy of the character limit.⁷⁰ Although some of the suggestions may have been feasible, such as asking “Quon to count the characters himself,” they would have been burdensome and inefficient since the usage had clearly gone over 25,000 characters.⁷¹ A more practical solution advocated by the court was to warn Quon that he was forbidden from using his pager for personal communication and to review his messages from that point forward to ensure the device was used for work-related purposes only.⁷²

Using the specific facts of the case, the Ninth Circuit properly held that Chief Scharf was entitled to qualified immunity because there was no clearly established law in this area.⁷³ The court granted the protection reluctantly as it explicitly reasoned that its decision was based on the lack of precedential law on this issue.⁷⁴ Therefore, future individuals facing a similar situation as Scharf may not obtain a similar outcome. Furthermore, the court correctly applied section 821.6 of the California Government Code— since Quon’s actions did not constitute misconduct and did not fall within the scope of the

66. See S. REP. NO. 99-541, *supra* note 33 at 3.

67. See *id.* (listing examples of RCS functions to include file storage and data processing, none of which describe the service that Arch Wireless provided to the City).

68. *Quon*, 529 F.3d at 904.

69. *Id.* at 907-08; *United States v. Kriesel*, 508 F.3d 941, 947 (9th Cir. 2007).

70. *Quon*, 529 F.3d at 908.

71. See *Quon v. Arch Wireless Operating Co.*, 445 F. Supp. 2d 1116, 1126 (C.D. Cal. 2006) (stating that the “transcripts for Quon’s pages tallied forty-six pages in length”).

72. See *Quon*, 529 F.3d at 909.

73. *Id.* at 910.

74. *Id.*

Code, the City and Department were not protected by statutory immunity.⁷⁵ These two holdings are narrowly tailored to the details of the present case, and therefore, they may not be directly applicable to another situation with dissimilar facts.

I. IMPLICATIONS OF THE COURT'S HOLDING

Immediately after the Ninth Circuit published this opinion, media coverage on the case seemed to imply a revolution in workplace wireless communications as a number of articles viewed the ruling as a tremendous victory for online privacy.⁷⁶ Information Week, a business technology publication, stated that, "Employees' text messages are private, even when transmitted on devices their companies pay for."⁷⁷ Although statements like these are technically true to a certain extent, they are misleading because *Quon* is limited to a specific set of facts and does not apply in every situation involving text-messages.

First, the court's holding that *Quon* had a reasonable expectation of privacy will only protect employees that work for public employers because the Fourth Amendment does not apply to private actors.⁷⁸ It is incorrect to state that employees that work for private companies enjoy the same protection. Second, public employers still have the right to monitor text-message transmissions on government-owned devices. If an employer has a monitoring policy in place but does not enforce it, the "operational reality" of the policy may defeat the later ability to monitor unannounced. Therefore, individuals in charge of workplace monitoring should never make representations to employees that an electronic resources policy will not be followed or will be loosely followed. The present case makes it clear that employees should be continually and repeatedly reminded of precise monitoring policies and privacy disclaimers so they are on notice that their text-messages can and will be checked for improper usage.

75. See CAL. GOV'T CODE § 821.6 (2006); See *Quon*, 529 F.3d at 910.

76. See, e.g., Maura Dolan, LOS ANGELES TIMES, Jun. 19, 2008, available at <http://articles.latimes.com/2008/jun/19/local/me-text19>.

77. K.C. Jones, *Court Rules Employee Text Messages Are Private*, INFORMATION WEEK, Jun. 19, 2008, available at <http://www.informationweek.com/news/security/privacy/showArticle.jhtml?articleID=208700666>.

78. See U.S. CONST. amend. IV; see *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (stating that, "This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.").

J. OVERVIEW OF THE CRITIQUE

Aside from protecting privacy rights, this holding may be a double-edged sword. With the rising trend of company-issued electronic devices, it is likely that more and more messages unrelated to official business matters are sent every day. Public entities taking note of this decision should strengthen their auditing policies, such as implementing regular monitoring, to avoid the problems that Arch Wireless and the Ontario Police Department were faced with. On the other hand, a savvy employee who realizes their employer has an “informal monitoring policy” similar to the one in *Quon* may carefully be able to avoid their communication transcripts being analyzed. This decision does not afford broad privacy protections for text-messaging because the holding is tailored to the facts of the case. However, as a case of first-impression, “[t]he extent to which the Fourth Amendment provides protection for the contents of electronic communications in the Internet age is an open question.”⁷⁹ Indisputably, the holding in *Quon* is at the forefront of Internet and electronic jurisprudence, and it is likely to help shape other decisions in this area of law.

79. *Quon*, 529 F.3d at 904.

