

S150792

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

PALLORIUM, INC.,

Plaintiff and Appellant,

vs.

STEPHEN J. JARED,

Defendant and Respondent.

After a Decision by the Court of Appeal
Fourth Appellate District, Division Three
[G036124]

ANSWER TO PETITION FOR REVIEW

Aaron P. Morris (Bar No. 130727)
THE MORRIS LAW FIRM
1851 E. First Street, Suite 900
Santa Ana, CA 92705
Telephone: (714) 954-0700
Facsimile: (714) 242-2058
E-mail: amorris@toplawfirm.com

Attorneys for Defendant and Respondent, STEPHEN J. JARED

TABLE OF CONTENTS

I.	SUMMARY OF FACTS AND ARGUMENT.....	1
II.	THE TRIAL COURT PROPERLY FOUND JARED WAS IMMUNE FROM LIABILITY UNDER SECTION 230(c)(2)(B).	4
III.	THE TRIAL COURT PROPERLY FOUND JARED WAS IMMUNE FROM LIABILITY UNDER SECTION 230(c)(2)(A).	7
	A. The Act does not require that spam filters be content-based; the user decides what is objectionable.	8
	B. Jared acted in good faith to restrict access to or availability of “harassing, or otherwise objectionable ... material.	12
IV.	THE TRIAL COURT DID NOT IMPROPERLY DENY APPELLANT’S RIGHT TO A JURY TRIAL	15
	A. Pallorium never objected to the bifurcated trial, and cannot raise the issue for the first time on appeal. ...	15
V.	APPELLANT NEVER RAISED THE ALLEGED “CRIMINAL CONDUCT” DURING THE TRIAL, AND MAY NOT RAISE THE ISSUE FOR THE FIRST TIME ON APPEAL.....	18
VI.	CONCLUSION.....	20

TABLE OF AUTHORITIES

Cases:

<i>America Online v. Greatdeals.net</i> (S.D.W.Va 1999) 49 F.Supp.2d 858.....	9-10
<i>Ferguson v. Factfinders, Inc.</i> (2002) 94 Cal.App.4th 1255.....	11
<i>Mainstream Loudoun v. Board of Trustees</i> (E.D.Va 1998) 2 F.Supp.2d 783.....	9
<i>Windsor Square Homeowners Ass’n v. Citation Homes</i> (1997) 54 Cal.App.4th.....	18

Statutes:

47 U.S.C. section 230(f).....	7, 13
47 U.S.C. section 230(b)(1).....	13
47 U.S.C. section 230(b)(2).....	13
47 U.S.C. section 230(c)(2)(a).....	7-8
47 U.S.C. section 230(c)(2)(b).....	4-6

I. SUMMARY OF FACTS AND ARGUMENT.

This petition for review follows an action that the trial court determined was barred by a Federal immunity statute and an unremarkable appeal from that decision. The case involves no important questions of law since the facts fell squarely within the applicable immunity statute.

Unsolicited e-mail costs the world billions in wasted time and resources, and Respondent Stephen Jared joined the fight against that plague of spam. Although virtually every Internet Service Provider now offers spam filters to its customers, at that time spam filters were still in their infancy. Spam filters use a number of approaches. For example, they can block messages that contain no subject line, those that include certain banned words, or those that contain links to web sites operated by known spammers. No perfect spam filter has ever been invented, and no one can reasonably claim that the publisher of a spam filter should be held liable for false positives, since it is the ultimately the end user that decides whether to employ a spam filter. Indeed, the Communications Decency Act recognizes the importance of spam filters, and affords immunity to anyone who makes them available to others.

Jared created, originally for his own use, a system designed to minimize the amount of spam flowing into his own computer servers. (RT

36:2–24; 40:8-42:25.) Jared tried to create the best spam filter available, and never intended to interfere with legitimate e-mail. (RT 35:23-26.) His spam filter used various techniques to identify spammers. In addition to drawing upon lists of known spammers, it used a computer program written by Jared to identify “open relays” and block spam from them as well. (RT 40:8-42:25; 47:6-9.) An open relay or server is a computer that has been left open to invasion (often inadvertently) on the Internet. Spammers seek out open servers, because they can hide their identities by sending the spam through these computers. (RT 36:20-24.) By doing so, the e-mail’s identification information shows the open server’s address, not the spammer’s. Thus, open servers thwart any spam list that is based on the spammer’s Internet address, because it will appear as though it is coming from the address of the open server. Approximately 18 percent of spam comes through open servers¹; as much as 54 percent comes through open proxies and hijacked systems. (RT 38:3-13.)

After seeing the positive affect his filter had on stopping junk e-mail, Respondent Jared decided to make his filter, and list of addresses used in

¹ Although Appellant did not agree with this number, it conceded that the number is at least ten percent. Inexplicably, Steven Rambam testified that in his opinion addressing the open server problem would be an ineffective way to curb spam, because it would “only” eliminate that ten percent. (RT 86:2-7.)

the filter, available at no cost to others through his web site. (RT 44:22-24.) No advertising occurred, and no sums were received by Jared from those who chose to use the filter. (RT 44:12-24.) The decision regarding whether, or how, to use the filter was left entirely to those third parties who accessed the site. They could use the filter as-is, or remove that portion of the list based on open servers.

Pallorium claimed that some of its e-mails were blocked by an internet service provider that had elected to use Jared's technical means for blocking spam.² Although Jared had no control over this third party's use of the system, and was not responsible for blocking any of Pallorium's e-mails, Pallorium sought to hold Jared liable, claiming that Jared's system had incorrectly identified Pallorium's computer as an open relay.

Both the trial court and Court of Appeal reached the correct and obvious conclusion that Jared's efforts to block spam were afforded immunity from civil liability under both 47 U.S.C. 230(c)(2)(A) *and* (B) of the Communications Decency Act. Pallorium claims that the issue presented by this appeal is whether any means to block spam, "technical or

² Appellant goes far beyond the record in its Petition and claims that its business was "crippled" as a result of blocked e-mails. In reality, Pallorium was not able to produce a single blocked e-mail message, offering instead only a compilation of three e-mails it contended were blocked, and it confirmed that it could have used other servers to avoid any blocks. (RT 98:1-11.)

not”, qualifies for immunity under the Act. In reality, there is no such issue. The evidence clearly demonstrated to the satisfaction of both the trial court and Court of Appeal that Jared had used technical means – a software program that he wrote – to block “harassing, or otherwise objectionable material.” That is all that is required for immunity under the Act.

II. THE TRIAL COURT PROPERLY FOUND JARED WAS IMMUNE UNDER SECTION 230(c)(2)(B).

The Communications Decency Act provides:

- “(2) . . . 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

[subparagraph (A)].”³ 47 U.S.C. § 230(c)(2)

(emphasis added).

Although subsection A requires a showing of good faith, no such showing is required for subsection B. Subsection B is therefore discussed first, since if immunity was correct under that subsection, all of Pallorium’s arguments relating to good faith become moot. The only facts relevant to this section go to the issue of whether Jared provided a technical means to restrict spam.

Jared testified that he created a software program called RB Check that allowed Jared, and third parties, to test for open servers. (RT 40:12-19.) Other spam blocking sites and services, such as Spamcop, would send addresses to Jared’s servers for testing. (RT 40:26-41:4.) Jared’s software would automatically attempt to relay an e-mail message back to the server, which would indicate an open server if a response was received. (RT 41:1-20.) Again, these were tests that were automatically performed based on the requests of third parties, all accessing Jared’s servers and utilizing the technology he had created. These were not manual tests by Jared. (RT 43:2-4.)

³ Original wording was “subparagraph 1” but all reported cases have recognized this as a scrivener’s error.

Appellant's only response to this reality is to argue that Jared's method of blocking spam was not "technical" enough to satisfy §230(c)(2)(B) because it did not involve the creation of software. This is completely contrary to the evidence presented. Jared testified to the intricacies of his spam blocking system, including how he had written software that permitted others to test for open servers, and there was no contradictory evidence offered by Pallorium. (RT 40:12-41:4.)

Appellant offers no authority for the proposition that there is some high threshold for what constitutes "technical" within the meaning of the Communications Decency Act, and bases this unsupported contention on a misstatement of the code section. Section 230(c)(2)(B) affords immunity to "**any action taken to enable or make available** to information content providers **or others** the technical means to restrict access to material described in [subparagraph (A)]." (Emphasis added.) The party need only make available the technical means to restrict access; there is no requirement that the party invented some advance, new technology. Jared both gathered the information and created an open server tester to create a very good spam blocker, and made that means to block spam available to others. His efforts fall squarely under the aforesaid section.

III. THE TRIAL COURT PROPERLY FOUND JARED WAS IMMUNE FROM LIABILITY UNDER SECTION 230(c)(2)(A).

The Communications Decency Act provides:

“(2) . . . 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” (Emphasis added.)

The statute defines the term “interactive computer service” as “any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server” (47 U.S.C. section 230(f)(2-3).)

It is specifically alleged in the complaint that Respondent’s block lists were “designed to limit or prevent unwanted, mass-market solicitations via e-mail, known as SPAM” and that these block lists were used by third-parties. Complaint, ¶ 5. Thus, as Appellant conceded below, Jared’s goal was to create a tool to block unwanted and harassing e-mail. To that end,

Jared created “enabling tools” designed to “filter, screen, allow or disallow content.” Since Jared’s filter was used by “multiple users to a computer server,” Respondent’s activities therefore fell squarely within the protections of the Act.

A. The Act does not require that spam filters be content-based; the user decides what is objectionable.

Since there is no dispute that Jared was seeking to “restrict access to” spam, the next inquiry, then, is whether spam is “harassing” or “otherwise objectionable” material under §230(c)(2)(A). Although Pallorium repeatedly claims that Jared’s efforts were not content-based, in fact Jared testified that he had received and was trying to block spam concerning “[p]enis enlargement, Viagra, web hosting” and “pornography.” Thus, as an initial matter, Jared’s efforts were directed to certain objectionable content.

However, that distinction is unimportant. Under the statute, it is the “user” that determines what is objectionable. Thus, in this case, Jared had the unfettered right to determine what he wants to block. The Act provides that there can be no liability if the effort is to block “material that the **provider or user** considers to be . . . harassing, or otherwise objectionable . . .” That could range from *all* unsolicited e-mail, down to specifically

objectionable materials such as pornography.

Given the pervasive nature of spam and its threat to literally cripple Internet commerce, that spam is harassing and objectionable is not an open question. As noted by one federal court, blockage of unsolicited bulk e-mail was “encouraged” by § 230(c)(2). *America Online v. Greatdeals.net* (S.D.W.Va 1999) 49 F.Supp.2d 851, 855, 864 (dismissing tortious interference with contractual relations and prospective economic advantage claim on basis that unsolicited bulk e-mail is “harassing” or “otherwise objectionable” and therefor the blockage of same was subject to the immunities afforded by §230(c)).

Congress explained the policy of §230 was “to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or state regulation.” (47 U.S.C. § 230(b)(2).) Section 230 “was enacted to minimize state regulation of Internet speech by encouraging private content providers to self-regulate against offensive material” *Mainstream Loudoun v. Board of Trustees* (E.D.Va 1998) 2 F.Supp.2d 783, 790 (citing *Zeran v. America Online* (4th Cir. (1997) 129 F.3d 327, 330.)) Congress, then, has made it clear that it would prefer for interactive computer service providers, rather than the government, regulate speech on the Internet. This supports

the argument that § 230(c)(2) encourages the blocking of spam.

The conclusion by the court in *Greatdeals.net* that §230 encourages the blocking of unsolicited bulk e-mail is correct. Pallorium contends that its e-mail did not amount to spam, and therefore Jared's filter was not protected because it was not 100 percent accurate. However, there is no such requirement. Section 230(c)(2)(A) provides immunity for any good faith effort to block spam. Any good faith but unintentional blockage of non-spam is therefore also afforded immunity. To rule otherwise would require litigation over whether the mail was spam, which would defeat the purpose in granting immunity. No spam filter will ever be 100 percent accurate.

Without offering any authority, Pallorium argues that an effort to block spam does not enjoy any form of immunity, unless it is directed to spam with some specific content. In other words, Pallorium claims that spam is not harassing or otherwise objectionable, and is therefore protected from any blocking efforts unless those blocking efforts are content based. Anyone who has endured the harassing and objectionable nature of spam will immediately understand why Appellant cannot offer any authority for such a position.

Public policy favors the creation of filters which help to eliminate

spam. In *Ferguson v. Friendfinders, Inc.* (2002) 94 Cal.App.4th 1255, the Court discussed the costs to internet service providers and businesses by the disbursement of unwanted spam, and the public policy surrounding laws which prohibit spam. The Court stated:

“The financial harms caused by the proliferation of UCE [spam] have been exacerbated by the use of deceptive tactics which are used to disguise the identity of the UCE sender and the nature of his or her message. Such deceptive tactics increase the already significant costs that UCE imposes on Internet users. . . . For example, by disguising the nature and origin of their messages, spammers evade attempts to filter out their messages and force ISPs to incur additional costs attempting to return messages to non-existent addresses or otherwise dispose of undeliverable messages. Likewise, e-mail recipients cannot easily identify unwanted UCE or promptly or effectively contact senders of such messages to request that future mailings not be sent. Furthermore, by using fraudulent domain names and return e-mail addresses, senders misdirect responses to their messages to innocent third parties who can suffer serious economic consequences. (*Ibid.*)

This ‘cost-shifting’ from senders of deceptive UCE to Internet

businesses and e-mail users ‘has been likened to sending junk mail with postage due or making telemarketing calls to someone's pay-per-minute cellular phone. . . . We agree with the *Heckel* court that protecting a state's citizens from the economic damage caused by deceptive UCE constitutes a ‘legitimate local purpose.’ (*Heckel, supra*, 24 P.3d at p. 410.)” *Ferguson*, 94 Cal.App.4th at 1268.

As the discussion above indicates, both public policy and federal law support the creation of spam filters, and the sharing of information via the web. With its action, Pallorium attempted to state a cause of action against Jared by alleging that policy favors holding users or promulgators of spam filters liable for blocking legitimate e-mail messages. Public policy is against the extension of liability as requested by Pallorium.

B. Jared acted in good faith to restrict access to or availability of “harassing, or otherwise objectionable . . . material.”

Again, Jared did not need to establish good faith to prevail at trial or on the appeal below. The trial court found that Jared was immune from liability under both § 230(c)(2)(A) *and* (B). Only subsection (A) requires the party to act in good faith. Since a verdict will be upheld if there is any basis for that verdict, the pending Petition for Review does not turn on a showing of good faith.

With that said, the courts below were correct in concluding that Jared acted in good faith. Appellant Pallorium was unable to provide any relevant evidence that Jared somehow acted in bad faith. Rather, Appellant could argue only that Jared was rude to Steve Rambam, the Pallorium representative, when he called to complain. (RT 90:1-3.) Appellant further claimed the complaint procedure on Respondent's website was inadequate.

Taking these contentions in turn, the Act is not so frivolous and does not define bad faith as being impolite. By definition, if Appellant was calling to complain about being included on the open server list, that is already after the list was created, and provides no insight into the relative good faith exhibited in creating that list.

As to the contention that Respondent had some duty to have a complaint system in place, if such were true then the Communications Decency Act would be meaningless as it applies to blocking objectionable material. The Act is designed to "preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation" (47 U.S.C. § 230(b)(1),(2)) and to promote the creation and use of tools designed to "filter, screen, allow or disallow content" (47 U.S.C. § 230(f)(4)). Following Appellant's reasoning, no filtering software or block lists could

ever be created, because spammers would always contend, just like Appellant, that the messages they were sending were not spam. Purveyors of spam could effectively silence any blocking efforts by tying up the anti-spam forces in court, forcing them to justify their decisions.

Every major ISP and Internet portal – AOL, Earthlink, Yahoo, MSN – now offers spam blockers. Determining what is spam is a matter of opinion, and any effort is an approximation at best. For example, many ISPs elect to block all e-mail messages containing the word “Viagra” in the subject line in order to stem the flood of spam relating to that drug, even though doing so may block some legitimate messages. No doubt this causes problems for Pfizer, the drug manufacturer, but should it be permitted to bring suit to force ISPs to allow all Viagra messages to pass?

In the instant case, Jared’s good faith opinion that open servers provide an unacceptable risk of transmission of spam is equally protected, and not subject to suit simply because Pallorium does not agree with that opinion. The public policy favoring the development and use of spam blocking tools cannot be questioned, and the freedom to do so should not be chilled by lawsuits such as this one.

There was ample evidence of Jared’s good faith. He testified that he never intended to interfere with legitimate e-mail. (RT 35:23-26.) Further,

he could not have been acting in bad faith toward Appellant Pallorium, because he had nothing to do with adding Pallorium to the open server list. (RT 55:24-56:1.) Any reference to Pallorium's open server would necessarily have been added because a third party requested a check through Jared's automated open server software. (RT 40:12-25.)

IV. THE TRIAL COURT DID NOT IMPROPERLY DENY APPELLANT'S RIGHT TO A JURY TRIAL.

A. Pallorium never objected to the bifurcated trial, and cannot raise the issue for the first time on appeal.

Jared attempted to dispose of this action by way of a motion for judgment on the pleadings, on the issue of immunity. However, like a demurrer, such a motion cannot be based on evidence, and the trial court decided that a determination of immunity would require information beyond the four corners of the complaint.

Therefore, the trial court concluded that the affirmative defense of immunity under the Communications Decency Act was a legal issue, and should properly be determined by the court. At no point did counsel for Appellant ever object to this approach. Quite to the contrary, counsel for Pallorium, Gary Kurtz, outlined and confirmed the procedure.

“Mr. Kurtz: Your Honor, can we set it the first day to try the affirmative defenses to the court and the next day, if the case survives, to go to the full hearing on the merits of the case? My client has to travel.” (RT 2:15-18.)

When the bifurcation was initially discussed, Kurtz did state that the issue of good faith should be left to the jury (RT 5:5-7), but he never objected to the trial court deciding the overall issue of immunity. The court responded as follows, with no objection from Plaintiff’s counsel:

“The Court: But everything else, the application of the federal privilege, if you will, that is really – we’re going to talk about every aspect of that and then every aspect. And if it is dispositive, it is. If it is not, then the jury will decide the rest of it.

Mr. Morris: Thank you. your honor.

Mr. Kurtz: Thank you, your honor.” (RT 5:20-26.)

The bifurcated trial was scheduled for June 20, 2005; three months after the above hearing. Plaintiff never objected to the bifurcation during those three months. The same was true at the commencement of the bench trial on the issue of immunity. (RT 7:6-8:8.) The first time Pallorium ever objected to the court deciding the issue of immunity, was after the court

issued its statement of decision. (CT 245:8-246:10.)² Even then, Pallorium’s objection was based only on the trial court’s determination that Jared had acted in good faith. (CT 245:12-14.) Pallorium argued that a determination of good faith was a factual issue, and should have been left to the jury. However, on the next page, Plaintiff argues that the determination of bad faith can be decided as a matter of law. (CT 246:12-16.)

The trial court’s decision did not turn on a determination of good faith. As set forth more fully elsewhere in this brief, the trial court found that Jared was immune under two independent sections of the Communications Decency Act, and only one of those sections requires that the party was acting in good faith.

Appellant Pallorium conceded below that the trial court was deciding a legal issue, stating, “the issue presented in this appeal are generally matters of law.” Appellant’s Opening Brief, p. 9. There may be no right to jury trial on special defenses that constitute a bar to plaintiff's claim (*e.g.*, a prior judgment as *res judicata*). These defenses involve questions that are “peculiarly legal determinations.” Consequently, the court can order such issues bifurcated and tried first without a jury even where factual issues

² Pages 243-266 of the Clerk’s Transcript were added pursuant to Appellant’s motion to augment record, and are attached to the Order granting that motion in the Court of Appeal’s miscellaneous papers file.

underlie the defense raised (*e.g.*, identity of parties and existence of privity for *res judicata* purposes). *Windsor Square Homeowners Ass'n v. Citation Homes* (1997) 54 Cal.App.4th 547, 557-558.

V. APPELLANT NEVER RAISED THE ALLEGED “CRIMINAL CONDUCT” DURING THE TRIAL, AND MAY NOT RAISE THE ISSUE FOR THE FIRST TIME ON APPEAL.

As an initial matter, it must be noted that Respondent Jared did not engage in any criminal conduct. In his efforts to stamp out spam, he checked for open servers since they assist spammers in their efforts. The process of checking for an open server simply entails sending an e-mail to that server. Noting this simple procedure, Appellant then makes a quantum leap in logic, and argues that since the sending of an e-mail to a server can identify it as an open server, and a party might therefore elect to refuse e-mail from that server since it may be forwarding spam, Respondent was guilty of a criminal act because the act ultimately damaged Appellant. For obvious reasons, Appellant cannot cite any authority for the proposition that Respondent’s method of testing servers was criminal.

However, aside from the lack of authority, this issue was never presented during the trial. At no time during the trial did Pallorium present

evidence, or even argue, that Jared could not have been acting in good faith because his conduct was criminal. Rather, this argument was advanced for the first time when Pallorium objected to the statement of decision. (CT 246:12-17.) The trial court overruled “the new argument based upon criminality because it was not argued during the hearing.” (CT 266.)

Respondent cannot discuss the evidence presented at trial on this issue, because it was never raised at trial. Therefore, it will have to suffice to point out that Jared testified that his mechanism for checking servers was passive and automatic. Jared’s software would automatically attempt to relay an e-mail message back to the server, which would indicate an open server. (RT 41:1-20.) A review of Jared’s testimony regarding how he tested for open servers reveals there was nothing criminal about this activity. (RT 38:3-40:7; 40:8-42:25; 58:2-60:3; 61:6-62:1.)

///

///

///

///

///

///

///


VI. CONCLUSION.

For all the reasons set forth hereinabove, the Petition for Review should be denied.

Respectfully submitted,

Dated: March 28, 2007

THE MORRIS LAW FIRM

By:  _____
Aaron P. Morris

Attorneys for Respondent
STEPHEN J. JARED

CERTIFICATION OF WORD COUNT

_____ Counsel of record hereby certifies that pursuant to Rule 8.504(d) of the California Rules of Court, the enclosed brief by Respondent is produced using 13-point type including footnotes and contains approximately 4151 words, which is less than the 8,400 words permitted by this rule. Counsel relies on the word count of the computer program used to create this brief.

Dated: March 28, 2007

THE MORRIS LAW FIRM

By: 

Aaron P. Morris

Attorneys for Respondent
STEPHEN J. JARED