

S _____

**IN THE SUPREME COURT
OF THE STATE OF CALIFORNIA**

PALLORIUM, INC., a Texas Corporation,

Plaintiff and Appellant,

vs.

STEPHEN J. JARED, etc.,

Defendant and Respondent.

PETITION FOR REVIEW

After A Decision From The Court of Appeal
Fourth Appellate District (G0361124)

Gary Kurtz, SBN 128295
Law Office of Gary Kurtz
A Professional Law Corp.
20335 Ventura Boulevard
Suite 200
Woodland Hills, CA 91364
Telephone: (818) 884-8400
Telefax: (818) 884-8404

Attorneys for Plaintiff and Appellant
Pallorium, Inc.

Table of Conents

<u>Section</u>	<u>Page</u>
I. Issue Presented	1
II. Introduction	1
III. Summary Of The Case	2
IV. Procedural Background	4
V. Overview Of Argument	7
VI. Legal Argument	9
A. Defendant's Block Lists Were Not "technical means", So His Block Lists Cannot Qualify For Immunity Based On Subsection (2)(B)	9
B. The Trial Court Improperly Denied Plaintiff's Right To A Jury Trial With Respect To Subsection 2(A) Immunity	13
1. Trial By Jury Is A Guaranteed Right	13
2. Section 2(A) Immunity Cannot Be Found Because Defendant's Conduct Was Criminal	15
3. Defendant's Conduct Was Not In Good Faith	19
C. Defendant's Block Lists Are Not Content Based, So He Cannot Claim Immunity Pursuant To 47 U.S.C. § 230(c)(2)	20

Table of Authorites

<u>Authority</u>	<u>Page</u>
<i>Bardis v. Oates</i> , 119 Cal.App.4 th 1 (2004)	19
<i>Batzel v. Smith</i> , 333 F.3d 1018 (9 th Cir. 2003)	7
<i>Brashers Cascade Auto Auction v. Valley Auto Sales And Leasing</i> , 119 Cal.App.4 th 1038 (2004)	19
<i>California v. Dept. of the Navy</i> , 624 F.2d 885 (9 th Cir. 1980)	10
<i>Chavers v. Gatke Corp.</i> , 107 Cal.App.4 th 606 (2003)	15
<i>Gemini Aluminum Corp. v. California Custom Shapes, Inc.</i> , 95 Cal.App.4 th 1249 (2002)	14
<i>Grafton Partners LP v. Superior Court</i> , 115 Cal.App.4 th 700 (2004)	15
<i>In re Pen Register</i> , 610 F.2d 1148 (3d Cir. 1979)	11
<i>People v. Frazier</i> , 128 Cal.App.4 th 807 (2005)	14
<i>People v. Neidinger</i> , 127 Cal.App.4 th 1120 (2005)	14
<i>Raedeke v. Gibraltar Savings & Loan Ass'n</i> , 10 Cal.3d 665, 672 (1974)	14
<i>State Farm Mutual Ins. Co v. Superior Court</i> , 114 Cal.App.4 th 434, 453 (2003)	19
<i>United Artists Television, Inc. v. Fournightly Corp.</i> , 377 F.2d 872 (2 nd Cir. 1967)	11

<u>Authority</u>	<u>Page</u>
<i>U.S.A v. Snepp</i> , 456 F.Supp. 176 (E.D. Va. 1978)	10
California Constitution art. I, § 16	13
Rule 8.500(b)(1)	i
18 U.S.C. § 1030(a)(5)(A)	16
47 U.S.C. § 230(c)(2)(B)	1,2,9,13
47 U.S.C. § 230(c)(2)(A)	1,2,13,15

PETITION FOR REVIEW

I. Issue Presented

Appellant asks this Court to review whether the term “technical means” in the Communications Decency Act, 47 U.S.C. § 230(c)(2)(B) requires the means employed to be “technical,” or can any means, whether *technical* or not, to restrict access to information on the Internet qualify for immunity. Review is requested pursuant to Rule 8.500(b)(1) “to settle an important question of law.”

II. Introduction

This appeal seeks the reversal of a judgment entered by the trial court for the Defendant based on factual and legal findings with respect to an immunity affirmative defense litigated in the first stage of a bifurcated trial. The trial court found Defendant’s conduct was *immune based on 47 U.S.C. § 230(c)(2)(A), which requires a finding of good faith and 47 U.S.C. § 230(c)(2)(B) which does not require a finding of good faith.*

Appellant challenged both findings in the Court of Appeal. The Court of Appeal affirmed the trial court’s judgment based on 47

U.S.C. § 230(c)(2)(B), deferring as moot issues relating to 47 U.S.C. § 230(c)(2)(A). Appellant asks this Court to review the issues relating to 47 U.S.C. § 230(c)(2)(B), and specifically if applies in a situation where there were no “technical” means used. Appellant further asks that the matter be remanded to the Court of Appeal to resolve the issues relating to 47 U.S.C. § 230(c)(2)(A) in his favor.

III. Summary Of The Case

Plaintiff and Appellant Pallorium, Inc. (“Appellant” or “Pallorium”) is an investigative agency that conducts business nationally and internationally. Pallorium’s manager Steven Rambam appeared and testified at the bifurcated trial in this matter. Because of the nature of its business and its national and international scope, communication via Internet e-mail is critical to Pallorium’s business operations. [Reporter’s Transcript (“RT”): 75-76.]

Defendant and Respondent Stephen Jared (“Defendant”) is an individual who has an overly zealous loathing of unwanted or unsolicited junk e-mail, known as SPAM. Defendant initiated a crusade to rid SPAM from his personal computer and then the world. Defendant first gathered lists of SPAM addresses and then augmented

these lists with his own SPAM detecting systems. He then made his list of suspected Spammers (hereinafter "Block Lists") available to the general public. Defendant's Block Lists became wildly popular, and at one time up to a quarter of e-mail communications were filtered through the Block Lists. Unfortunately, Defendant's Block Lists were more popular than reliable and listed e-mail addresses that did not generate SPAM.

Pallorium's e-mail server address was never used to generate SPAM. Rather, it was an integral part of a legitimate business. These facts did not prevent Pallorium's e-mail server address from being listed on Defendant's Block lists, crippling Pallorium's business.

Mr. Rambam promptly learned that Pallorium's e-mail server address had been listed on Defendant's Block Lists and immediately contacted Defendant to report the error. Defendant moved from disinterested to belligerent in his refusal to remove Pallorium's e-mail server address from the Block Lists. Accordingly, Pallorium spent considerable amounts to circumvent the Block Lists and filed the instant action.

The matter proceeded through discovery, and an initial trial date was set. The trial was continued to allow Defendant's new counsel to

familiarize himself with the case, and it was continued again to allow Mr. Rambam to present testimony in Nevada.

After the original and the continued trial dates, the trial court permitted Defendant to amend his answer and assert an affirmative defense after discovery ended. The trial court then bifurcated the affirmative defense, stating that there would be a court trial on the legal issue of whether Defendant was "an internet content provider" [RT: 5, lines 11 and 12.] If the answer to that threshold issue was yes, then the trial court indicated there would be a full jury trial on all other issues, possibly including a jury determination of a good faith element of the affirmative defense. [RT: 5, lines 5 to 8 and lines 20 to 24.] Ultimately, the trial court usurped the jury, decided the factual issue of whether Defendant was acting in good faith, and issued a judgment for Defendant.

IV. Procedural Background

The complaint in this action was filed on October 10, 2003, alleging four causes of action: (1) Negligence; (2) Negligent Interference With Economic Advantage And Prospective Economic Advantage; (3) Intentional Interference With Economic Advantage

And Prospective Economic Advantage; and (4) Unfair Business Practices. [Clerk's Transcript ("CT"): 8 to 18.] Defendant, in pro per, entered a general appearance in the form of a document entitled a "Motion to Strike". [CT: 19 to 25.] At the hearing on that motion, the parties agreed to the trial court's suggestion to deem the motion as Defendant's answer. No affirmative defenses were raised in the deemed answer.

A trial was set and continued because counsel had just appeared to represent Defendant. [CT: 3.] The trial was continued again, from September 10, 2004 to November 8, 2004, at Appellant's request because Mr. Rambam was required to testify before a Grand Jury in Nevada. [CT: 26 to 37.]

Defendant took advantage the fact that Mr. Rambam honored his civic responsibility. After the date the trial should have been concluded, Defendant filed a motion for judgment on the pleadings [CT: 4, 38] and also an in limine motion [CT: 4] both asserting an immunity affirmative defense that was not even in the case. Thereafter, the trial court permitted Defendant to amend his answer, over objection. [CT: 5, 116-155, 208-216.] Defendant filed another motion for judgment on the pleadings. [CT: 156-207.] The trial court

later denied Defendant's motion for judgment on the pleadings based on his assertion of an immunity affirmative defense. [CT: 217-19.]

The trial court conducted a trial setting conference, where he bifurcated Defendant's immunity defense. It appeared from the hearing that the trial court was first going to try the issue whether the affirmative defense applied as a matter of law, reserving factual disputes for a jury trial. [RT: 2-6.] Jury fees were properly posted. [CT: 4.]

The trial court conducted a trial over two days – with one day of testimony and another partial day spent on argument. The trial court issued a tentative decision, finding for Defendant on both the legal and the factual issues. [CT: 220-32.] Thereafter, plaintiff filed objections to the tentative decision, which were summarily rejected. [Motion to Augment] A timely appeal followed.

The Court of Appeal affirmed the trial court's judgment based on a finding that Defendant used technical means to restrict access to the material. That finding lacks factual and legal support. No petition for rehearing was filed in the Court of Appeal. Appellant suggests that review by this Court is more appropriate because this matter

involves an important issue because of the increasing importance of the Internet.

V. Overview Of Argument

This matter was resolved in the trial court by the application of an affirmative defense based on the Communications Decency Act ("CDA") 47 U.S.C. § 230 disposes of the complaint. The intent of the CDA was summarized in *Batzel v. Smith*, 333 F.3d 1018 (9th Cir. 2003). That court explained that the statute was designed to encourage self-policing of the Internet, allowing interactive computer services to police content or refrain from policing content with no liability. In addition, the CDA was designed to overrule one case holding an ISP liable for defamation based on content posted on its service. None of those objectives was promoted by finding Defendant in the instant case immune.

The relevant immunity standards are as follows.

(1) Treatment of publisher or speaker - No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

(2) Civil liability - No provider or user of an interactive computer service shall be held liable on account of -

(A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or

(B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1). [1] (A)."

The trial court held Defendant immune pursuant to the (2)(A) section of the CDA. [CT: 225-26.] To do so, the trial court had to and did make the factual findings that Defendant (1) was a provider or user of an Internet computer service; (2) acted in good faith. Moreover, the finder of fact should have been required to determine whether the restriction was content based, but, instead, the trial court read that requirement out of the statute. [CT: 227-28.]

The trial court also held Defendant immune pursuant to the (2)(B) section of the CDA. [CT: 228-29.] In doing so, the trial court had to find that Defendant's lists were "technical means", and they restricted access to the content-based materials identified in of section (2)(A).

The trial court correctly found section (1) did not apply [CT: 223-24], so that section will not be discussed at this point.

VI. Legal Argument

A. Defendant's Block Lists Were Not "technical means", So His Block Lists Cannot Qualify For Immunity Based On Subsection (2)(B)

Subsection 2(B) is so poorly written that it cannot be the basis of any finding of immunity. The statute immunizes:

any action taken to enable or make available
to information content providers or others
the technical means to restrict access to
material described in paragraph (1).

The Court of Appeal, and many commentators, assume that "(1)" means "(A)", however, that is not what the law says. Accordingly, the lower courts decisions, which both assume that the statute means "access to material described in paragraph (A)" are not supported by the statutory language.

Assuming, for the sake of argument, this Court permits the lower courts to rewrite the federal statute, this subsection would still not apply because Defendant ~~did not~~ provide "technical means." Contrary to the comments of the Court of Appeal, Defendant did not provide any "technical means" to restrict access to a content that the user considers to be "obscene, lewd, lascivious, filthy, excessively

violent, harassing, or otherwise objectionable" The "technical means" mentioned by the Court of Appeal were used exclusively by Defendant to compile his block lists. He was sued because he circulated the lists, not the means to compile the lists. Accordingly, Appellant asks this Court to review whether a list constitutes "technical means."

Congress did not assist the public by defining the term "technical means." The issue before this Court, which seems to be one of first impression, is whether the distribution of a list fits the meaning of the term "technical means." A review of federal decisional authorities using the term "technical means" suggests something more than a list is required.

California v. Dept. of the Navy, 624 F.2d 885 (9th Cir. 1980) involved the application of pollution standards. The term "technical means" was used to determine what could be done to an engine to satisfy emission standards. In context, the term applied to emission controlling technology.

U.S.A. v. Snepp, 456 F.Supp. 176 (E.D. Va. 1978) involved a former C.I.A. agent's publication of a book. Although most of the discussion is irrelevant to the instant case, the court did discuss the

C.I.A.'s method of intelligence gathering. One method is through "technical means" where a machine does the collection. Some form of technology had to do the data collection to satisfy the definition.

In re Pen Register, 610 F.2d 1148 (3d Cir. 1979) addressed the issue of ordering a telephone company to assist law enforcement in tracing telephone calls. The court discussed the technical requirements of tracing calls, including electronic impulses generated from dialing and switching equipment to connect dialing and receiving numbers. The technological method was contrasted with manual tracing techniques. The court interpreted technological means as the application of physical or mechanical technology to accomplish a purpose.

United Artists Television, Inc. v. Fourtnightly Corp., 377 F.2d 872 (2nd Cir. 1967) was a copyright infringement case between a cable television system and the copyright owner. The court used the term "technical means" to refer to the amplification or transmission of television signals. This was more than merely providing a list of programs available to cable subscribers.

The term "technical means" must mean that the party seeking immunity protection must provide some technology or mechanical

means to restrict access to material that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable"

This cannot mean merely making a list available to the general public, as a list is not a "technical means" as federal courts have applied that term. With respect to controlling SPAM, this could be providing software or hardware to the general public but not merely providing information for existing "technical means" to draw from. Defendant permitted access to information, not anything that fits the definition of "technical means."

Defendant's own use of "technical means" to create his lists does not transform his lists (the products of his use of "technical means") into "technical means" themselves. Defendant did not provide access to the "technical means" by which he generated his lists but rather the results of his employing "technical means." The (2)(b) protection is, therefore, inapplicable to the conduct for which Defendant was sued.

B. The Trial Court Improperly Denied Plaintiff's Right To A Jury Trial With Respect To Subsection 2(A) Immunity

1. Trial By Jury Is A Guaranteed Right

Subsection 2(A) immunity requires a finding of good faith. Appellant suggests that the trial court denied the right to jury by making a finding of good faith. The Court of Appeal did not resolve the issue based its finding of Subsection 2(B) immunity. If this Court reviews and reverses that finding, the Subsection 2(A) issues would become relevant.

The California Constitution guarantees the right to a jury trial. See art. I, § 16. Code of Civil Procedure § 592 codifies the right, as follows:

In actions for the recovery of specific, real, or personal property, with or without damages, or for money claimed as due upon contract, or as damages for breach of contract, or for injuries, an issue of fact must be tried by a jury, unless a jury trial is waived, or a reference is ordered, as provided in this Code. Where in these cases there are issues both of law and fact, the issue of law must be first disposed of. In other cases, issues of fact must be tried by the Court, subject to its power to order any such issue to be tried by a jury, or to be referred to a referee, as provided in this Code.

In this case, the trial court was at liberty to make a preliminary or threshold determination as to whether a jury should hear the CDA defense, e.g. something akin to an offer of proof. Because the right to jury had been preserved [RT: 2.] – with fees posted – and not waived, the trial court was not within its power to make the ultimate ruling.

“The California Constitution . . . set out the right to a jury trial in the strongest possible terms.” Appellant had a right to a jury because it pleaded causes of action were legal, not equitable, seeking damages. *See Raedeke v. Gibraltar Savings & Loan Ass’n*, 10 Cal.3d 665, 672 (1974). In *Gemini Aluminum Corp. v. California Custom Shapes, Inc.*, 95 Cal.App.4th 1249 (2002), the court resolved issues regarding the allocation of a burden of proof in jury instructions regarding an affirmative defense. Although the decisional authorities generally deal with affirmative defenses in criminal cases, the right to a jury clearly includes the resolution of affirmative defenses. *See People v. Frazier*, 128 Cal.App.4th 807 (2005); *People v. Neidinger*, 127 Cal.App.4th 1120 (2005).

Assuming, arguendo, the validity of the Court’s tentative analysis, the immunity issue should have been presented to the jury to determine the factual issues in dispute, particularly whether Defendant

was acting in good faith. The court could go so far as determining that Defendant presented sufficient evidence so that there was legal basis for a jury trial on whether Defendant was entitled to immunity. At that point, a jury should have been assembled to decide the case.

A jury instruction should have been drafted to tell the jury that they should find Defendant immune from liability if they find that he: (1) was an Internet provider or user of an interactive computer service; (2) was acting in good faith; and (3) acted to restrict access to or availability of material that he considered to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable. The trial judge did not have the constitutional or legal authority to do anything other than pass the issue to a jury to decide the disputed factual issues and apply the law to those facts.

"[T]he improper denial of the right to jury is reversible error per se." *Grafton Partners LP v. Superior Court*, 115 Cal.App.4th 700, 705 (2004).

2. Section 2(A) Immunity Cannot Be Found Because Defendant's Conduct Was Criminal

47 U.S.C. § 230(2)(A) requires that the proponent of the defense demonstrate that his actions were in good faith. Obviously,

criminal activity cannot be in “good faith”. *See Chavers v. Gatke Corp.*, 107 Cal.App.4th 606, 612 (2003). Because Defendant’s conduct violated federal criminal statutes, there can be no finding of good faith in this case.

Defendant testified to violating the terms of 18 U.S.C. § 1030(a)(5)(A). That statute imposes criminal penalties on anyone who:

- (i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
- (ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
- (iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

The code section continues to define “protected computer” to include any computer “which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States,” 18 U.S.C. § 1030(e)(2)(B).

The UCLA Journal of Law and Technology published an article on this statute, which ironically was directed to prevent DDOS attacks. A copy of the article is contained in the motion to augment the record on appeal. The authors reframe the language of the statute to set forth the following elements:

Title 18 U.S.C. § 1030(5)(B) was essentially crafted to mimic Section A of Title 18 U.S.C. § 1030(5). However, Section B requires a lower standard of knowledge to invoke a violation. It states:

"through means of a computer used in interstate commerce or communication, knowingly causes the transmission of a program, information, code, or command to a computer or computer system -

(I) with reckless disregard of a substantial and unjustifiable risk that the transmission will -

(I) damage, or cause damage to, a computer, computer system, network, information, data or program; or

(II) withhold or deny or cause the withholding or denial of the use of a computer, computer services, system, network, information, data, or program.

Defendant in this case was proud to have **criminally** created a program and code that denied use of computers, computer systems and networks of third parties, including Pallorium. Further, Defendant admitted a criminal violation of this federal statute.

Pallorium's computer mail server was a "protected computer" because it was used to do interstate and foreign commerce and communications. [RT: 75.] Defendant violated each and every subsection set forth above:

- Defendant knowingly caused the transmission of an e-mail (information) to test whether Pallorium had an open server with the intent to block e-mails (causing damage) if there was a positive response (or in the instant case a false positive) to the test. [violating (A)(i)] [RT: 42, 50, 51, 58, 59.]

- Defendant intentionally accessed Pallorium's e-mail server without authorization and got a false positive response indicating it was an open server. He then recklessly caused damage by blocking e-mail without an effective way to remove the IP addresses from Defendant's black lists. [violating (A)(ii)] [RT: 43, 55-57, 62, 69-72.]

- Defendant intentionally accessed Pallorium's e-mail server and, as a result, received a false positive response indicating it was an open server, which resulted in damage because Pallorium's e-mail was blocked. [violating (A)(iii)] [RT: 43, 62.]

3. Defendant's Conduct Was Not In Good Faith

The definition of "good faith" commonly requires honesty in fact, as well as reasonable and fair conduct. It is often interpreted based on an objective standard. See *Brashers Cascade Auto Auction v. Valley Auto Sales and Leasing*, 119 Cal.App.4th 1038 (2004); *Bardis v. Oates*, 119 Cal.App.4th 1 (2004). In *State Farm Mutual Ins. Co v. Superior Court*, 114 Cal.App.4th 434, 453 (2003), the court explained: "The doctrine of good faith then requires the party vested with contractual discretion to exercise that discretion reasonably and with proper motive, not arbitrarily, capriciously, or in a manner inconsistent with the reasonable expectations of the parties." [citation omitted.] A key element is "honesty of purpose." *Id.* at 450.

Defendant certainly did not conduct himself in good faith with respect to Pallorium. [RT: 88-90.] All he had to do was shut off his system or remove Pallorium from his list, and the problems would have been mitigated to a trivial level. [RT: 91-92.] To do so, he would have had to travel back to California from Memphis to get into his system. This would have been prudent and in good faith, independent of Pallorium's problems, because all of Defendant's safeguards had been disabled by a DDOS attack. Defendant could not

be bothered to return to California to fix or shut down his system. Instead, he said he fretted unproductively in Memphis. [RT: 52-60.]

Pallorium was improperly listed, and that listing obstructed considerable legitimate business. Mr. Rambam used every fail safe on Defendant's system. He used the internal complaint method. He sent e-mails. He sent telefaxes. He called Defendant. Defendant's response was to do nothing to help or remove Pallorium from his blacklist. Instead, Defendant told Mr. Rambam to go "F" himself, hung up on Mr. Rambam and did nothing to solve the problem. [RT: 89-90.] Those were **not** the acts of a man conducting himself in good faith. That was **not** the conduct of a man deserving of federal immunity for "good faith" conduct.

C. Defendant's Block Lists Are Not Content Based, So He Cannot Claim Immunity Pursuant To 47 U.S.C. § 230(c)(2)

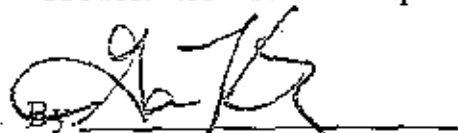
Section (2) only applies to material that the "user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Defendant did not block e-mail on the basis of content. [RT: 82-83.] He did not block because he considers the content of e-mails to be "be obscene, lewd, lascivious, filthy,

excessively violent, harassing, or otherwise objectionable." He blocked e-mail based on the content neutral factor of the configuration of e-mail servers, which does not qualify for protection.

The lower courts erred when they expanded immunity to content-neutral communications. That application of the statute fails to give meaning to the word "material". The material must "be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." That means content – not simply the fact that the e-mails were unsolicited or, in this case, were transmitted through an open e-mail server. It is not the "material" that Defendant found offensive or objectionable, and he did not filter based on material he believed to "be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." Accordingly, Defendant's content neutral filtering did not fit within the statutory language.

Dated: February 22, 2007

Law Office of Gary Kurtz
A Professional Law Corp.

By: 

Gary Kurtz, Esq.
Attorney for Appellant
Pallorium, Inc.

Certification of Word Count

Pursuant to the applicable Rule of Court, Appellant's Counsel hereby certifies that this brief contains 4,074 words, excluding tables.

Dated: February 22, 2007



Gary Kurtz