JERILYN QUON; APRIL FLORIO; JEFF QUON; STEVE TRUJILLO
v.
ARCH WIRELESS OPERATING COMPANY, INCORPORATED; CITY OF ONTARIO; LLOYD SCHARF; ONTARIO POLICE DEPARTMENT; DEBBIE GLENN

No. 07-55282

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

2008 U.S. App. LEXIS 12766

June 18, 2008, Filed

WARDLAW, Circuit Judge:

This case arises from the Ontario Police Department's review of text messages sent and received by Jeff Quon, a Sergeant and member of the City of Ontario's SWAT team. We must decide whether (1) Arch Wireless Operating Company Inc., the company with whom the City contracted for text messaging services, violated the Stored Communications Act, *18 U.S.C. §§ 2701-2711 (1986)*; and (2) whether the City, the Police Department, and Ontario Police Chief Lloyd Scharf violated Quon's rights and the rights of those with whom he "texted"--Sergeant Steve Trujillo, Dispatcher April Florio, and his wife Jerilyn Quon --under the Fourth Amendment to the United States Constitution and Article I, Section 1 of the California Constitution.

I. FACTUAL BACKGROUND

On October 24, 2001, Arch Wireless ("Arch Wireless") contracted to provide wireless text-messaging services for the City of Ontario. The City received twenty two-way alphanumeric pagers, which it distributed to its employees, including Ontario Police Department ("OPD" or "Department") Sergeants Quon and Trujillo, in late 2001 or early 2002.

According to Steven Niekamp, Director of Information Technology for Arch Wireless:

> A text message originating from an Arch Wireless two-way alphanumeric text-messaging pager is sent to another two-way text-messaging pager as follows: The message leaves the originating pager via a radio frequency transmission. That transmission is received by any one of many receiving stations, which are owned by Arch Wireless. Depending on the location of the receiving station, the message is then entered into the Arch Wireless computer network either by wire transmission or via satellite by another radio frequency transmission. Once in the Arch Wireless computer network, the mes-

> sage is sent to the Arch Wireless computer server. Once in the server, a copy of the message is archived. The message is also stored in the server system, for a period of up to 72 hours, until the recipient pager is ready to receive delivery of the text message. The recipient pager is ready to receive delivery of a message when it is both activated and located in an Arch Wireless service area. Once the recipient pager is able to receive delivery of the text message, the Arch Wireless server retrieves the stored message and sends it, via wire or radio frequency transmission, to the transmitting station closest to the recipient pager. The transmitting stations are owed [sic] by Arch Wireless. The message is then sent from the transmitting station, via a radio frequency transmission, to the recipient pager where it can be read by the user of the recipient pager.

The City had no official policy directed to text-messaging by use of the pagers. However, the City did have a general "Computer Usage, Internet and E-mail Policy" (the "Policy") applicable to all employees. The Policy stated that "[t]he use of City-owned computers and all associated equipment, software, programs, networks, Internet, e-mail and other systems operating on these computers is limited to City of Ontario related business. The use of these tools for personal benefit is a significant violation of City of Ontario Policy." The Policy also provided:

> C. Access to all sites on the Internet is recorded and will be periodically reviewed by the City. The City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.
>
> D. Access to the Internet and the e-mail system is **not** confidential; and information produced either in hard copy or in electronic form is considered City property. As such, these systems should not be used for personal or confidential communications. Deletion of e-mail or other electronic information may not fully delete the information from the system.
>
> E. The use of inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail system will not be tolerated.

In 2000, before the City acquired the pagers, both Quon and Trujillo had signed an "Employee Acknowledgment," which borrowed language from the general Policy, indicating that they had "read and fully understand the City of Ontario's Computer Usage, Internet and E-mail policy." The Employee Acknowledgment, among other things, states that "[t]he City of Ontario reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Two years later, on April 18, 2002, Quon attended a meeting during which Lieutenant Steve Duke, a Commander with the Ontario Police Department's Administration Bureau, informed all present that the pager messages "were considered e-mail, and that those messages would fall under the City's policy as public information and eligible for auditing." Quon "vaguely recalled attending" this meeting, but did not recall Lieutenant Duke stating at the meeting that use of the pagers was governed by the City's Policy.

Although the City had no official policy expressly governing use of the pagers, the City did have an informal policy governing their use. Under the City's contract with Arch Wireless, each

pager was allotted 25,000 characters, after which the City was required to pay overage charges. Lieutenant Duke "was in charge of the purchasing contract" and responsible for procuring payment for overages. He stated that "[t]he practice was, if there was overage, that the employee would pay for the overage that the City had. . . . [W]e would usually call the employee and say, 'Hey, look, you're over X amount of characters. It comes out to X amount of dollars. Can you write me a check for your overage[?]' "

The informal policy governing use of the pagers came to light during the Internal Affairs investigation, which took place after Lieutenant Duke grew weary of his role as bill collector. In a July 2, 2003 memorandum entitled "Internal Affairs Investigation of Jeffery Quon," (the "McMahon Memorandum") OPD Sergeant Patrick McMahon wrote that upon interviewing Lieutenant Duke, he learned that early on

> Lieutenant Duke went to Sergeant Quon and told him the City issued two-way pagers were considered e-mail and could be audited. He told Sergeant Quon it was not his intent to audit employee's [sic] text messages to see if the overage is due to work related transmissions. He advised Sergeant Quon he could reimburse the City for the overage so he would not have to audit the transmission and see how many messages were non-work related. Lieutenant Duke told Sergeant Quon he is doing this because if anybody wished to challenge their overage, he could audit the text transmissions to verify how many were non-work related. Lieutenant Duke added the text messages were considered public records and could be audited at any time.

For the most part, Lieutenant Duke agreed with McMahon's characterization of what he said during his interview. Later, however, during his deposition, Lieutenant Duke recalled the interaction as follows:

> I think what I told Quon was that he had to pay for his overage, that I did not want to determine if the overage was personal or business unless they wanted me to, because if they said, "It's all business, I'm not paying for it," then I would do an audit to confirm that. And I didn't want to get into the bill collecting thing, so he needed to pay for his personal messages so we didn't--pay for the overage so we didn't do the audit. And he needed to cut down on his transmissions.

According to the McMahon Memorandum, Quon remembered the interaction differently. When asked "if he ever recalled a discussion with Lieutenant Duke that if his textpager went over, his messages would be audited . . . Sergeant Quon said, 'No. In fact he [Lieutenant Duke] said the other, if you don't want us to read it, pay the overage fee.' "

Quon went over the monthly character limit "three or four times" and paid the City for the overages. Each time, "Lieutenant Duke would come and tell [him] that [he] owed X amount of dollars because [he] went over [his] allotted characters." Each of those times, Quon paid the City for the overages.

In August 2002, Quon and another officer again exceeded the 25,000 character limit. Lieutenant Duke then let it be known at a meeting that he was "tired of being a bill collector with guys going over the allotted amount of characters on their text pagers." In response, Chief Scharf ordered Lieutenant Duke to "request the transcripts of those pagers for auditing purposes." Chief

Scharf asked Lieutenant Duke "to determine if the messages were exclusively work related, thereby requiring an increase in the number of characters officers were permitted, which had occurred in the past, or if they were using the pagers for personal matters. One of the officers whose transcripts [he] requested was plaintiff Jeff Quon."

City officials were not able to access the text messages themselves. Instead, the City e-mailed Jackie Deavers, a major account support specialist for Arch Wireless, requesting the transcripts. According to Deavers,

> I checked the phone numbers on the transcripts against the e-mail that I had gotten, and I looked into the system to make sure they were actually pagers that belonged to the City of Ontario, and they were. So I took the transcripts and put them in a manila envelope [and brought them to the City].

Deavers stated that she did not determine whether private messages were being released, though she acknowledged that, upon reviewing approximately four lines of the transcript, she had realized that the messages were sexually explicit. She also stated that she would only deliver messages to the "contact" on the account, and that she would not deliver messages to the "user" unless he was also the contact on the account. In this case, the "contact" was the City.

After receiving the transcripts, Lieutenant Duke conducted an initial audit and reported the results to Chief Scharf. Subsequently, Chief Scharf and Quon's supervisor, Lieutenant Tony Del Rio, reviewed the transcripts themselves. Then, in October 2002, Chief Scharf referred the matter to internal affairs "to determine if someone was wasting . . . City time not doing work when they should be." Sergeant McMahon, who conducted this investigation on behalf of Internal Affairs, enlisted the help of Sergeant Glenn, also a member of Internal Affairs. Sergeant McMahon released the McMahon Memorandum on July 2, 2003. According to the Memorandum, the transcripts revealed that Quon "had exceeded his monthly allotted characters by 15,158 characters," and that many of these messages were personal in nature and were often sexually explicit. These messages were directed to and received from, among others, the other Appellants.

II. PROCEDURAL BACKGROUND

On May 6, 2003, Appellants filed a Second Amended Complaint in the District Court for the Central District of California alleging, *inter alia*, violations of the Stored Communications Act ("SCA") and the *Fourth Amendment*. After the district court dismissed one of Appellants' claims against Arch Wireless pursuant to *Federal Rule of Civil Procedure 12(b)(6)*, all parties filed numerous rounds of summary judgment motions. On August 15, 2006, the district court denied Appellants' summary judgment motion in full, and granted in part and denied in part Appellees' summary judgment motions.

Appellants appeal the district court's holding that Arch Wireless did not violate the SCA, *18 U.S.C. §§ 2701-2711*. The district court found that Arch Wireless was a "remote computing service" under *§ 2702(a)*, and that it therefore committed no harm when it released the text-message transcripts to its "subscriber," the City.

Appellants also appeal the district court's resolution of their claims against the City, the Department, Scharf, and Glenn. Appellants argue that the City, the Department, and Scharf violated Appellants' *Fourth Amendment* rights to be free from unreasonable search and seizure pursuant

to *42 U.S.C. § 1983*, and that the City, Department, Scharf, and Glenn violated *Article I, Section 1 of the California Constitution*, which protects a citizen's right to privacy. [4] The district court addressed only the *Fourth Amendment* claim. [5] Relying on *O'Connor v. Ortega, 480 U.S. 709, 715, 725-26, 107 S. Ct. 1492, 94 L. Ed. 2d 714 (1987)*, the district court determined that to prove a *Fourth Amendment* violation, the plaintiff must show that he had a reasonable expectation of privacy in his text messages, and that the government's search or seizure was unreasonable under the circumstances. The district court held that, in light of Lieutenant Duke's informal policy that he would not audit a pager if the user paid the overage charges, Appellants had a reasonable expectation of privacy in their text messages as a matter of law. Regarding the reasonableness of the search, the district court found that whether Chief Scharf's intent was to uncover misconduct or to determine the efficacy of the 25,000 character limit was a genuine issue of material fact. If it was the former, the search was unreasonable; if it was the latter, the search was reasonable. Concluding that Chief Scharf was not entitled to qualified immunity on the *Fourth Amendment* claim, and that the City and the Department were not entitled to statutory immunity on the California constitutional privacy claim, the district court held a jury trial on the single issue of Chief Scharf's intent. The jury found that Chief Scharf's intent was to determine the efficacy of the character limit. Therefore, all defendants were absolved of liability for the search.

> 4 "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." *CAL. CONST. art. I, § 1*.
>
> 5 The district court limited its discussion to the *Fourth Amendment* because "the arguments lodged by the governmental defendants against plaintiffs' invasion of privacy claim and state constitutional claim are the same as those pressed against plaintiffs' *Fourth Amendment* claim . . . ."

On December 7, 2006, Appellants filed a motion to amend or alter the judgment pursuant to *Federal Rule of Civil Procedure 59(e)*, and a motion for new trial pursuant to *Rule 59(a)*. The district court denied each of these motions. Appellants timely appeal.

III. JURISDICTION AND STANDARD OF REVIEW

The district court had jurisdiction pursuant to *28 U.S.C. §§ 1331* and *1343*. We have jurisdiction over final judgments of the district courts pursuant to *28 U.S.C. § 1291*.

We review a district court's grant of summary judgment de novo. *Bagdadi v. Nazar, 84 F.3d 1194, 1197 (9th Cir. 1996)*. In reviewing the grant of summary judgment, we "must determine, viewing the evidence in the light most favorable to the nonmoving party, whether genuine issues of material fact exist and whether the district court correctly applied the relevant substantive law." *Id.*

IV. DISCUSSION

A. Stored Communications Act

Congress passed the Stored Communications Act in 1986 as part of the Electronic Communications Privacy Act. The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the *Fourth Amendment* does not address. *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, 1209-13 (2004)*. Generally, the SCA prevents "providers" of communication services from divulging private communications to certain entities and/or individuals. *Id. at 1213*. Appellants challenge the district court's finding that Arch Wireless is a "remote computing service" ("RCS") as opposed to an "electronic communication service" ("ECS") under the *SCA, §§ 2701-2711*. The district court correctly concluded that if Arch Wireless is an ECS, it is liable as a matter of law, and that if it is an RCS, it is not liable. However, we disagree with the district court that Arch Wireless acted as an RCS for the City. Therefore, summary judgment in favor of Arch Wireless was error.

Section 2702 of the SCA governs liability for both ECS and RCS providers. *18 U.S.C. § 2702(a)(1)-(2)*. The nature of the services Arch Wireless offered to the City determines whether Arch Wireless is an ECS or an RCS. As the Niekamp Declaration makes clear, Arch Wireless provided to the City a service whereby it would facilitate communication between two pagers--"text messaging" over radio frequencies. As part of that service, Arch Wireless archived a copy of the message on its server. When Arch Wireless released to the City the transcripts of Appellants' messages, Arch Wireless potentially ran afoul of the SCA. This is because both an ECS and RCS can release private information to, or with the lawful consent of, "an addressee or intended recipient of such communication," *id. § 2702(b)(1)*, *(b)(3)*, whereas only an RCS can release such information "with the lawful consent of . . . the subscriber." *Id. § 2702(b)(3)*. It is undisputed that the City was not an "addressee or intended recipient," and that the City was a "subscriber."

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id. § 2510(15)*. The SCA prohibits an ECS from "knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service," unless, among other exceptions not relevant to this appeal, that person or entity is "an addressee or intended recipient of such communication." *Id. § 2702(a)(1)*, *(b)(1)*, *(b)(3)*. "Electronic storage" is defined as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." *Id. § 2510(17)*.

An RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id. § 2711(2)*. Electronic communication system--which is simply the means by which an RCS provides computer storage or processing services and has no bearing on how we interpret the meaning of "RCS"--is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id. § 2510(14)*. The SCA prohibits an RCS from "knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service." Unlike an ECS, an RCS may release the contents of a communication with the lawful consent of a "subscriber." *Id. § 2702(a)(2)*, *(b)(3)*.

We turn to the plain language of the SCA, including its common-sense definitions, to properly categorize Arch Wireless. An ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *18 U.S.C. § 2510(15)*. On its face, this describes the text-messaging pager services that Arch Wireless provided. Arch Wireless provided a "service" that enabled Quon and the other Appellants to "send or receive . . . elec-

tronic communications," i.e., text messages. Contrast that definition with that for an RCS, which "means the provision to the public of computer storage or processing services by means of an electronic communications system." *Id. § 2711(2)*. Arch Wireless did not provide to the City "computer storage"; nor did it provide "processing services." By archiving the text messages on its server, Arch Wireless certainly was "storing" the messages. However, Congress contemplated this exact function could be performed by an ECS as well, stating that an ECS would provide (A) temporary storage incidental to the communication; and (B) storage for backup protection. *Id. § 2510(17)*.

This reading of the SCA is supported by its legislative history. The Senate Report identifies two main services that providers performed in 1986: (1) data communication; and (2) data storage and processing. First, the report describes the means of communication of information:

> [W]e have large-scale electronic mail operations, computer-to-computer data transmissions, cellular and cordless telephones, paging devices, and video teleconferencing . . . . [M]any different companies, not just common carriers, offer a wide variety of telephone and other communications services.

S. REP. NO. 99-541, at 2-3 (1986). Second,

> [t]he Committee also recognizes that computers are used extensively today for the storage and processing of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference. This information is processed for the benefit of the user but often it is maintained for approximately 3 months to ensure system integrity.

Id. at 3. Under the heading "Remote Computer Services," the Report further clarifies that term refers to the processing or storage of data by an off-site third party:

> In the age of rapid computerization, a basic choice has faced the users of computer technology. That is, whether to process data inhouse on the user's own computer or on someone else's equipment. Over the years, remote computer service companies have developed to provide sophisticated and convenient computing services to subscribers and customers from remote facilities. Today businesses of all sizes--hospitals, banks and many others--use remote computing services for computer processing. This processing can be done with the customer or subscriber using the facilities of the remote computing service in essentially a time-sharing arrangement, or it can be accomplished by the service provider on the basis of information supplied by the subscriber or customer. Data is most often transmitted between these services and their customers by means of electronic communications.

Id. at 10-11.

In the Senate Report, Congress made clear what it meant by "storage and processing of information." It provided the following example of storage: "physicians and hospitals maintain medical files in offsite data banks." Congress appeared to view "storage" as a virtual filing cabinet, which is not the function Arch Wireless contracted to provide here. The Senate Report also provided an example of "processing of information": "businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services." In light of the Report's elaboration upon what Congress intended by the term "Remote Computer Services," it is clear that, before the advent of advanced computer processing programs such as Microsoft Excel, businesses had to farm out sophisticated processing to a service that would process the information. *See* Kerr, *72 GEO. WASH. L. REV. at 1213-14*. Neither of these examples describes the service that Arch Wireless provided to the City.

Any lingering doubt that Arch Wireless is an ECS that retained messages in electronic storage is disposed of by *Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004)*. In *Theofel*, we held that a provider of e-mail services, undisputedly an ECS, stored e-mails on its servers for backup protection. *Id. at 1075*. NetGate was the plaintiffs' Internet Service Provider ("ISP"). Pursuant to a subpoena, NetGate turned over plaintiffs' e-mail messages to the defendants. We concluded that plaintiffs' e-mail messages--which were stored on NetGate's server after delivery to the recipient--were "stored 'for purposes of backup protection' . . . . within the ordinary meaning of those terms." *Id.* (citation omitted).

The service provided by NetGate is closely analogous to Arch Wireless's storage of Appellants' messages. Much like Arch Wireless, NetGate served as a conduit for the transmission of electronic communications from one user to another, and stored those communications "as a 'backup' for the user." *Id.* Although it is not clear for whom Arch Wireless "archived" the text messages--presumably for the user or Arch Wireless itself--it is clear that the messages were archived for "backup protection," just as they were in *Theofel*. Accordingly, Arch Wireless is more appropriately categorized as an ECS than an RCS.

Arch Wireless contends that our analysis in *Theofel* of the definition of "backup protection" supports its position. There, we noted that "[w]here the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages." *Id. at 1070*. Thus, the argument goes, Arch Wireless's permanent retention of the Appellants' text messages could not have been for backup purposes; instead, it must have been for storage purposes, which would require us to classify Arch Wireless as an RCS. This reading is not persuasive. First, there is no indication in the record that Arch Wireless retained a permanent copy of the text-messages or stored them for the benefit of the City; instead, the Niekamp Declaration simply states that copies of the messages are "archived" on Arch Wireless's server. More importantly, *Theofel's* holding--that the e-mail messages stored on NetGate's server after delivery were for "backup protection," and that NetGate was undisputedly an ECS--forecloses Arch Wireless's position.

We hold that Arch Wireless provided an "electronic communication service" to the City. The parties do not dispute that Arch Wireless acted "knowingly" when it released the transcripts to the City. When Arch Wireless knowingly turned over the text-messaging transcripts to the City, which

was a "subscriber," not "an addressee or intended recipient of such communication," it violated the SCA, *18 U.S.C. § 2702(a)(1)*. Accordingly, judgment in Appellants' favor on their claims against Arch Wireless is appropriate as a matter of law, and we remand to the district court for proceedings consistent with this holding.

B. *Fourth Amendment*

Appellants assert that they are entitled to summary judgment on their *Fourth Amendment* claim against the City, the Department, and Scharf, and on their California constitutional privacy claim against the City, the Department, Scharf, and Glenn. Specifically, Appellants agree with the district court's conclusion that they had a reasonable expectation of privacy in the text messages. However, they argue that the issue regarding Chief Scharf's intent in authorizing the search never should have gone to trial because the search was unreasonable as a matter of law. We agree.

"The 'privacy' protected by [*Article I, Section 1 of the California Constitution*] is no broader in the area of search and seizure than the 'privacy' protected by the *Fourth Amendment* . . . ." *Hill v. Nat'l Collegiate Ath. Ass'n, 7 Cal. 4th 1, 30 n.9, 26 Cal. Rptr. 2d 834, 865 P.2d 633 (1994)*. Accordingly, our analysis proceeds under the *Fourth Amendment to the United States Constitution*. The *Fourth Amendment* protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." *U.S. CONST. amend. IV*. "[T]he touchstone of the *Fourth Amendment* is reasonableness." *United States v. Kriesel, 508 F.3d 941, 947 (9th Cir. 2007)* (citing *Samson v. California, 547 U.S. 843, 126 S. Ct. 2193, 2201 n.4, 165 L. Ed. 2d 250 (2006))*. Under the "general *Fourth Amendment* approach," we examine "the totality of the circumstances to determine whether a search is reasonable." *Id.* "The reasonableness of a search is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." *United States v. Knights, 534 U.S. 112, 118-19, 122 S. Ct. 587, 151 L. Ed. 2d 497 (2001)* (internal quotation marks omitted).

"Searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the *Fourth Amendment*." *O'Connor, 480 U.S. at 715*. In *O'Connor*, the Supreme Court reasoned that "[i]ndividuals do not lose *Fourth Amendment* rights merely because they work for the government instead of a private employer." *Id. at 717*. However, the Court also noted that "[t]he operational realities of the workplace . . . may make *some* employees' expectations of privacy unreasonable." *Id.* For example, "[p]ublic employees' expectations of privacy in their offices, desks, and file cabinets . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation." *Id.* The Court recognized that, "[g]iven the great variety of work environments in the public sector, the question whether an employee has a reasonable **[*27]** expectation of privacy must be addressed on a case-by-case basis." *Id. at 718*.

Even assuming an employee has a reasonable expectation of privacy in the item seized or the area searched, he must also demonstrate that the search was unreasonable to prove a *Fourth Amendment* violation: "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct, should be judged by the standard of reasonableness under all the circumstances." *Id. at 725-26*. Under this standard, we must evaluate 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." *Id. at 726* (internal quotation marks omitted).

1. Reasonable Expectation of Privacy

The extent to which the *Fourth Amendment* provides protection for the contents of electronic communications in the Internet age is an open question. The recently minted standard of electronic communication via e-mails, text messages, and other means opens a new frontier in *Fourth Amendment* jurisprudence that has been little **[*28]** explored. Here, we must first answer the threshold question: Do 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? We hold that they do.

In *Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967)*, the government placed an electronic listening device on a public telephone booth, which allowed the government to listen to the telephone user's conversation. *Id. at 348*. The Supreme Court held that listening to the conversation through the electronic device violated the user's reasonable expectation of privacy. *Id. at 353*. In so holding, the Court reasoned, "One who occupies [a phone 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. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication." *Id. at 352*. Therefore, "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably **[*29]** relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the *Fourth Amendment*." *Id. at 353*.

On the other hand, the Court has also held that the government's use of a pen register--a device that records the phone numbers one dials--does not violate the *Fourth Amendment*. This is because people "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Smith v. Maryland, 442 U.S. 735, 742, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)*. The Court distinguished *Katz* by noting that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." *Id. at 741*.

This distinction also applies to written communications, such as letters. It is well-settled that, "since 1878, . . . the *Fourth Amendment's* protection against 'unreasonable searches and seizures' protects a citizen against the warrantless opening of sealed letters and packages addressed to him in order to examine the contents." *United States v. Choate, 576 F.2d 165, 174 (9th Cir. 1978)* (citing *Ex parte Jackson, 96 U.S. 727, 24 L. Ed. 877 (1877)*; *see also United States v. Jacobsen, 466 U.S. 109, 114, 104 S. Ct. 1652, 80 L. Ed. 2d 85 (1984)* **[*30]** ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy."). However, as with the phone numbers they dial, individuals do not enjoy a reasonable expectation of privacy in what they write on the outside of an envelope. *See United States v. Hernandez, 313 F.3d 1206, 1209-10 (9th Cir. 2002)* ("Although a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior" (citations omitted)).

Our Internet jurisprudence is instructive. In *United States v. Forrester*, we held that "e-mail . . . users have no expectation of privacy in the to/from addresses of their messages . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)*. Thus, we have extended the pen register and outside-of-envelope rationales to the "to/from" line of e-mails. But we have not ruled on whether **[*31]** persons have a reasonable expectation of privacy in the content of e-mails. Like the Supreme Court in *Smith*, in *Forrester* we explicitly noted that "e-mail to/from addresses . . . constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Id.* Thus, we concluded that "[t]he privacy interests in these two forms of communication [letters and e-mails] are identical," and that, while "[t]he contents may deserve *Fourth Amendment* protection . . . the address and size of the package do not." *Id. at 511*.

We see no meaningful difference between the e-mails at issue in *Forrester* and the text messages at issue here. [6] Both are sent from user to user via a service provider that stores the messages on its servers. Similarly, as in *Forrester*, we also see no meaningful distinction between text messages and letters. As with letters and e-mails, it is not reasonable to expect privacy in the information used to "address" a text message, such as the dialing of a phone number to send a message. However, users do have a reasonable expectation of privacy in the content of their text messages vis-a-vis the service provider. *Cf. United States v. Finley, 477 F.3d 250, 259 (5th Cir. 2007)* (holding that defendant had a reasonable expectation of privacy in the text messages on his cell phone, and that he consequently had standing to challenge the search). That Arch Wireless may have been able to access the contents of the messages for its own purposes is irrelevant. *See United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007)* (holding that a student did not lose his reasonable expectation of privacy in information stored on his computer, despite a university policy that it could access his computer in limited circumstances while connected to the university's network); *United States v. Ziegler, 474 F.3d 1184, 1189-90 (9th Cir. 2007)* (holding that an employee had a reasonable expectation of privacy in a computer in a locked office despite a company policy that computer usage would be monitored). For, just as in *Heckencamp*, where we found persuasive that there was "no policy allowing the university actively to monitor or audit [the student's] computer usage," *482 F.3d at 1147*, Appellants did not expect that Arch Wireless would monitor their text messages, much less turn over the messages to third parties **[*33]** without Appellants' consent.

> 6 Because Jeff Quon's reasonable expectation of privacy hinges on the OPD's informal policy regarding his use of the OPD-issued pagers, *see infra* pages 7027-29, this conclusion affects only the rights of Trujillo, Florio, and Jerilyn Quon.

We do not endorse a monolithic view of text message users' reasonable expectation of privacy, as this is necessarily a context-sensitive inquiry. Absent an agreement to the contrary, Trujillo, Florio, and Jerilyn Quon had no reasonable expectation that Jeff Quon would maintain the private nature of their text messages, or vice versa. *See United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996)* ("[T]he maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others." (citing *Hoffa v. United States, 385 U.S. 293, 302, 87 S. Ct. 408, 17 L. Ed. 2d 374 (1966)*)). Had Jeff Quon voluntarily permitted the Department to review his text messages, the remaining Appellants would have no claims. Nevertheless, the OPD surreptitiously reviewed messages that all parties reasonably believed were

free from third-party review. As a matter of law, Trujillo, Florio, and Jerilyn Quon had a reasonable expectation that the Department would not review their messages absent consent from either a sender or recipient of the text messages.

We now turn to Jeff Quon's reasonable expectation of privacy, which turns on the Department's policies regarding privacy in his text messages. We agree with the district court that the Department's informal policy that the text messages would not be audited if he paid the overages rendered Quon's expectation of privacy in those messages reasonable.

The Department's general "Computer Usage, Internet and E-mail Policy" stated both that the use of computers "for personal benefit is a significant violation of City of Ontario Policy" and that "[u]sers should have no expectation of privacy or confidentiality when using these resources." Quon signed this Policy and attended a meeting in which it was made clear that the Policy also applied to use of the pagers. If that were all, this case would be analogous to the cases relied upon by the Appellees. *See, e.g., Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002)* ("[Employer] 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 that [employee] might have had and so scotches his claim."); *Bohach v. City of Reno, 932 F. Supp. 1232, 1234-35 (D. Nev. 1996)* (finding a diminished expectation of privacy under the *Fourth Amendment* where police department had issued a memorandum informing employees that messages sent on city-issued pagers would be "logged on the [department's] network" and that certain types of messages were "banned from the system," and because any employee "with access to, and a working knowledge of, the Department's computer system" could see the messages); *see also O'Connor, 480 U.S. at 719* (noting that expectation of privacy would not be reasonable if the employer "had established any reasonable regulation or policy discouraging employees . . . from storing personal papers and effects in their desks or file cabinets"); *Schowengerdt v. General Dynamics Corp., 823 F.2d 1328, 1335 (9th Cir. 1987)* ("We conclude that [the employee] would enjoy a reasonable expectation of privacy in areas given over to his exclusive use, unless he was on notice from his employer that searches of the type to which he was subjected might occur from time to time for work-related purposes.").

As the district court made clear, however, such was not the "operational reality" at the Department. The district court reasoned:

> Lieutenant Duke made it clear to the staff, and to Quon in particular, that he would *not* audit their pagers so long as they agreed to pay for any overages. Given that Lieutenant Duke was the one in charge of administering the use of the city-owned pagers, his statements carry a great deal of weight. Indeed, before the events that transpired in this case the department did not audit any employee's use of the pager for the eight months the pagers had been in use.

Even more telling, Quon had exceeded the 25,000 character limit "three or four times," and had paid for the overages every time without anyone reviewing the text of the messages. This demonstrated that the OPD followed its "informal policy" and that Quon reasonably relied on it. Nevertheless, without warning, his text messages were audited by the Department. Under these circumstances, Quon had a reasonable expectation of privacy in the text messages archived on Arch Wireless's server.

Appellees argue that, because Lieutenant Duke was not a policymaker, his informal policy could not create an objectively reasonable expectation of privacy. Moreover, Lieutenant Duke's statements "were specific to his own bill-collecting practices" and were "limited to . . . an accounting audit. He did not address privacy rights." However, as the district court pointed out, "Lieutenant Duke was the one in charge of administering the use of the city-owned pagers, [and] his statements carry a great deal of weight." That Lieutenant Duke was not the official policymaker, or even the final policymaker, does not diminish the chain of command. He was in charge of the pagers, and it was reasonable for Quon to rely on the policy--formal or informal--that Lieutenant Duke established and enforced.

Appellees also point to the California Public Records Act ("CPRA") to argue that Quon had no reasonable expectation of privacy because, under that Act, "public records are open to inspection at all times . . . and every person has a right to inspect any public record." *CAL GOV'T CODE § 6253*. Assuming for purposes of this appeal that the text messages archived on Arch Wireless's server were public records as defined by the CPRA, [7] we are not persuaded by Appellees' argument. The CPRA does not diminish an employee's reasonable expectation of privacy. As the district court reasoned, "There is no evidence before the [c]ourt suggesting that CPRA requests to the department are so widespread or frequent as to constitute 'an open atmosphere so open to fellow employees or the public that no expectation of privacy is reasonable.' " (quoting *Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)* (internal quotation marks omitted)).

> 7 The Act defines "public records" as "any writing containing information relating to the conduct of the public's business prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics." *CAL GOV'T CODE § 6252(e)*.

The *Fourth Amendment* utilizes a reasonableness standard. Although the fact that a hypothetical member of the public may request Quon's text messages might slightly diminish his expectation of privacy in the messages, it does not make his belief in the privacy of the text messages objectively unreasonable. *See Zaffuto v. City of Hammond, 308 F.3d 485, 489 (5th Cir. 2002)* ("[Defendant] also argues that the existence of Louisiana's public records law and a department policy that calls would be taped suggests that it would not be objectively reasonable for [plaintiff] to expect privacy in making a personal phone call from work . . . . [The officers testified that] they understood the policy to mean that only calls coming into the communications room (where outside citizens would call) were being recorded, not calls from private offices. A reasonable juror could conclude, on this evidence, that [plaintiff] expected that his call to his wife would be private, and that that expectation was objectively reasonable."). Therefore, Appellees' CPRA argument is without merit.

2. Reasonableness of the Search

Given that Appellants had a reasonable expectation of privacy in their text messages, we now consider whether the search was reasonable. We hold that it was not.

The district court found a material dispute concerning the "actual *purpose* or *objective* Chief Scharf sought to achieve in having Lieutenant Duke perform the audit of Quon's pager." It reasoned that if Chief Scharf's purpose was to uncover misconduct, the search was unreasonable at its inception because "the officers' pagers were audited for the period when Lieutenant Duke's informal, but express policy of *not* auditing pagers unless overages went unpaid was in effect." The district court further reasoned, however, that if the purpose was to determine "the utility or

efficacy of the existing monthly character limits," the search was reasonable because "the audit was done for the benefit of (not as a punishment against) the officers who had gone over the monthly character limits." Concluding that a genuine issue of material fact existed on this point, the district judge determined that this was a question for the jury. The jury found that Chief Scharf's purpose was to "determine the efficacy of the existing character limits to ensure that officers were not being required to pay for work-related expenses," rendering a verdict in favor of the City, the Department, Scharf, and Glenn.

Given that a jury has already found that Chief Scharf's purpose in auditing the text messages was to determine the efficacy of the 25,000 character limit, we must determine--keeping that purpose in mind--whether the search was nevertheless unconstitutional.

A search is reasonable "at its inception" if there are "reasonable grounds for suspecting . . . that the search is necessary for a noninvestigatory work-related purpose such as to retrieve a needed file." *O'Connor, 480 U.S. at 726*. Here, the purpose was to ensure that officers were not being required to pay for work-related expenses. This is a legitimate workrelated rationale, as the district court acknowledged.

However, the search was not reasonable in scope. As *O'Connor* makes clear, a search is reasonable in scope "when the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of . . . the nature of the [misconduct]." *Id.* (internal quotation marks omitted). Thus, "if less intrusive methods were feasible, or if the depth of the inquiry or extent of the seizure exceeded that necessary for the government's legitimate purposes . . . the search would be unreasonable . . . ." *Schowengerdt, 823 F.2d at 1336*. The district court determined that there were no less intrusive means, reasoning that talking to the officers beforehand or looking only at the numbers dialed would not have allowed Chief Scharf to determine whether 25,000 characters were sufficient for work-related text messaging because that required examining the content of all the messages. Therefore, "the only way to accurately and definitively determine whether such hidden costs were being imposed by the monthly character limits that were in place was by looking at the actual text-messages used by the officers who exceeded the character limits."

We disagree. There were a host of simple ways to verify the efficacy of the 25,000 character limit (if that, indeed, was the intended purpose) without intruding on Appellants' *Fourth Amendment* rights. For example, 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. Under this process, Quon would have an incentive to be truthful because he may have previously paid for work-related overages and presumably would want the limit increased to avoid paying for such overages in the future. These are just a few of the ways in which the Department could have conducted a search that was reasonable in scope. Instead, the Department opted to review the contents of all the messages, work-related and personal, without the consent of Quon or the remaining Appellants. This 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.

3. Qualified Immunity for Chief Scharf

Chief Scharf asserts that, even if we conclude that he violated Appellants' *Fourth Amendment* and California constitutional privacy rights, he is entitled to qualified immunity. We agree.

. . .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. Therefore, Chief Scharf is entitled to qualified immunity.

4. Statutory Immunity on the California Constitutional Claim

The City and the Department contend that they are shielded from liability on the California constitutional claim. We conclude that the district court correctly determined that the City and the Department are not protected by statutory immunity. . . .

V. CONCLUSION

As a matter of law, Arch Wireless is an "electronic communication service" that provided text messaging service via pagers to the Ontario Police Department. The search of Appellants' text messages violated their *Fourth Amendment* and California constitutional privacy rights because they had a reasonable expectation of privacy in the content of the text messages, and the search was unreasonable in scope. While Chief Scharf is shielded by qualified immunity, the City and the Department are not shielded by statutory immunity. In light of our conclusions of law, we affirm in part, reverse in part, and remand to the district court for further proceedings on Appellants' Stored Communications Act claim against Arch Wireless, and their claims against the City, the Department, and Glenn under the *Fourth Amendment* and California Constitution.

Because we hold that Appellants prevail as a matter of law on their claims against Arch Wireless, the City, the Department, and Glenn, we need not reach their appeal from the denial of their motions to alter or amend the judgment and for a new trial under *Federal Rule of Civil Procedure 59*. The parties shall bear their own costs of appeal.