UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

CIVIL MINUTES - GENERAL

Case No. ED CV 03-199 RT (SGLx) Date: March 23, 2004

Title: Jeff Quon, et al. v. Arch Wireless Operating Co., Inc., et al.

==========

PRESENT:

ROBERT J. TIMLIN, JUDGE

Lenora Pulliam	None
Courtroom Clerk	Court Reporter

ATTORNEYS PRESENT FOR PLAINTIFFS:	ATTORNEYS PRESENT FOR DEFENDANTS:
NONE	NONE

PROCEEDINGS: ORDER GRANTING IN PART AND DENYING IN PART DEFENDANT ARCH WIRELESS OPERATING CO., INC.'S MOTION TO DISMISS THE FIRST, THIRD AND FOURTH CLAIMS OF THE SECOND AMENDED COMPLAINT

The court, Judge Robert J. Timlin, has read and considered defendant Arch Wireless Operating Co., Inc. ("Arch Wireless")'s motion to dismiss the first, third and fourth claims of the Second Amended Complaint ("SAC") against it ("motion") for failure to state a claim pursuant to Federal Rule of Civil Procedure 12(b)(6) ("Rule 12(b)(6)"); plaintiffs Jeff Quon ("Jeff"), Jerilyn Quon ("Jerilyn"), April Florio ("Florio"), Doreen Klein ("Klein"), and Steve Trujillo ("Trujillo") (collectively "Plaintiffs")' opposition; and Arch Wireless's reply. Based on such consideration, the court concludes as follows:

I.
BACKGROUND[1]

The City of Ontario Police Department ("OPD") issues alphanumeric pagers to many of its employees. Through a wireless electronic text messaging service provided by defendant Arch Wireless pursuant to a contract with the City of Ontario ("City"), users of the alphanumeric pagers can send and receive electronic text messages. OPD issued wireless alphanumeric text pagers to plaintiffs Jeff and Trujillo, employees of the City. Plaintiffs Jerilyn, Florio, and Klein, also employees of the City, individually and personally owned their wireless alphanumeric text pagers. All Plaintiffs have their own personal and specific text messaging address. Jeff and Jerilyn are husband and wife.

Sometime during 2002, at the direction of the City's chief of police, a City employee, without a warrant, subpoena, or consent of the Plaintiffs, requested from Arch Wireless, the transcripts of every electronic text message ("text message") sent and received by Jeff on his pager. Although Plaintiffs never granted anyone permission to read or review the text messages sent and received by them on their pagers, Arch Wireless complied with such request and, on or about October 9, 2002, disclosed to OPD the content of private text messages sent and received by Jeff. Sometime during 2002, Arch Wireless disclosed by transcription the content of private text messages sent and received by each Plaintiff. Arch Wireless did not make these disclosures in connection with a criminal investigation.

On or about October 14, 2002, City employees confronted Jeff with the transcripts of the

[1] The statement of facts in the Background is taken from Plaintiff's SAC. When the court acts on a defendant's motion to dismiss pursuant to Rule 12(b)(6), the court must accept as true all material allegations in the SAC, as well as reasonable inferences to be drawn from them. Pareto v. FDIC, 139 F.3d 696, 699 (9th Cir. 1998).

text messages, demanded an explanation, and warned him that he might be subject to disciplinary action. Jeff was later denied a special assignment within the OPD. Klein was terminated by the City partially based on the content of the text messages on her pager. Florio was issued a Notice of Intent to Impose Disciplinary Action by the City partially based on the content of the text messages on her pager.

Plaintiffs filed their SAC against Arch Wireless, among other defendants. Arch Wireless is named as a defendant in the SAC's first claim for violation of 18 U.S.C. §§ 2702-2703 of the Stored Communications Act ("Section 2702"), in the third claim for violation of Cal. Penal Code § 629.86 ("Section 629.86"), and in the fourth claim for invasion of privacy, California Constitution Article I, Section 1. Arch Wireless now moves the court to dismiss all claims against it in the SAC for failure to state a claim upon which relief can be granted pursuant to Rule 12(b)(6).

II.
ANALYSIS

A. Legal Standard for a Rule 12(b)(6) Motion to Dismiss

A Rule 12(b)(6) motion to dismiss for failure to state a claim is viewed with disfavor and rarely granted. Gilligan v. Jamco Dev. Corp., 108 F.3d 246, 249 (9th Cir.1997). A motion to dismiss for failure to state a claim should not be granted unless it appears beyond doubt that the plaintiff can prove no set of facts in support of her claim that would entitle her to relief. Neighbors of Cuddy Mountain v. Alexander, 303 F.3d 1059, 1068 (9th Cir. 2002). To survive a motion to dismiss, a plaintiff need not set forth the legal basis for his claim, only the facts underlying it. McCalden v. California Library Ass'n., 955 F.2d 1214, 1223 (9th Cir. 1990); see

also 5A Charles Alan Wright & Arthur R. Miller, Federal Practice and Procedure § 1356, at 294-96 (1990).

In determining whether to grant a motion under Rule 12(b)(6) for failure to state a claim, all material allegations in the complaint are taken as true and construed in the light most favorable to the plaintiff. Galbraith v. County of Santa Clara, 307 F.3d 1119, 1121 (9th Cir. 2002). The court, however, need not accept as true conclusory allegations or unreasonable inferences. Miranda v. Clark County, 279 F.3d 1102, 1106 (9th Cir. 2002); Transphases Sys., Inc. v. Southern Cal. Edison Co., 839 F.Supp. 711, 718 (C.D. Cal. 1993).

B. First Claim of the SAC for Violation of Section 2702.

1. "Electronic Storage"

In 1996, Congress passed the Electronic Communications Privacy Act ("ECPA") in order to ensure the security of electronic communications. In Title I, the ECPA amended the Wiretap Act, and in Title II it created the Stored Communications Act ("SCA"), which contains Section 2702. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Lopez v. First Union Nat'l Bank, 129 F.3d 1186, 1189 (11th Cir. 1997); S. Rep. No. 99-541, at 3 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3557. The SCA was intended to address "access to stored wire and electronic communications and transactional records." S. Rep. No. 99-541, at 3; 1986 U.S.C.C.A.N. at 3557. Courts have noted that the language of the ECPA is not always clear. E.g., Konop, 302 F.3d at 874; United States v. Smith, 155 F.3d 1051, 1055 (9th Cir. 1998).

Section 2702(a)(1) provides that "a person or entity providing electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a

communication while in electronic storage by that service." The SCA allows for a private right of action for any person aggrieved by any violation of the SCA, see 18 U.S.C. § 2707, and adopts the same definitions used in the federal Wiretap Act. See 18 U.S.C. § 2711.

Arch Wireless contends that Plaintiffs' SAC fails to state a valid claim against it for violation of Section 2702 because the subject text messages it disclosed to the City were not in "electronic storage" for purposes of the SCA. "Electronic storage" is defined in the Wiretap Act, and thus the SCA, 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 the purposes of backup protection of such communication." See 18 U.S.C. § 2510(17) ("Section 2510(17)"). Either part of the definition of "electronic storage" is sufficient under the SCA. S. Rep. No. 99-541, at 35; 1986 U.S.C.C.A.N. at 3590.

To support its contention, Arch Wireless relies on Fraser v. Nat'l Mut. Ins. Co., 135 F.Supp.2d 623 (E.D. Pa. 2001), in which the court held that a company's post-transmission retrieval of the plaintiff's e-mail messages sent using the company's electronic messaging server did not violate the SCA. Id. at 636. Under that court's interpretation of the statutory language, Part (A) of the definition of "electronic storage" applies to interception of an electronic message while it is in intermediate storage with the server before being sent to the intended recipient, a window of time which may last a fraction of a second. Id. Part (B), the court continued, applies only to the time interval after delivery but before receipt during which back-up protection of the message is needed in the event that the e-mail system crashes, a similarly fleeting time period. Id. Thus, the court determined that the SCA "provides protection only for messages while they

are in the course of transmission." Id.

Fraser's austere interpretation of "electronic storage" is inconsistent with the Ninth Circuit's interpretation of the ECPA in Konop. That court held that while a defendant's unauthorized disclosure of the contents of the plaintiff's secure website did not violate the Wiretap Act, it did violate the SCA. In order for an electronic message to be intercepted under the Wiretap Act, the court said, the electronic message must be acquired during transmission. Id. at 878. The SCA, on the other hand, relates to electronic messages that are not intercepted, but rather are extracted from electronic storage. Id. at 878-79. Under Fraser's interpretation of "electronic storage," the Konop court's distinction between the Wiretap Act and the SCA would be largely eviscerated with respect to electronic messaging since liability under both for violating either Act would attach only when an electronic message was acquired during transmission.

Moreover, further persuasive authority undermines Fraser. In Lopez, the court held that a bank could incur liability under Section 2702 for disclosing the contents of electronic funds transfers after transmission of the funds transfers to the plaintiff's account. 129 F.3d at 1190. "Electronic storage," according to the court, occurred after transmission of the electronic funds transfers. Id. Also, in Fischer v. Mt. Olive Lutheran Church, 207 F.Supp.2d 914 (W.D. Wis. 2002), the court determined that e-mail was in "electronic storage" for purposes of the SCA when it was retrieved from plaintiff's e-mail account after transmission. Id. at 925. The court rejected the defendants' contentions that the plaintiff's e-mail messages were not in "electronic storage" based on Fraser, but chose not to opine whether Fraser was correctly decided. Instead it distinguished Fraser on the grounds that the plaintiff's e-mail messages were stored on an internet-based server as opposed to the company's server. Id.

The ECPA does not create a distinction between transmission and post-transmission of electronic messages in defining "electronic storage." Fraser's view that Part (B) of the definition of "electronic storage" applies only between the time interval the message is sent and received is nowhere to be found in the statute. Part (B) states that the storage must be "for the purpose of backup protection." Backup protection clearly may be needed after transmission. The plain meaning of the phrase "backup protection" encompasses creating duplicate copies of the electronic message in the event of post-transmission loss or unavailability, as well as a loss occurring during transmission.[2] In another portion of the SCA, Congress uses the common meaning of the term "backup" to indicate a duplicate copy of a message that an electronic communications service can maintain after transmission, rather than the pre-transmission meaning employed in Fraser. See 18 U.S.C. § 2704; see also S. Rep. No. 99-541, at 39; 1986 U.S.C.C.A.N. at 3593 (stating that Section 2704 allows the government to require that an electronic communications service provider "create and maintain a duplicate copy of the contents of the electronic communications sought").

The ECPA's legislative history indicates that Congress passed the SCA to prohibit a provider of an electronic communications service "from knowingly divulging the contents of any communication while in electronic storage by that service to any person other then the addressee or intended recipient." S. Rep. No. 99-541, at 37; 1986 U.S.C.C.A.N. at 3591. If "electronic storage" was interpreted to apply only to pre-transmission storage, an electronic communications service would be permitted to freely divulge the contents of electronic communications to

[2] The New Shorter Oxford English Dictionary, (Lesley Brown ed., 1993), defines "backup" as "[a] reserve, a stand-by or spare; support, backing; *Computing* (the making of) a duplicate copy of a disk, file, program, etc." Id. at 167. The Webster's II: New Riverside University Dictionary, (Anne H. Soukhanov ed., 1994), defines "back-up" as "1. A reserve or substitute. 2.a. Support or backing." Id. at 146.

individuals or entities that were not intended to receive the messages merely by storing a copy of the message and waiting the negligible period necessary for transmission to be completed to reveal its contents. Such an interpretation would contravene Congress's expressed intent in enacting the SCA.

Therefore, the court concludes that the SCA's definition of "electronic storage" in Section 2510(17), Part (B) includes storage after transmission of a copy of an electronic communication made for the purpose of backup protection. The SAC's allegations that Arch Wireless without authorization disclosed the contents of backup copies of Plaintiffs' text messages after transmission of those messages come within the SCA's definition of "electronic storage."

2. "Electronic Communication Service"

Arch Wireless further contends that the SAC does not properly allege a Section 2702 claim against it because Plaintiffs were not "users" of its service under the SCA. It contends only the City was a user because it was the only subscribing party to the provider service contract with Arch Wireless. It argues that SCA applies only to an "entity providing an electronic communication service." See 18 U.S.C. § 2702(a)(1). An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." See 18 U.S.C. § 2510(15) ("Section 2510(15)"). A "user" is defined as "any person or entity who (A) uses an electronic communication service; and (B) is duly authorized by the provider of such service to engage in such use." See 18 U.S.C. § 2510(13) ("Section 2510(13)"). Because ArchWireless's customer was the City, and not Plaintiffs, Arch Wireless asserts that Plaintiffs do not come within the definition of "user" in the

SCA. In other words, only the City was authorized by Arch Wireless under the provider service contract to use the pagers; not the Plaintiffs.

The SCA's definition of "user" is unambiguous and controlling. Konop, 302 F.3d at 880. The court must apply the ordinary definition of "use," which is "'to put into action or service, avail oneself of, employ.'" Id. at 880 (quoting Webster's Ninth New Collegiate Dictionary 1299 (1985)). The allegations in the SAC and reasonable inferences therefrom make clear that Plaintiffs used the electronic communication service, and that they were authorized by the City to do so. Arch Wireless provided the alphanumeric text messaging pagers to the City knowing the pagers would be distributed to and used by City employees.

There is no indication in the SCA and Arch Wireless provides no authority showing that contractual privity between the service provider and the user is necessary under the statute to enable a claim by the user against the provider for violation of Section 2702. Such a requirement is inconsistent with cases in which ECPA protections have been extended to employees using electronic communication devices provided by their employers. E.g., Adams v. Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001). The court finds that the SAC properly alleges that Plaintiffs were "users" under the applicable SCA definition.

Based on the foregoing discussion, the Court will deny Arch Wireless's motion to dismiss the first claim of the SAC for violation of Section 2702.

C. Third Claim of the SAC for Violation of Section 629.86

California Penal Code Chapter 1.4, See Cal. Penal Code §§ 629.50-629.98, is intended to provide exceptions to the general rule prohibiting wiretapping in California. California v.

Zepeda, 87 Cal.App.4th 1183, 1195, 105 Cal.Rptr.2d 187, 193 (Ct. App. 2001). Chapter 1.4 was crafted to emulate the federal Wiretap Act. Id. at 1196; 105 Cal.Rptr.2d at 194. Section 629.86 allows for a civil cause of action by "[a]ny person whose wire, electronic pager, or electronic cellular telephone communication is intercepted, disclosed, or used in violation of this chapter." See Cal. Penal Code § 629.86.

Plaintiffs state that because nothing in Chapter 1.4 denies them a civil remedy under Section 629.86, the SAC states a valid Section 629.86 claim. Section 629.86, however, does not independently establish a claim, rather a Section 629.86 claim must be premised on a violation of one of Chapter 1.4's other provisions. Although Chapter 1.4 does prohibit private parties from disclosing intercepted information prior to a public court hearing, by and large, it applies to law enforcement personnel and agencies. Furthermore, Chapter 1.4 is modeled on the federal Wiretap Act and covers interception of wire and electronic communications, not the acquisition of electronically stored communications and the disclosure of such stored communications as Plaintiffs have alleged against Arch Wireless.

Plaintiffs fail to specify a particular provision of Chapter 1.4 which would support their claim against Arch Wireless under Section 629.86, and the court finds none of Chapter 1.4's provisions to be applicable to the SAC's allegations against Arch Wireless. Therefore, the court will grant Arch Wireless's motion to dismiss the SAC's third claim for violation of Section 629.86 with prejudice.

D. Fourth Claim of the SAC for Invasion of Privacy - California Constitution, Article I, Section 1.

In order to prevail on a claim for invasion of privacy under the California Constitution, a plaintiff must establish 1) a legally protected privacy interest, 2) a reasonable expectation of privacy in the circumstances, and 3) conduct by the defendant constituting a serious invasion of privacy. Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal.4th 1, 39-40, 26 Cal.Rptr.2d 834, 859 (1994).

California law provides that under certain circumstances individuals have a privacy interest in confidential communications. In Flanagan v. Flanagan, 27 Cal.4th 766, 117 Cal.Rptr.2d 574, 581 (2002), the court held that a conversation is a confidential communication if a "party to that conversation has an objectively reasonable expectation that the conversation is not being overheard or recorded." Id. at 776-77; 117 Cal.Rptr.2d at 581; see also Frio v. Super. Ct., 203 Cal.App.3d 1480, 1490, 250 Cal.Rptr. 819, 824 (Ct. App. 1988). Furthermore, the Supreme Court has recognized that an individual has a legitimate privacy interest in confidential letters. United States v. Jacobsen, 466 U.S. 109, 114, 104 S.Ct. 1652, 1657 (1984) ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy."). Moreover, the Ninth Circuit has recognized that an employee's privacy interests may be violated when an employer rummages through her personal letters. Ortega v. O'Connor, 146 F.3d 1149, 1163 (9th Cir. 1998).

Arch Wireless contends based on Guest v. Leis, 255 F.3d 325 (6th Cir. 2001), that Plaintiffs lack a privacy interest in the text messages they transmitted more than a month before Arch Wireless obtained them from electronic storage and disclosed them to City employees. In

Guest, the court stated that the plaintiffs "would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient" since they are analogous to letter writers, whose expectation of privacy terminates upon delivery of the letter to the recipient. Id. at 333.

Guest, however, is distinguishable. The cited statement in Guest addressed an individual's ability to assert Fourth Amendment standing in an E-mail message sent to another,[3] not whether the sender had a valid claim for invasion of privacy under the California constitution. Furthermore, Guest only stated that an individual does not possess an expectation of privacy in messages sent; it did not opine that an individual does not have a privacy interest in received messages. The fourth claim of the SAC alleges that Arch Wireless invaded Plaintiffs' privacy by disclosing text messages they *received*, as well as text messages they sent. The Court concludes that Plaintiffs have stated a sufficient claim for invasion of privacy under the California Constitution and will deny Arch Wireless's motion to dismiss the SAC's fourth claim for invasion of privacy under the California Constitution.

[3] Guest relied on another Sixth Circuit case, United States v. King, 55 F.3d 1193 (6th Cir. 1995), which states that a sender's expectation of privacy terminates upon delivery of the letter. Id. at 1196. King, in turn, cited to United States v. Knoll, 16 F.3d 1313 (2d. Cir. 1994) and 4 Wayne R. LaFave, Search and Seizure, § 11.3(f) (1987). Knoll states that an individual does not have an expectation of privacy in a letter sent "to an individual with whom he had no relationship of confidentiality." Id. at 1322. LaFave cites to Knoll. 5 Wayne R. LaFave, Search and Seizure, § 11.3(f), at 206 (1996).

This accumulated authority suggests that it is not axiomatic that an individual has no privacy interest in messages sent to another party. If the two parties have a relationship of confidentiality, the sender may still possess a privacy interest in the transmitted message.

III.
DISPOSITION

ACCORDINGLY, IT IS ORDERED THAT:

1) Arch Wireless's motion to dismiss the first and fourth claims of the SAC is DENIED;

2) Arch Wireless's motion to dismiss the third claim of the SAC is GRANTED with prejudice; and,

2) Arch Wireless shall file an answer to the first and fourth claims of the SAC within eighteen (18) days from the date of this order.