P Send

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JUSTIN BUNNELL, FORREST PARKER, WES PARKER, and VALENCE MEDIA, LTD.,

Plaintiffs,

vs.

MOTION PICTURE ASSOCIATION OF AMERICA,

Defendant.

Case No. 2:06-cv-03206-FMC-JCx

ORDER GRANTING DEFENDANT'S MOTION FOR SUMMARY JUDGMENT

ORDER DENYING PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT

#185

This matter is before the Court on Defendant's Motion for Summary Judgment (docket no. 136), filed July 2, 2007, and Plaintiffs' Motion for Summary Judgment (docket no. 169), filed July 24, 2007. The Court has read and considered the moving, opposition, and reply documents submitted in connection with these motions. The matter was heard on August 20, 2007, at which time the parties were in receipt of the Court's Tentative Order. For the reasons and in the manner set forth below, the Court hereby **GRANTS** Defendant's Motion for Summary Judgment and **DENIES** Plaintiffs' Motion for Summary Judgment.

I. BACKGROUND

This case involves Defendant Motion Picture Association of America's (Defendant or MPAA) acquisition of emails that were sent from or received by Plaintiffs Justin Bunnell, Forrest Parker, Wes Parker and Valence Media, LLC (Plaintiffs or Bunnell parties).

A. Factual Background

Plaintiffs own and operate a website as part of an online computer network known as "BitTorrent," which is a peer-to-peer network that facilitates the copying and distribution of large files. Defendant is a motion picture trade association that, among other things, conducts copyright infringement investigations and assists with criminal and civil litigation involving copyright infringement.[1] Plaintiffs allege Defendant procured and conspired to procure "hacked" private information that Defendant then used to interfere with Plaintiffs' business operations.

The alleged "hacker" is Mr. Rob Anderson (Anderson), a former business associate of Plaintiff Justin Bunnell (Bunnell). In 2001, Bunnell employed Anderson as an independent contractor for BA Ventures, a company Bunnell owned at the time. BA Ventures was in the business of online advertising and Anderson earned commissions by selling said advertising. In the spring of 2005, Anderson and Bunnell's relationship soured and Anderson left BA Ventures.

However, before Anderson left, he "hacked" into Plaintiffs' email system. First, Anderson calculated Plaintiff's IP address to connect to Plaintiff's actual server. Then, he used the standard administration name as the account name or "log in" name, and guessed the correct password. Once he obtained access to the

---

[1] In a related case in front of this Court, *Columbia Pictures, et. al. v. Justin Bunnell et. al*, CV 06-1093 FMC (C.D.Cal.), plaintiffs are motion picture studios that have sued the Bunnell parties for operating a website that allegedly enables and encourages Internet users to locate and download unauthorized copies of copyrighted motion pictures and television shows for free.

administrative functions of Plaintiffs' email server software, he enabled the software's "copy and forward" function. Anderson configured the server software so that every incoming and outgoing email message would also be copied and forwarded to his anonymous Google email account. Anderson's original intent in hacking into Plaintiffs' email system was to keep track of what the Bunnell parties were saying about him after he left BA Ventures.

On June 7, 2005, Anderson emailed the MPAA to offer antipiracy consulting services. Anderson stated that his company, Vaga Ventures, had obtained possession of documents regarding Torrentspy.com and other pirate BitTorrent sites. Anderson was referred to MPAA senior legal counsel, Dean Garfield. The two first spoke on June 14, 2005. Anderson told Garfield he had an informant who could get him anything he wanted. Anderson offered to sell the information to the MPAA. Two weeks later, after negotiations regarding a formal written agreement, Anderson emailed 34 pages of documents to the MPAA in return for $15,000. The final agreement, signed by Anderson on June 30, 2005, represented that Vaga Ventures was in lawful possession of the information, the information was obtained through legal means, and that the disclosure did not violate any contract or agreement between Vaga Ventures and any third party.

B. The Instant Motions

The above facts are not in serious dispute. Rather, with their cross motions for summary judgment, the parties ask the Court to determine whether Anderson's actions violated the federal Wiretap Act, 18 U.S.C.§§ 2510 et seq., and the California Invasion of Privacy Act, Cal. Penal Code§§ 631 et seq..

Plaintiffs claim that Anderson's actions in configuring the email software to copy and forward Plaintiffs' incoming and outgoing emails constituted an interception of electronic communications under the Wiretap Act. Plaintiffs also move the Court to conclude as a matter of law that the MPAA knew or had

reason to know of Anderson's alleged violations of the Wiretap Act.

On the other hand, Defendant claims that Anderson's activities were not an "interception" because the emails were in storage at the time, and the Ninth Circuit has held that a communication acquired while in "electronic storage" is not "intercepted" under the Wiretap Act.

Additionally, Defendant also moves for summary judgment as to whether Plaintiffs have identified valuable trade secrets. Defendant claims that Plaintiffs' trade secrets claim must fail because they have not met their burden in describing the subject matter of the trade secret with sufficient particularity to separate it from matters of general knowledge.

II. APPLICABLE LAW

A. Summary Judgment Standard

Summary judgment is proper only where "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." Fed. Rule Civ. Pro. 56(c); *see also Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 106 S.Ct. 1348, 89 L.Ed.2d 538 (1986).

The moving party bears the initial burden of demonstrating the absence of a genuine issue of material fact. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 256, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). Whether a fact is material is determined by looking to the governing substantive law; if the fact may affect the outcome, it is material. *Id.* at 248, 106 S.Ct. 2505.

If the moving party meets its initial burden, the "adverse party may not rest upon the mere allegations or denials of the adverse party's pleading, but the adverse party's response, by affidavits or as otherwise provided in this rule, must set forth specific facts showing that there is a genuine issue for trial." Fed. R. Civ. P. 56(e). Mere disagreement or the bald assertion that a genuine issue of

material fact exists does not preclude the use of summary judgment. *Harper v. Wallingford*, 877 F.2d 728 (9th Cir. 1989).

The Court construes all evidence and reasonable inferences drawn therefrom in favor of the non-moving party. *Anderson*, 477 U .S. at 255; *Brookside Assocs. v. Rifkin*, 49 F.3d 490, 492-93 (9th Cir. 1995).

B. Electronic Communications Privacy Act

In 1986, Congress passed the Electronic Communications Privacy Act (ECPA) "to afford privacy protection to electronic communications." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir.2002). Congress has allowed a private right of action to any "person aggrieved by any violation of this chapter." 18 U.S.C. § 2707(a).

There are two distinct sets of claims under the ECPA. First, under Title I of the ECPA, the Wiretap Act makes it an offense to "intentionally intercept [ ] ... any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). Second, under Title II of the ECPA, the Stored Communications Act (SCA), is designed to "address access to stored wire and electronic communications and transactional records." 18 U.S.C. § 2701(a).

The Bunnell parties make their claims under the Wiretap Act. This Court must therefore determine if Anderson's actions constituted an "interception" of "electronic communication" under Title I of the ECPA, the Wiretap Act.

III. DISCUSSION

A. Wiretap Act Claim

Neither party disputes that Anderson configured the "copy and forward" function on Plaintiffs' email server so that he would receive copies of all Plaintiffs' emails in his Google email account. The parties also do not dispute that the emails are "electronic communications" as defined by the ECPA. Therefore, the Court's inquiry begins with whether said communications were

"intercepted" or acquired while in "electronic storage."

For purposes of the ECPA, at any given time, an electronic communication may either be intercepted and actionable under the Wiretap Act, or acquired while in electronic storage and actionable under the SCA. *Konop*, 302 F.3d at 877. An electronic communication may not simultaneously be actionable under both the Wiretap Act and the SCA. *Id.* The Ninth Circuit has rejected the argument that "intercept" must apply to electronic communications in storage because storage is at some point necessary for the transmission of electronic communication. *Id.* It has held that Congress understood that electronic storage was an inherent part of electronic communication and still chose to craft the statute so that "storage" and "interception" do not coincide under the statute's definitions of the terms. *Id.* at 879, (quoting 18 U.S.C. § 2510(17)(A)). Thus, if Anderson acquired Plaintiffs' emails while they were in "electronic storage," Plaintiffs' claim under the Wiretap Act necessarily fails.

The ECPA defines "electronic storage" as either "temporary, intermediate storage ... incidental to ... electronic transmission," or "storage ... for purposes of backup protection." 18 U.S.C. § 2510(17); *Theofel v. Farey-Jones,* 359 F.3d 1066, 1072 (9th Cir., 2004). The Ninth Circuit has noted that the ECPA's framework is at times "ill suited to address modern forms of communication" because the statute was passed before mass use of email and the Internet. *Konop*, 302 F.3d at 874, 876. It further recognized that the transmission time of email messages is very short, as it travels through wires "at the speed of light." *Id.* at 879. Nevertheless, it has held that the duration of the storage of the electronic communication is immaterial. *Id.* Even if the storage phase is transitory and lasts only a few seconds, it is still considered "electronic storage" under the ECPA. *Konop*, 302 F.3d at 874, 876. The Ninth Circuit observed that the statute specifically states "*any* temporary storage" is covered under the SCA, and not the Wiretap Act, and that Congress understood the transmission time of

emails when it passed the ECPA. *Id.*

In *Konop v. Hawaiian Airlines*, the plaintiff was an employee of Hawaiian Airlines who operated a secure website which posted criticism of his employer. A vice-president of the airline obtained access to the website by using another employee's password. The plaintiff sued, alleging the airline had violated the Wiretap Act when it failed to comply with the terms of use of the website and entered a secure website under false pretenses. The *Konop* court held that the "acquisition of email messages stored on an electronic bulletin board system, but not yet retrieved by the intended recipients, was not an interception under the Wiretap Act." *Id.* at 879.

The Ninth Circuit further elaborated on the definition of "storage" in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), when it held that copies of opened email messages on Internet Service Provider (ISP) servers are also in "electronic storage." *Theofel*, 359 F.3d at 1076-77. *Theofel* involved the alleged unlawful disclosure of emails after a subpoena was served upon the subject ISP. The Court determined that prior access to the email messages by the account holder was irrelevant as to whether the messages at issue were in electronic storage. *Id* at 1077. Accordingly, an email message on an ISP server is in "storage" regardless of whether or not the account holder opens or reads the message. *Id.* The Ninth Circuit determined that the district court correctly dismissed plaintiffs' Wiretap Act claim, noting that *Konop* was dispositive. It reiterated that the Wiretap Act applies only to "acquisition contemporaneous with transmission," and that "Congress did not intend for 'intercept' to apply to electronic communications when those communications are in 'electronic storage.' " *Id.* at 1077-78, quoting *Konop* at 302 F.3d at 877.

The Ninth Circuit's definitions of "intercept" and "electronic storage" for purposes of the ECPA are recognized in *Quon v. Arch Wireless Operating Co., Inc.*, 445 F.Supp.2d 1116, 1134 (C.D.Cal. 2006) (where district court was

required to determine, *inter alia*, the applicability of the SCA due to a police department's investigation and audit of text messages sent by its employees). There, the district court noted that even transitory storage of electronic communications lasting only a few seconds fell within the provisions of the SCA, as the Ninth Circuit's "narrow definition" of "intercept" for purposes of the Wiretap Act meant that only an acquisition of communication "contemporaneous with transmission" would fall within the scope of the Wiretap Act. Accordingly, any communication acquired when in transitory storage, even if said storage lasted only a few seconds, was within the purview of the SCA, and not the Wiretap Act. *Id.* at 1134.

In the instant case, Anderson's actions necessarily fall outside the scope of the Wiretap Act. Anderson configured the Bunnell parties' email server software so that all Plaintiffs' messages were copied and forwarded from the server to his Google email account. If the emails had not been stored on the server, Anderson would not have acquired copies of them. In *Konop*, messages on a secure website bulletin board that were read by an unauthorized user were deemed in "electronic storage" so that they were outside the purview of the Wiretap Act. Similarly, here there is also an unintended reader, Anderson, who read copies of the message that had been forwarded to him. The only distinguishing characteristic between the facts of *Konop* and the instant case is the place where the messages are stored. In *Konop,* they were stored on a website bulletin board. Here, they were stored on a server.

However, the place of storage will not transform Anderson's actions into an interception under the Wiretap Act. In *Theofel,* copies of email messages on an ISP server were determined to be in "storage." In the instant case, Plaintiffs' server stored the emails before they were copied and forwarded to Anderson's email account.

Further, the Ninth Circuit has determined in both *Konop* and *Theodel* that

the amount of time a message is in storage is immaterial. As such, Anderson could have received the forwarded messages in milliseconds or days, it makes no difference. Under the Wiretap Act, his receipt of the messages does not constitute an "interception."

The Ninth Circuit's interpretation of the word "intercept" also comports with the ordinary meaning of the word, which is "to stop, seize, or interrupt in progress or course before arrival." *Konop*, 302 F.3d at 878 (quoting Webster's Ninth New Collegiate Dictionary 630 (1985)). Anderson did not stop or seize any of the messages that were forwarded to him. Anderson's actions did not halt the transmission of the messages to their intended recipients. As such, under well-settled case law, as well as a reading of the statute and the ordinary meaning of the word "intercept," Anderson's acquisition of the emails did not violate the Wiretap Act.

Defendant's motion for summary judgment as to Plaintiffs' Wiretap Act claim is GRANTED and Plaintiffs' motion for summary judgment is DENIED.

B. California Invasion of Privacy Claim

The federal ECPA preempts the parallel state wiretap claim. First, the federal Wiretap Act contains and express preemption:

> "The remedies and sanctions described in this chapter with respect to the interception of electronic communications are the only judicial remedies and sanctions for nonconstitutional violations of this chapter involving such communications."

18 U.S.C.A. § 2518(10)(c).

Second, Plaintiffs' state wiretap act claim is preempted by "field preemption." As the Ninth Circuit states when describing the preemption doctrine:

> "Even in the absence of express preemptive text, Congress' intent to preempt an entire field of state law may be inferred "where the scheme of

federal regulation is sufficiently comprehensive to make reasonable the inference that Congress 'left no room' for supplementary state regulation" (field preemption)."

In re Cybernetic Servs., Inc., 252 F.3d 1039, 1045-46 (9th Cir.2001). The scheme of the ECPA is very comprehensive: it regulates private parties' conduct, law enforcement conduct, outlines a scheme covering both types of conduct and also includes a private right of action for violation of the statute. As such, it is apparent to this Court "that Congress 'left no room' for supplementary state regulation." *Id.* at 1045.

Additionally, the ECPA's preemption over state law claims has been recognized by the district court in *Quon v. Arch Wireless Operating Co., Inc.* The *Quon* court noted that "the remedies outlined in the SCA [Title II of the ECPA] are the exclusive ones a party may pursue in court for conduct covered by the statute: 'The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.'" *Quon v. Arch Wireless Operating Co., Inc.*, 445 F.Supp.2d 1116, 1138 (C.D.Cal.,2006).

Accordingly, Plaintiffs' state wiretap act claims are preempted by the ECPA and Defendant's motion for summary judgment as to Plaintiffs' claim under California Invasion of Privacy Act, Cal. Penal Code §§ 631 *et seq.*, is GRANTED.

C. Trade Secrets Claim

The California Uniform Trade Secrets Act (UTSA) provides for damages and injunctive relief for the "misappropriation" of "trade secrets." See Cal. Civil Code §§ 3426.2 -.3. Pursuant to the UTSA, "trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(1) Derives independent economic value, actual or potential, from not

being generally known to the public or to other persons who can obtain economic value from its disclosure or use; and

(2) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Cal. Civil Code § 3426.1(d).

The trade secret's subject matter must be described with "sufficient particularity to separate it from matters of general knowledge in the trade or of special knowledge of those persons ... skilled in the trade." *Imax Corp. v. Cinema Technologies, Inc.* 152 F.3d 1161, 1164 -1165 (9th Cir.,1998) (quoting *Universal Analytics v. MacNeal-Schwendler Corp.*, 707 F.Supp. 1170, 1177 (C.D.Cal.1989), aff'd, 914 F.2d 1256 (9th Cir.1990)). The trade secret also has to be described with sufficient particularity "to permit the defendant to ascertain at least the boundaries within which the secret lies." *Diodes, Inc. v. Franzen,* 260 Cal.App.2d 244 (1968), *accord Imax Corp*, 152 F.3d at 1163-64.

The Ninth Circuit affirmed the district court's granting of summary judgment against the plaintiff on a claim of trade secret misappropriation under California law because the plaintiff failed to adequately identify its claimed trade secrets in response to the defendant's interrogatories. *Id.* A broad interrogatory answer that unspecified "dimensions and tolerances" of the plaintiff's movie projector system were the trade secrets failed to provide the required level of specificity. " A plaintiff must do more than just identify a kind of technology and then invite the court to hunt through the details in search of items meeting the statutory definition [of a trade secret]." *Id.*

Similarly, in the instant case, Plaintiffs have failed to identify exactly what the trade secret is and apparently expect the Court to determine how the documents delivered to the MPAA by Anderson constitute a trade secret. Anderson's one time deliverance of 34 documents to the MPAA does not in and of itself constitute a trade secret violation. Plaintiffs claim that said

documentation "as a whole" derives value. The *Imax* plaintiffs also tried to refer to a range of documents when asked to identify their trade secrets, to no avail. Plaintiffs in this case have not identified with any measure of particularity what trade secrets the documents given to MPAA contain. As such, they have failed to meet their burden. Accordingly, Defendant's motion for summary judgment as to plaintiffs' trade secrets claim is GRANTED.

D. §17200 Claim

Plaintiffs' claim under California's Unfair Competition Law, Cal. Bus. & Prof. Code §§17200, *et seq*, focuses solely on the provision supporting claims based on another "violation of law." As Plaintiffs have not shown any violation of law under either the Wiretap Act or the Trade Secrets Act, their §§17200 claim fails as well. Accordingly Defendant's motion for summary judgment as to this claim is GRANTED.

V. CONCLUSION

Therefore, Plaintiff's Motion for Summary Judgment (docket no. 169) is DENIED. Defendant's Motion for Summary Judgment (docket no. 136) is GRANTED.

Defendants are ordered to submit a proposed judgment, consistent with this Order, to the Court within 20 days of the date of this Order.

August 21, 2006

FLORENCE-MARIE COOPER, Judge
UNITED STATES DISTRICT COURT