Civil No. H028579

IN THE

Court of Appeal

FOR THE

STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

JASON O'GRADY, MONISH BHATIA, AND KASPER JADE,
Petitioners,

v.

SUPERIOR COURT OF THE STATE OF CALIFORNIA, COUNTY OF SANTA CLARA,
Respondent,

and

APPLE COMPUTER, INC.,
Real Party in Interest.

Petition for a Writ of Mandate And/Or Prohibition from the Superior Court
for the County of Santa Clara
Case No. 1-04-CV-032178
The Honorable James Kleinberg

REAL PARTY IN INTEREST APPLE COMPUTER, INC.'S RESPONSE TO BRIEFS OF *AMICI CURIAE* (1) JACK M. BALKIN *ET AL.*, (2) THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS *ET AL.*, (3) BEAR FLAG LEAGUE, AND (4) UNITED STATES INTERNET INDUSTRY ASSOCIATION AND NETCOALITION

GEORGE A. RILEY (S.B. #118304)
DAVID R. EBERHART (S.B. #195474)
JAMES A. BOWMAN (S.B. #220227)
IAN N. RAMAGE (S.B. #224881)
O'MELVENY & MYERS LLP
Embarcadero Center West
275 Battery Street
San Francisco, California 94111
Phone: (415) 984-8700
Fax: (415) 984-8701

Attorneys for Real Party in Interest
Apple Computer, Inc.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

Page

TABLE OF AUTHORITIES

Page

CASES

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

TABLE OF AUTHORITIES
(continued)

Page

STATUTES

TABLE OF AUTHORITIES
(continued)

Page

OTHER AUTHORITIES

RULES

INTRODUCTION

Apple Computer, Inc. seeks discovery from a third party necessary to recover Apple's stolen property and identify the individuals responsible for misappropriating its trade secrets. Apple's discovery is also necessary to learn whether Petitioners – website operators who deliberately disseminated these stolen secrets and thereby injured Apple – were complicit in this theft. Petitioners claim that Apple's discovery is barred by special protections they believe attach to their self-proclaimed role as "online journalists" – protections unavailable to other citizens. Four groups of *amici curiae* have filed briefs in support of Petitioners' attempt to block Apple's discovery.

Many arguments raised by Petitioners' *amici* have been addressed in the briefs previously submitted to this Court. Apple will accordingly focus its response on those parts of *amici*'s briefs that make new arguments or provide different perspectives on earlier issues briefed by the parties.

Jack M. Balkin *et al.* ("*Amici I*"), a coalition of "webloggers," contend that anyone who operates a web page that disseminates information to the public is entitled to invoke the First Amendment reporter's privilege (the "Federal Privilege") preventing disclosure of a reporter's sources. Because California has not established a test for who, beyond the traditional media, can claim this privilege, *Amici I* urge this Court to adopt the Ninth Circuit test in *Shoen v. Shoen*, 5 F.3d 1289 (9th Cir. 1993). Petitioners, however, cannot satisfy the *Shoen* standard, because accepting stolen trade secrets and copyrighted images and reproducing them wholesale on a website is not legitimate journalism worthy of such protection. Moreover, even if Petitioners had a legitimate claim to this privilege, it is a qualified privilege that is overcome by Apple's satisfaction of the factors in *Mitchell v. Superior Court*, 37 Cal. 3d 268 (1984).

The Reporters Committee For Freedom of the Press *et al.* ("*Amici II*"), a group of news organizations, echo Petitioners' claim that Apple has not pursued available sources of information that might have identified the persons responsible for the trade secret theft. That is simply not true. Before seeking this discovery, Apple pursued every reasonable lead in an effort to identify the responsible individuals. Moreover, the emails sought by Apple's subpoena contain the actual stolen materials. They are thus highly relevant to Apple's claims and are not available from other sources.

The Bear Flag League ("*Amici III*"), another coalition of "webloggers," expresses concern that identifying the trade secret thieves might restrict the flow of information from confidential sources to journalists in the future. But the public's interest in the flow of information to journalists does not include the unrestricted dissemination of trade secrets. The public interest, as expressed in both criminal and civil laws protecting trade secrets, is manifestly served by safeguarding such information.

United States Internet Industry Association and NetCoalition ("*Amici IV*"), urge the Court to find that the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* (the "SCA"), prevents an email service provider from responding to a valid civil subpoena. But *Amici IV* overstate the reach of the SCA and ignore the key statutory provision that allows Nfox, the third party service provider in this case, to comply with Apple's subpoena. While *Amici IV* would no doubt prefer a rule that exempts all email service providers from civil discovery, the SCA does not provide such an unqualified immunity.

Finally, Petitioners' *amici* try to expand the scope of these proceedings far beyond the issues presented in the petition. *Amici* broadly assert that webloggers are absolutely immune from liability for disseminating trade secrets and that persons who acquire trade secrets have

a constitutional right to anonymity. These attempts to raise new issues violate the rule that *amici* are not permitted to introduce issues not raised by the parties themselves. *See Bruno v. Superior Court*, 219 Cal. App. 3d 1359, 1365 (1990); *San Franciscans for Reasonable Growth v. City & County of San Francisco*, 209 Cal. App. 3d 1502, 1515 n.10 (1989). These arguments, moreover, contradict established principles regarding protections accorded legitimate news gathering. Thus, even if the Court addresses the substance of these arguments, none of them justifies the writ relief sought by Petitioners.

It has been almost six months since Apple's trade secrets, along with a copyrighted rendering of an unreleased product, were stolen and it commenced this action seeking redress. Apple should be accorded the opportunity to recover the stolen property and identify the responsible individuals. The *amicus curiae* briefs submitted in support of the petition do not provide reason to deny this discovery or overturn the trial court's decision.

ARGUMENT

I. THE FEDERAL PRIVILEGE DOES NOT BAR APPLE'S DISCOVERY FROM NFOX.

A. Illegal Dissemination Of Trade Secrets Is Not News Gathering Activity Protected By The Federal Privilege.

California courts have not yet established a test for who, beyond the traditional media, can invoke the qualified Federal Privilege. *Amici I* urge the Court to adopt the test developed by the Ninth Circuit in *Shoen* and find that online publishers are able to invoke the Federal Privilege. (*Amici I* Br. at 1.)[1]

[1] *Amici I* also incorrectly assert that the trial court and Apple have recognized that Petitioners are able to invoke the Federal Privilege. (*Amici*

But even if this Court adopts the *Shoen* standard, Petitioners cannot invoke the privilege under this test. Under *Shoen*, "the critical question for deciding whether a person may invoke the journalist's privilege is whether she is gathering news for dissemination to the public." 5 F.3d at 1293. This inquiry is not only directed towards the party's general activities, but also considers the *specific information* for which she seeks to invoke the privilege. *See In re Madden*, 151 F.3d 125, 130 (3d Cir. 1998) (person seeking to invoke the privilege must show that she was "engaged in investigative reporting, gathering news, and [had] the intent at the beginning of the news-gathering process to disseminate [the] information to the public"). Thus, although the Federal Privilege is not restricted to any particular medium, it "does not grant [journalist] status to any person with a manuscript, a web page, or a film . . . ." *Id.*

Petitioners cannot credibly claim that they obtained stolen trade secrets related to Apple's unreleased Asteroid product as part of legitimate investigative reporting activities. Petitioners knew, or certainly had reason to know, that this information was highly confidential and had been obtained in violation of confidentiality obligations owed to Apple. The information they posted on their websites was copied directly from an internal Apple document, stolen from Apple's secure facilities, that was prominently labeled "Apple Need-to-Know Confidential." (Zonic Decl. in Support of Opp'n to Mot. ¶¶ 4, 6, 19 (Ex. 28 at 396:24-397:1, 397:16-28,

---

I Br. at 1, 8.) The trial court did ***not*** rule that Petitioners were entitled to claim the Federal Privilege. Instead, the trial court concluded that it did not have to resolve this issue because Apple's need to identify the thieves overcomes this qualified privilege. Mar. 11, 2005 Order at 8-9, 11 (Ex. 34 at 462:14-464:8, 465:1-6). Apple, for its part, has consistently disputed that Petitioners can invoke the privilege to block discovery into the theft of the Asteroid trade secrets. (Opp'n to Pet. at 15; Opp'n to Mot. at 4-5 (Ex. 24 at 366:26-367:6).)

403:17-19).) As self-styled experts on Apple and the computer industry, Petitioners can hardly claim ignorance that Apple protected this sensitive information with strict confidentiality agreements and stringent security measures.

Regardless of their claim to be journalists, the dissemination of verbatim copies of Apple's confidential, proprietary information is not legitimate journalism or even news; it is trade secret misappropriation. Cal. Civ. Code § 3426.1(b); *United Liquor Co. v. Gard*, 88 F.R.D. 123, 131 (D. Ariz. 1980) (journalists have no right to publish confidential information and the public has no right to have it printed). Similarly, the publication of a copyrighted rendering of an unreleased product without Apple's permission is not proper news gathering; it is copyright infringement. *Zacchini v. Scripps-Howard Broad. Co.*, 433 U.S. 562, 576-79 (1977). Thus, even though the trial court found that it did not need to decide this issue, it was skeptical that Petitioners' reproduction of Apple's trade secrets qualifies to invoke any journalistic privilege. Mar. 11, 2005 Order at 11 n.7 (Ex. 34 at 465:24-25) (noting that Petitioner O'Grady likely could not invoke the Federal Privilege because he merely "took the information and turned around and put it on the PowerPage site with essentially no added value").

Accepting stolen property that is clearly marked as highly confidential and posting it on a website is not legitimate journalistic activity that merits protection under the Federal Privilege. *See Branzburg v. Hayes*, 408 U.S. 665, 691 (1972) ("Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news.").

B. Apple's Compelling Need For The Subpoenaed Information From Nfox Overcomes The Federal Privilege.

Even if Petitioners were able to invoke the Federal Privilege, the confidentiality of the sources of the stolen trade secrets must give way to Apple's need to seek redress for this theft. *Mitchell*, 37 Cal. 3d at 279. The trial court balanced these competing interests under the five-part *Mitchell* test and found that all five factors weigh in favor of disclosure. *See* Mar. 11, 2005 Order at 9-10 (Ex. 34 at 463:8-464:8).

The *amicus curiae* briefs filed in support of the petition address only two of the five *Mitchell* factors. First, *Amici II* argue that Apple has failed to pursue available sources of information that might identify the trade secret thieves. (*Amici II* Br. at 18-24.) Second, *Amici III* suggest that the need to maintain the free flow of information from confidential sources to reporters weighs against disclosure in this case. (*Amici III* Br. at 13-14.) Neither of these arguments has merit.

1. Apple Has No Reasonable Alternative Source For The Information It Seeks From Nfox.

Amici II contend that Apple has not pursued available sources of information that might identify the trade secret thieves. (*Amici II* Br. at 18-24.) This is simply not true. Apple has pursued every reasonable lead in an effort to identify the thieves before seeking this discovery. (Opp'n at 21-24.) Moreover, the emails sought by Apple's subpoena likely contain the stolen materials and are thus highly relevant to Apple's claims. These emails are not available from other sources and should be produced.

a. Apple has pursued all reasonable leads to identify the trade secret thieves.

Amici II ask this Court to hold Apple to an unreasonably high standard for overcoming the qualified Federal Privilege. They contend that

Apple cannot obtain the emails containing direct evidence of the theft without first (1) deposing every employee that it already interviewed about the theft, (2) seizing its employees' computers, and (3) hiring outside investigators to duplicate the investigation already conducted by Apple's highly experienced corporate security agents. (*Amici II* Br. at 22-23.)

But the authority cited by *Amici II* does not support this extreme view. Instead, in each of the cases cited by *Amici II*, the court faulted the party seeking discovery for failing to pursue a known source: not asking the right people the right questions or following up on a non-response. *See Zerilli v. Smith*, 656 F.2d 705, 714-15 (D.C. Cir. 1981) (plaintiffs made no effort to ask government employees about disclosure of confidential information before seeking discovery from reporter); *Shoen*, 5 F.3d at 1296 (plaintiff sought discovery from reporter without following up on defendant's uninformative discovery response on the same issue); *Condit v. Nat'l Enquirer, Inc.*, 289 F. Supp. 2d 1175, 1180 (E.D. Cal. 2003) (after learning that a Justice Department employee had provided false information to a reporter, plaintiff made no effort to locate that employee before seeking discovery from the reporter); *Rogers v. Home Shopping Network, Inc.*, 73 F. Supp. 2d 1140, 1145-46 (C.D. Cal. 1999) (plaintiff did not seek information from every potential witness before seeking discovery from reporter); *Los Angeles Memorial Coliseum Comm'n v. Nat'l Football League*, 89 F.R.D. 489, 494 (C.D. Cal. 1981) (defendant could not seek unpublished information related to biased media coverage because relevant information was available from public sources); *Food Lion, Inc. v. Capital Cities/ABC, Inc.*, No. 6:92CV00592, 1996 WL 575946, at *2 (M.D.N.C. Sept. 6, 1996) (information sought by plaintiff was marginally relevant and available from other sources).

By contrast, in *Star Editorial v. United States District Court*, 7 F.3d 856 (9th Cir. 1993), a case cited by *Amici II*, the plaintiff in a libel case was

granted discovery of a reporter's sources after taking reasonable steps to acquire the information through other sources. The court noted the clear need for the information: proof of malice could be established by showing that the informants were unreliable or that no informants existed. The court found that the plaintiff had reasonably pursued alternative sources of information, even though he had not questioned the reporter who had interviewed the informants.

Amici II's argument rests on a mistaken view of *Mitchell*. The actual test under *Mitchell* is quite clear. *Mitchell* requires that Apple pursue all ***reasonable*** alternative sources of information before seeking this discovery from Nfox. *Mitchell*, 37 Cal. 3d at 282 (disclosure is appropriate where there is "no other practical means of obtaining the information"); *see also Zerilli,* 656 F.2d at 713 (party must show that he has pursued "every reasonable alternative source of information"); *Condit*, 289 F. Supp. 2d at 1179 (party must pursue "reasonable alternative sources").

Apple's thorough investigation into the theft of the Asteroid trade secrets meets this requirement. As Apple explained at length in its opposition, Apple's highly experienced investigators identified the employees who had access to the stolen Asteroid information and interviewed each of them one by one. (Opp'n at 7-8, 21; Zonic Decl. in Support of Opp'n to Mot. ¶¶ 18-19, 21-23 (Ex. 28 at 403:9-19, 403:28-404:13); Ortiz Decl. ¶¶ 7-8 (Ex. 27 at 391:15-27).) All of them had a duty, under the terms of their employment, to tell the truth or be terminated. (Zonic Decl. in Support of *Ex Parte* Application ¶ 8 (Ex. 5 at 30:9-17, 36).)

Apple's investigators pursued the leads that resulted from these interviews but were unable to discover who was responsible for the theft. (Zonic Decl. in Support of Opp'n to Mot. ¶¶ 17, 19-23 (Ex. 28 at 402:28-403:8, 403:15-404:13).) Apple also ran forensic searches of its email servers to determine whether the stolen secrets had been forwarded to

anyone outside the company, or even to any additional employees within it. (Ortiz Decl. ¶ 9 (Ex. 27 at 391:28-392:4).)

Amici curiae Intel Corporation and Genentech, Inc., in opposing the petition, explain that the additional steps suggested by *Amici II* of seizing employees' computers and taking their depositions would be "pointless formalities" and would not add any information not already obtained from Apple's thorough investigation. (Intel Br. at 4, 9; Genentech Br. at 16.) Making such efforts a precondition to discovery of information from third parties such as Nfox would also stifle innovation and unnecessarily disrupt the workplace. (Intel Br. at 9; Genentech Br. at 16-17.) These severe measures are entirely impractical and inconsistent with *Mitchell*.

Because Apple's thorough investigation did not identify the trade secret thieves, Apple must now be allowed to seek the direct evidence of this theft contained in the emails held by Nfox.

b. The emails subpoenaed from Nfox are relevant and not obtainable from alternative sources.

In addition to identifying the sources of the stolen information, the emails held by Nfox are themselves highly relevant to Apple's claims. These emails contain the actual stolen materials that Apple is entitled to recover. They are also necessary to establish that Petitioner O'Grady knew that the information he posted on his website had been acquired by improper means or from a person who owed Apple a duty of secrecy. These emails thus bear directly on Petitioner O'Grady's liability. (Opp'n at 18.)

Disclosure of such relevant evidence is appropriate if there is no reasonable alternative source of that information. *See In re Ramaekers*, 33 F. Supp. 2d 312, 316 (S.D.N.Y. 1999) (ordering production of recorded interview that was relevant and not obtainable from alternative sources);

Gonzales v. Nat'l Broad. Co., 194 F.3d 29, 36 (2d Cir. 1998) (ordering production of videotaped interview not available from other sources). In *Ramaekers*, investors sued a company after statements made by the company's CEO in a Reuters article caused its stock to plummet. When the investors subpoenaed Reuters for a tape of its interview with the CEO, Reuters asserted the Federal Privilege. The court ordered production of the audiotape because the tape itself was relevant and not obtainable from any other source. 33 F. Supp. 2d at 316.

Like the evidence at issue in *Ramaekers*, no other source can provide the highly relevant emails sought by Apple from Nfox.[2] The emails in Nfox's possession constitute direct evidence of (1) who provided the stolen information, (2) what exactly was provided, (3) when it was provided, and (4) the conditions, including any consideration, under which the stolen materials were provided. Moreover, the internal Apple document presumably attached to those emails – which includes a copyrighted rendering of Asteroid – is stolen property that Apple is entitled to recover. For that reason, the third *Mitchell* factor weighs heavily in favor of disclosure.

2. Preserving The Trade Secret Thieves' Confidentiality Is Contrary To The Public Interest.

The fourth *Mitchell* factor considers the public's interest in protecting the confidentiality of the reporter's source. *Mitchell*, 37 Cal. 3d at 282-83. *Amici III* argue that this factor weighs against disclosure

---

[2] O'Grady is not an "an alternative source" because seeking these emails directly from him would implicate the same privilege he is asserting over the discovery from Nfox. *See Star Editorial*, 7 F.3d at 861 (journalist was not an "alternative source" of information sought from newspaper because he would likely invoke the same privilege being asserted over the discovery at issue).

because the public has an interest in ensuring "the free flow of information from confidential sources to broadcast reporters, magazine writers, and even Bloggers." (*Amici III* Br. at 13.) They also express concern that identifying the thieves in this case would have a "chilling effect" on the willingness of sources to give information to journalists in the future. (*Id.*)

The public would not benefit from protecting the trade secret thieves in this case. *Mitchell* emphasized that protection should be afforded to whistleblowers who provide information on matters of public concern, such as abuse of power or corporate malfeasance. 37 Cal. 3d at 283. But the court also recognized that there is very little public benefit in protecting confidential sources who engage in conduct that harms society, such as making false accusations. *Id.*

The individuals that Petitioners are trying to protect in this case are not "whistleblowers," they are thieves who stole trade secrets related to an unreleased commercial product and had them posted on Petitioners' websites. Preserving the anonymity of these individuals would turn this factor on its head by shielding – rather than exposing – criminal and unethical conduct. Far from having an interest in protecting these individuals, the public has a strong interest in seeing that these thieves are unmasked and forced to account for their wrongdoing. *See Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 487 (1974) ("A most fundamental human right, that of privacy, is threatened when [trade secret theft] is condoned or is made profitable; the state interest in denying profit to such illegal ventures is unchallengeable.").

Moreover, the public's interest in the "free flow" of information from confidential sources to journalists does not include the unrestricted disclosure of proprietary trade secrets. *Branzburg*, 408 U.S. at 691-92 ("The [First] Amendment does not reach so far as to override the interest of the public in ensuring that neither reporter nor source is invading the rights

of other citizens through reprehensible conduct forbidden to all other persons."). The public interest, as expressed in both criminal and civil laws protecting trade secrets, is instead manifestly served by safeguarding such information. *See* Cal. Penal Code § 499; Cal. Civ. Code § 3426.1. Courts have consistently held that the public interest demands the protection of trade secrets. *See, e.g., DVD Copy Control Ass'n v. Bunner*, 31 Cal. 4th 864, 880 (2003) ("[W]ithout trade secret protection, organized scientific and technological research could become fragmented, and society, as a whole, would suffer.") (internal quotations omitted); *Merrill Lynch, Pierce, Fenner & Smith, Inc. v. Wertz*, 298 F. Supp. 2d 27, 34-35 (D.D.C. 2002) ("[T]he public interest is served by protecting confidential business information and trade secrets.").

The public would be greatly harmed if individuals were able to disclose trade secrets on the Internet with impunity. For example, an investment by Genentech of hundreds of millions of dollars in a new drug therapy, such as its product Avastin, could be rendered nearly worthless by the theft and publication of a few pages from a lab notebook. (Genentech Br. at 2.) Once proprietary information about an unreleased product has been disclosed to the public, competitors are free to "copy the designs and attempt to free-ride off the insights." (Intel Br. at 5.)

Apple was substantially harmed by the disclosure of the Asteroid trade secrets in this case. Petitioners' *amici* trivialize this harm, claiming that Apple is only upset about the timing of "when the newsworthy information was released." (*Amici II* Br. at 28.) But Petitioners did not merely reveal that Apple was developing a new product. Instead, they disclosed a broad array of highly sensitive information, including detailed technical specifications, pricing projections for the device, competitive analyses, and confidential details regarding Apple's plans to manufacture the product. (Opp'n at 5-8; Zonic Decl. in Support of Opp'n to Mot. ¶¶ 5-

15 (Ex. 28 at 397:2-402:14).) Even if Apple eventually released the Asteroid product (not every product under development is eventually released) none of this sensitive information would have been disclosed to the public. By revealing these trade secrets to the world, including Apple's competitors, their value was largely destroyed. *See Bunner*, 31 Cal. 4th at 881 (the "only value [of trade secrets] consists in their being kept private").

The public has a strong interest in preventing individuals from illegally disclosing trade secrets to anyone, including the media. Conversely, there is no public interest in shielding individuals that misappropriate trade secrets from accountability for their illegal actions. The fourth *Mitchell* factor therefore weighs heavily in favor of Apple's discovery.

II. THE STORED COMMUNICATIONS ACT DOES NOT BAR DISCOVERY FROM NFOX.

Amici IV urge this Court to interpret the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, as completely exempting email service providers from the rules of civil discovery. This interpretation is not supported by the statute itself or the interpreting case law, and the Court should reject this unwarranted expansion of the SCA.

A. The SCA Does Not Bar All Civil Discovery Propounded Upon Email Service Providers.

Amici IV contend that the SCA generally prohibits an email service provider from divulging the contents of stored email communications. (*Amici IV* Br. at 6.) They argue that this prohibition bars Nfox from producing the PowerPage emails requested in Apple's court-approved subpoena. (*Id.*)

Amici IV misconstrue the function and scope of the SCA. This statute was not enacted to preempt all civil discovery; indeed, not once in

nearly 300 pages of legislative history did Congress indicate that it intended to change the rules of civil discovery, let alone erect such a comprehensive barrier. *See, e.g.*, H. REP. 99-647 (1986), S. REP. NO. 99-541 (1986), 132 CONG. REC. H8977-01 (June 23, 1986), 132 CONG. REC. H8977-02 (Oct. 2, 1986), 132 CONG. REC. S14441-04 (Oct. 1, 1986).

Instead, the legislative history reveals that the SCA was enacted to extend Fourth Amendment protections to email service providers and establish a framework for government searches of emails held by third parties. *See* 132 CONG. REC. H4039-01 (Oct. 2, 1986); O. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2003).

The Fourth Amendment provides strong privacy protections against government intrusions into an individual's home. O. Kerr, *A User's Guide*, 72 Geo. Wash. L. Rev. at 1210. Before the SCA was enacted, courts had held that this protection did not apply to information revealed to third parties, including information sent over the Internet or stored by an Internet service provider. *Id.* at 1210-11. Thus, unlike information stored in an individual's home, the government could obtain electronic information stored by a service provider without a showing of probable cause. *Id.* at 1212. Even in situations where the Fourth Amendment barred the government from obtaining communications held by a service provider, nothing prevented that provider from disclosing stored communications to the government on its own accord. *Id.* Congress enacted the SCA to address this imbalance by extending Fourth Amendment protections applicable to information stored in the home to information stored by a third party service provider. *Id.* at 1212-13.[3]

---

[3] Congress also enacted the SCA to punish and deter unauthorized access to email service providers' facilities by so-called "hackers." *See* A. Carter, *Computer Crimes*, 41 Am. Crim. L. Rev. 313, 337 (2004); *see also* S. REP.

The SCA did not create new protections against civil discovery for email held by service providers for a simple reason: there was no corresponding disparity between the methods for and restrictions on civil discovery of emails from individuals or their service providers. The federal and state discovery rules applied whether the email was located at the service provider, the individual's home, the individual's workplace, or elsewhere. This was fundamentally different from the pre-SCA gaps in Fourth Amendment protections for email. Nor can Petitioners' *amici* explain why, as they would have it, Congress created an impenetrable bar to civil discovery from service providers but placed no new restriction on civil discovery of emails from individuals or their employers. In short, nothing in the legislative history of the SCA suggests the creation of an absolute prohibition on civil discovery – discovery that is under the ultimate supervision of the courts. Such a reading would imply a profound change to civil litigation and is not supportable.

As the party moving for a protective order, Petitioners have the burden of establishing that the SCA prevents Apple from obtaining relevant information in response to its subpoena. Cal. Civ. Proc. Code § 2017(c); *Emerson Elec. Co. v. Superior Court*, 16 Cal. 4th 1101, 1110 (1997).[4] But neither *Amici IV* nor Petitioners can cite a single case holding that the SCA

NO. 99-541, at 3 (1986) (the SCA is intended to prevent "wrongful use and disclosure by law enforcement authorities as well as *unauthorized* private parties") (emphasis added).

[4] Apple does not concede that Nfox provides an electronic communication service to the public. Petitioner O'Grady's declaration filed in support of the motion for protective order does not provide a foundation for knowledge that Nfox provides services to anyone other than O'Grady. (*See* Declaration of Jason O'Grady in Support of Mot. for Protective Order ¶ 23 (Ex. 18 at 131:6-7).)

bars civil discovery propounded on an email service provider.[5] In fact, the leading decision addressing the application of the SCA to a third-party subpoena proceeds from the proposition that the SCA does ***not*** bar a valid civil subpoena. *Theofel v. Farey-Jones*, 359 F.3d 1066, 1073 (9th Cir. 2004) (finding that the overbreadth of a civil subpoena to an email service provider transformed what would have been "a bona fide state-sanctioned inspection" into unauthorized access under the SCA).[6]

Under *Amici IV*'s sweeping interpretation of the statute, the SCA would be the only federal privacy statute that has no exception whatsoever for civil discovery in response to a court order or subpoena. *See, e.g.*, Privacy Act, 5 U.S.C. § 552a(b)(11) (allowing disclosure of an individual's private records and confidential information held by a government agency

---

[5] *Amici IV* claim that the court in *FTC v. Netscape*, 196 F.R.D. 559, 560-61 (N.D. Cal. 2000), implied that civil subpoenas are barred by the SCA. (*Amici IV* Br. at 11 n.7.) But *Netscape* involved discovery by a government agency, which is the primary focus of the SCA (other than hackers), and did not address discovery by private litigants. Specifically, *Netscape* held that section 2703's explicit provision for the use of "trial subpoenas" by government agencies necessarily precludes an agency from seeking discovery through a pre-trial discovery subpoena. 196 F.R.D. at 561. The SCA was intended to carefully regulate government access to private email communications, and the court's interpretation of section 2703 is consistent with that intent. In contrast, the exception that allows for discovery in response to civil subpoenas, section 2702(b)(5), is broad and does not specify particular types of discovery to the exclusion of others. *See* Section II(B), *infra*.

[6] That *Theofel* involved a claim for unauthorized access under section 2701 rather than wrongful disclosure under section 2702 does not change this analysis. The Ninth Circuit in *Theofel* spent six pages considering whether egregious flaws in the civil subpoena to the email service provider transformed that otherwise legitimate discovery request into unauthorized access of the provider's facility. 359 F.3d at 1072-77. But if section 2702 barred *any* disclosure in response to a civil subpoena, the court's detailed analysis could have been replaced with a single sentence asserting that the disclosure was "unauthorized" under section 2701 because section 2702 bars all such discovery.

pursuant to court order); Videotape Privacy Protection Act, 18 U.S.C. § 2710(b)(2)(F) (providing for disclosure of video rental activity pursuant to a court order in a civil proceeding); Gramm-Leach-Bliley Act, 15 U.S.C. § 6802(e)(8) (allowing a financial institution to disclose nonpublic personal information to comply with a properly authorized civil subpoena or judicial process); Health Insurance Portability and Accountability Act, 45 C.F.R. §§ 160-164 (providing for the disclosure of confidential medical records in response to a subpoena or discovery request); *see also ICG Communications, Inc. v. Allegiance Telecom*, 211 F.R.D. 610, 612-614 (N.D. Cal. 2002) (interpreting the Telecommunications Act as allowing civil discovery of confidential customer information pursuant to civil subpoena under 47 U.S.C. § 222(c)). Even the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, allows a civil litigant to obtain transcripts of intercepted telephone communications from the government. *See In re Motion to Unseal Elec. Surveillance Evidence*, 965 F.2d 637, 641-42 (8th Cir. 1992); *In re High Fructose Corn Syrup Antitrust Litig.*, 216 F.3d 621, 624 (7th Cir. 2000).

The SCA does not create the absolute barrier to civil discovery claimed by *Amici IV* and Petitioners.

B. Apple's Subpoena To Nfox Falls Within The SCA's Provisions Authorizing Disclosure Of Certain Communications.

Amici IV also contend that Apple's subpoena to Nfox does not fall within any of the SCA provisions expressly authorizing disclosures. (*Amici IV* Br. at 7-9.) This argument is fundamentally flawed because it fails to address the specific exception that allows for Apple's discovery.

Amici IV correctly recognize that the SCA has three general categories of provisions authorizing disclosures of stored communications. First, the SCA allows disclosures that are authorized by the sender or

recipient of the communication. 18 U.S.C. § 2702(b)(1), (3). Second, the SCA permits disclosures that are necessary for "the protection of the rights or property of the provider of that service." 18 U.S.C. § 2702(b)(5). Third, the SCA permits certain disclosures to government entities. 18 U.S.C. § 2702(b)(2), (6)-(8).

But *Amici IV* ignore the second category entirely. Instead, they argue that the civil discovery at issue does not fall within the exceptions to the SCA because (1) Petitioners have not consented to disclosure, (*Amici IV* Br. at 8), and (2) Apple is not a government agency, (*Id.* at 8-9).

As Apple explained in its opposition to the Petition, subsection (b)(5) is a broad category that includes the civil discovery at issue. (Opp'n at 35.)[7] Nfox faces valid civil subpoenas – reviewed and approved by the trial court – and faces civil contempt if it does not comply.[8] Thus, the SCA authorizes Nfox to comply with Apple's court-approved civil subpoenas to protect itself from a contempt judgment.[9]

---

[7] The exception for civil discovery in subsection (b)(5) is consistent with the provisions for government discovery of email communications in section 2703. Government agencies cannot avoid the restrictions of section 2703 by seeking discovery under subsection (b)(5) because the specific framework for government discovery in section 2703 trumps the general exception that allows for civil discovery. *See San Francisco Taxpayers Ass'n v. Bd. of Supervisors*, 2 Cal. 4th 571, 577 (1992) (a specific provision of a statute "relating to a particular subject will govern in respect to that subject, as against a general provision, although the latter, standing alone, would be broad enough to include the subject to which the more particular provision relates").

[8] The notion that the SCA would preempt a contempt judgment fails because its conclusion depends on the assumption that the SCA bars all civil discovery in the first instance.

[9] Contrary to *Amici IV*'s assertions, the fact that section 2702(c) permits a service provider to disclose non-content information does not preclude discovery of email communications under subsection (b)(5). (*Amici IV* Br. at 12-13.) The SCA provisions allowing for disclosure of non-content information are entirely distinct from the provisions allowing for discovery

The safe harbor in section 2707(e) further confirms that the SCA permits an email service provider to produce email communications to civil litigants. *See* 18 U.S.C. § 2707(e). Section 2707(e)'s explicit defense for a service provider that discloses emails in good faith reliance on a court order or legal process would be nonsensical if the SCA in fact barred all civil discovery.

Amici IV try to account for this discrepancy by arguing that section 2707(e) only provides a defense for disclosures in response to government-initiated discovery. (*Amici IV* Br. at 10.) But nothing in the language of section 2707(e) limits the application of this defense to disclosures in government-initiated cases. In fact, section 2707(e) specifically indicates that governmental requests under section 2703 are only one variety of accepted discovery. *See* 18 U.S.C. § 2707(e)(1).

Moreover, *Amici IV*'s attempt to restrict section 2707(e) to government-initiated discovery would render that provision entirely superfluous in light of the protection provided in section 2703(e). Section 2703 regulates discovery from email service providers by government agencies in criminal and government-initiated civil cases. Like the safe harbor in section 2707(e), section 2703(e) provides that compliance with valid legal process constitutes a complete defense. *Compare* 18 U.S.C.

---

of the contents of stored communications. *See* Kerr, *A User's Guide*, 72 Geo. Wash. L. Rev. at 1227-28 ("[V]oluntary disclosure of contents is regulated by 2702(b), while voluntary disclosure of noncontent records is regulated by 2702(c)."). The fact that a service provider may disclose non-content information to a private party for any reason, even absent a discovery request or subpoena, has no bearing on whether the service provider must produce email communications in response to a valid discovery request. *See* 18 U.S.C. § 2702(c); *see also* Kerr, *A User's Guide*, 72 Geo. Wash. L. Rev. at 1220 (noting that subsection (c) allows service providers to share subscriber information with marketing firms and other third parties that want to solicit business from the service provider's customers).

§ 2703(e) ("No cause of action shall lie in any court against [a service provider] for providing [information in response to] a court order, warrant, subpoena, [or other] statutory authorization") *with* 18 U.S.C. § 2707(e) ("[G]ood faith reliance on . . . a court warrant or order . . . is a complete defense to any civil or criminal action brought under" the act). Section 2703(e) provides a defense for compliance with a subpoena in a government-initiated case. The only logical interpretation of section 2707(e) is that it is distinct from section 2703(e) and applies to discovery from non-government litigants.

C. Email Service Providers Do Not Face An Undue Burden From The Civil Discovery Allowed Under The SCA.

Amici IV complain that the burden of responding to civil subpoenas is so onerous that it could threaten the health of the entire Internet services industry. (*Amici IV* Br. at 18-19.) But *Amici IV* provide no evidence supporting this dire prediction.[10] Nfox, the company directly facing the

---

[10] *Amici IV* ascribe significant import to the fact that the SCA neither compensates email service providers for responding to civil subpoenas nor requires notice to a subscriber whose emails have been subpoenaed. (*Amici IV* Br. at 13, 19.) But the omission of such provisions from the SCA is not a reflection of a bar on civil discovery; instead, it is a reflection of the fact that established civil discovery rules govern the compensation and notice required for such subpoenas. *See, e.g.*, Cal. Civ. Proc. Code § 2020(d); Cal. Evid. Code § 1563(b) (party propounding civil subpoena must compensate responding party for reasonable costs incurred in locating, storing, and producing records); Cal. Civ. Proc. Code § 2025(c) (subpoena must be served on every party who has appeared in the action); Cal. Civ. Proc. Code § 1985.3 (providing for notice when consumer's personal records are subpoenaed from certain third parties); Fed. R. Civ. P. 45(c)(2)(B) (order compelling a party to respond to a subpoena must protect that party from expenses incurred in responding to that discovery); *see also In re First Am. Corp.*, 184 F.R.D. 234, 240 (S.D.N.Y. 1998) (party requesting discovery may be ordered to pay for nonparty's expenses in complying with subpoena for documents or other materials).

"undue burden" claimed by *Amici IV*, has not complained of any burden posed by responding to Apple's subpoena. Instead, Nfox has asserted that it is ready and willing to provide the requested emails. (*See* Eberhart Decl. in Support of Opp'n to Mot. ¶ 10 (Ex. 25 at 379:9-11).)

All companies face some burden from responding to third-party discovery. Indeed, the publicly available terms of service of several members of *Amici IV* specifically inform their subscribers that they will produce the contents of stored email communications in response to civil discovery requests. (*See* Declaration of David R. Eberhart in Support of Apple's Response to *Amici Curiae* Briefs ¶¶ 4-6, Exs. 3-5.) While *Amici IV* might prefer to be immunized from the generally-applicable rules of civil procedure, the SCA does not elevate email service providers above the obligations of responding to third party civil discovery.

In sum, *Amici IV* fail to provide a compelling reason to overturn the trial court's decision. They greatly overstate the reach of the SCA and ignore the key exception that allows Nfox to comply with Apple's subpoena.[11]

---

[11] Apple notes that the *amicus curiae* brief filed by Genentech interprets Apple's subpoena to Nfox as requesting only non-content subscriber information. (Genentech Br. at 13-15.) For that reason, Genentech's brief only addresses the provisions of the SCA that allow for disclosure (even absent a subpoena) of such information. *See* 18 U.S.C. § 2702(c)(6). Although subsection (c)(6) certainly allows Nfox to disclose any non-content information related to the PowerPage emails at issue – including the email addresses of individuals that forwarded the stolen Asteroid information – Apple's subpoena clearly requires production of the contents of these emails as well.

III. PETITIONERS' *AMICI* RAISE NEW ISSUES THAT ARE NOT PROPERLY BEFORE THE COURT OR RELEVANT TO THE MATTERS PRESENTED IN THE PETITION.

Petitioners' *amici* raise several issues that go far beyond the scope of the petition. *Amici IV* contend that Apple's subpoena to Nfox violates the trade secret thieves' purported First Amendment right to remain anonymous. (*Amici IV* Br. at 14-17.) *Amici II* argue that Petitioners' potential complicity in trade secret misappropriation is irrelevant because Petitioners are immune from liability for acquiring and disseminating that information. (*Amici II* Br. at 24-34.) They also argue that journalistic privileges, such as the Federal Privilege, cannot be overcome by characterizing a journalist's otherwise legal news gathering or publishing activity as tortious or illegal. (*Id.* at 34-36.)

The Court should reject *amici*'s improper attempts to broaden the scope of these proceedings. It is well established that *amici* are required to take the case as they find it and cannot introduce issues not raised by the parties themselves. These arguments should be rejected on that basis alone. *See Bruno v. Superior Court*, 219 Cal. App. 3d 1359, 1365 (1990); *San Franciscans for Reasonable Growth v. City and County of San Francisco*, 209 Cal. App. 3d 1502, 1515 n.10 (1989); *Interinsurance Exch. v. Spectrum Inv. Corp.*, 209 Cal. App. 3d 1243, 1258-59 (1989).

Even if the Court addresses the substance of these arguments, none provides a reason to overturn the trial court's decision.

A. The Trade Secret Thieves Have No Right To Remain Anonymous.

Petitioners previously claimed that Apple's discovery was barred by the rights of individuals, writing under the pseudonyms "Kasper Jade" and "Dr. Teeth" to remain anonymous. (Mot. at 13 (Ex. 16 at 122:1-123:15).) The trial court did not address this issue – presumably because it agreed

with Apple that issues beyond the subpoena to Nfox were not ripe – and Petitioners abandoned it in their petition.

Amici IV make an entirely new anonymity argument. They argue that Apple's subpoena to Nfox threatens the trade secret thieves' right to speak anonymously over the Internet. (*Amici IV* Br. at 14-17.) But the individuals who stole Apple's trade secrets have no right to remain anonymous.

First, *Amici IV* ignore an important part of the right to speak anonymously. The First Amendment does not provide a right to prevent discovery of purely private communications. Instead, the First Amendment protects an individual's right to speak anonymously ***in a public forum***. All of the cases cited by *Amici IV* involve the right of an individual to broadcast his or her views anonymously on the Internet. *Doe v. 2TheMart.com*, 140 F. Supp. 2d 1088, 1091-92 (W.D. Wash. 2001) (discussing the qualified right to post anonymous messages on an Internet message board); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D. Cal. 1999) (anonymous owner of website that infringed plaintiff's trademark not entitled to remain anonymous); *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 510 (S.D.N.Y. 2004) (discussing the general right of an individual to broadcast views anonymously over the Internet).

None of these cases stands for the proposition, advanced by *Amici IV*, that the qualified right to anonymous speech in a public forum precludes discovery of private email communications. Their proposed expansion of this right would prevent discovery of every letter, phone call, or email between two people where one of the parties to the communication was not already known.

Second, even if the right to anonymous speech were properly at issue, the purported right to anonymity must yield for the same reasons that the Federal Privilege is overcome in this case. An anonymous Internet user

cannot maintain her anonymity in order to avoid the legitimate consequences of her own misdeeds. "The preference for anonymity of those confidential informants involved in actual criminal conduct is presumably a product of their desire to escape criminal prosecution, and this preference, while understandable, is hardly deserving of constitutional protection." *Branzburg*, 408 U.S. at 691.

Courts have thus held that a plaintiff's need to identify an anonymous individual in order to name him as a defendant overcomes the qualified anonymity right. *See Seescandy.com*, 185 F.R.D. at 578-80 (anonymous creator of Internet website address that infringed on the plaintiff's trademark was not entitled to remain anonymous to avoid service of process); *Sony Music Entm't, Inc. v. Does 1-40*, 326 F. Supp. 2d 556, 564-67 (S.D.N.Y. 2004); *Alvis Coatings, Inc. v. John Does 1-10*, No. 3L94 CV 374-H, 2004 WL 2904405, at *3-4 (W.D.N.C. Dec. 2, 2004) (plaintiff entitled to subpoena identity of anonymous individuals to name them as defendants).

Thus, unmasking an anonymous potential defendant is warranted where (1) the discovery is in good faith and central to the claims at issue, (2) the plaintiff attempted to obtain this information through less intrusive means, and (3) the plaintiff has made a *prima facie* showing on its claims. *See Seescandy.com*, 185 F.R.D. at 578; *Sony Music*, 326 F. Supp. 2d at 564-67; *Alvis Coatings*, 2004 WL 2904405, at *3.

These factors are nearly identical to the second, third, and fifth *Mitchell* factors. For the reasons addressed in Apple's opposition, (Opp'n at 17-28), they are easily met in this case. Moreover, the trial court made specific factual findings establishing that Apple's discovery satisfies each of these factors. Mar. 11, 2005 Order at 10-11 (Ex. 34 at 463:16-23, 464:6-8) (finding that Apple's discovery was central to its claims, that Apple had

pursued all reasonable alternative sources of the information, and that Apple had made a *prima facie* showing).

Thus, even if the right to anonymous speech were properly at issue, Apple's right to seek redress from the individuals who stole its trade secrets overcomes any such right.

B. The First Amendment Provides No Immunity For Trade Secret Misappropriation.

Amici II argue that Petitioners' potential complicity in the misappropriation of Apple's trade secrets is irrelevant to Apple's discovery because Petitioners are immune from liability under *Bartnicki v. Vopper*, 532 U.S. 514 (2001). (*Amici II* Br. at 25-34.)[12]

In *Bartnicki*, the Supreme Court held that the First Amendment prevented the imposition of liability under wiretapping statutes against media defendants who had lawfully acquired and subsequently broadcast a tape-recorded conversation about a matter of true public concern – a threat of violence during contentious labor negotiations. 532 U.S. at 518-19, 525. Although the communication had been illegally intercepted by a third party, the defendants had no knowledge of the illegal interception when they acquired it, and they neither encouraged nor participated in the interception. *Id.* at 525.

Amici II's reliance on *Bartnicki* is misplaced for several reasons. First and foremost, nothing in *Bartnicki* remotely suggests that a party cannot obtain discovery necessary to determine whether a journalist or a

---

[12] This argument directly contradicts Petitioners' assertion that *Bartnicki* is not relevant to the issues presented in the petition. (*See* Pet. at 44) (arguing that *Bartnicki* is "inapposite" because it did not have "anything to do with the reporter's shield, the reporter's privilege, or any other evidentiary privilege against discovery of a reporter's confidential sources and unpublished information").

source engaged in tortious or criminal conduct. Apple is entitled to discovery that is necessary to show whether Petitioners knew or had reason to know that the Asteroid trade secrets that they published on their websites had been acquired by improper means or from a person who owed Apple a duty of secrecy.

Second, the limited immunity discussed in *Bartnicki* does not protect the acquisition or dissemination of trade secrets. The Supreme Court in *Bartnicki* repeatedly emphasized that the published information at issue was protected because it related to a matter of ***great public interest***: a threat of physical violence during contentious labor negotiations between a teachers' union and a public school district. 532 U.S. at 525, 528, 533-34.

In contrast, the posts on Petitioners' websites did not relate to a matter of public concern at all. Instead, Petitioners simply reproduced Apple's trade secrets – information that Apple had a compelling right to keep secret, a right sanctioned by both civil and criminal statutes. The acquisition and dissemination of such private information is not protected under *Bartnicki*; the Supreme Court ***specifically excluded*** from its holding "disclosures of ***trade secrets*** or domestic gossip or other information of purely private concern." *Id.* at 533 (emphasis added). For that very reason, the California Supreme Court has held that *Bartnicki* offers no defense for publishing trade secrets. *Bunner*, 31 Cal. 4th at 833 ("It is something of a mystery as to how free and open debate is frustrated by offering property protection to trade secrets.").

Third, even if *Bartnicki* extended protection against liability to the innocent acquisition and subsequent dissemination of trade secrets – which the opinion refuses to do – the narrow ruling in *Bartnicki* offers no defense for a defendant who solicits and accepts information with the knowledge that it has been illegally obtained. *Bartnicki*'s holding relied on the fact that the defendants had not been involved in the illegal interception of the

published information. 532 U.S. at 525, 538. Cases after *Bartnicki* have consistently refused to grant immunity to defendants who "actively accept" information, knowing that it was obtained in violation of the law. *See Boehner v. McDermott*, 332 F. Supp. 2d 149, 168-169 (D.D.C. 2004) (rejecting First Amendment defense because the defendant knew "he was receiving a tape recording that had been illegally obtained"); *Quigley v. Rosenthal*, 327 F.3d 1044 (10th Cir. 2003) (no immunity where defendant knew information was illegally acquired); *see also Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 193 (5th Cir. 2000) (no immunity for television station that was involved in illegal acquisition of intercepted telephone conversations).

Amici II baldly assert that Petitioners' "access to the [Asteroid] information was obtained lawfully, even though the information itself may have been intercepted unlawfully by someone else." (*Amici II* Br. at 28.) But *Amici II* may not credibly argue that Petitioners innocently obtained this information when Petitioners themselves have never claimed that this is the case. (*See* Opp'n at 28) (discussing Petitioner O'Grady's failure, in two consecutive declarations, to deny that he knew the Asteroid information was a trade secret obtained in violation of a duty of confidentiality).

Moreover, the available evidence demonstrates that the information was not lawfully acquired. As discussed above in Section I(A), *supra*, the unrebutted evidence in this case is that Petitioners posted information on their websites that was copied directly from an internal Apple document stolen from a secure Apple facility. This document was prominently labeled "Apple Need-to-Know Confidential." (Zonic Decl. ¶¶ 4, 6, 19 (Ex. 28 at 396:24-397:1, 397:16-28, 403:17-19).) The acquisition of such information constitutes a violation of California's Uniform Trade Secrets Act. That Act prohibits the acquisition of a trade secret by a person "who

knows or has reason to know that the trade secret was acquired by improper means." Cal. Civ. Code § 3426.1(b)(1).

The constitutional guarantees of free speech and a free press do not offer Petitioners a defense for the misappropriation of Apple's trade secrets. *Bunner*, 31 Cal. 4th at 874-88. Nor do they serve to block Apple's discovery into the trade secret theft at issue in this case. Moreover, even if Petitioners were immune from liability – which they are not – Apple is still entitled under *Mitchell* to pursue discovery necessary to recover the stolen trade secrets and identify the persons responsible for the theft.

C. The First Amendment Does Not Shield Petitioners From Discovery Into Their Involvement In The Misappropriation Of Apple's Trade Secrets.

Amici II contend that the trial court mistakenly relied on allegations that Petitioners were guilty of misconduct in ruling that the Federal Privilege did not bar the discovery at issue. (*Amici II* Br. at 34.) They argue that under *Nicholson v. McClatchy Newspapers*, 177 Cal. App. 3d 509, 512-13 (1986), constitutional media protections cannot be overcome by characterizing a journalist's news gathering activities as tortious or illegal. (*Id.*) Thus, they claim that the Federal Privilege can only be overcome by evaluating the interests at stake under the *Mitchell* factors. (*Id.* at 35.)

Amici II's argument is unavailing for several reasons. First, it fails because the trial court did not refuse to apply the Federal Privilege on the basis of allegations of illegal behavior. Instead, the court applied *Mitchell*'s five-part test and determined that the Federal Privilege did not bar Apple's subpoena to Nfox. Mar. 11, 2005 Order at 9-10 (Ex. 34 at 463:8-464:8).

Second, *Nicholson* has no application to the facts of this case. The *Nicholson* court held that the First Amendment shielded two newspapers

from liability for invasion of privacy for reporting that the judicial appointment commission had found the plaintiff not qualified for appointment – clearly a matter of public interest. 177 Cal. App. 3d at 515. And although the commission's records were confidential, there was no prohibition on the unauthorized acquisition and disclosure of that information. *Nicholson* does not apply to the acquisition or publication of information that violates a specific statutory provision giving rise to civil or criminal sanctions, such as California's trade secret laws or the federal copyright statutes. *Id.* at 512-13 ("We agree that illegal conduct by a reporter is not privileged simply because the ultimate purpose is to obtain information to publish.").

The information at issue in *Nicholson*, moreover, was a matter of clear public concern. *Id.* at 515. By contrast, Petitioners had no right to acquire or publish Apple's trade secrets, just as they have no right to disclose an individual's personal tax information. *United Liquor*, 88 F.R.D. at 127. Nor were Petitioners entitled to publish Apple's copyrighted design for Asteroid. *Zacchini*, 433 U.S. at 576-79.

CONCLUSION

For the foregoing reasons, the *amicus curiae* briefs submitted in support of the petition do not provide reason to overturn the trial court's decision. The petition should be denied.

Dated: May 11, 2005

GEORGE A. RILEY
DAVID R. EBERHART
JAMES A. BOWMAN
IAN N. RAMAGE
O'MELVENY & MYERS LLP

By _____
David R. Eberhart
Attorneys for Real Party in Interest Apple Computer, Inc.

CERTIFICATE OF WORD COUNT

(Cal. Rules of Court Rule 14(c)(1))

The text of this brief consists of 8767 words (including footnotes) as counted by the Microsoft Word version 10.0 word-processing program used to generate this brief.

Respectfully submitted,

Dated: May 11, 2005

GEORGE A. RILEY
DAVID R. EBERHART
JAMES A. BOWMAN
IAN N. RAMAGE
O'MELVENY & MYERS LLP

By _____
David R. Eberhart
Attorneys for Real Party in Interest Apple Computer, Inc.

SF1:586406.2

PROOF OF SERVICE

I am a citizen of the United States and employed in the County of San Francisco, State of California, at the law firm of O'Melveny & Myers, located at 275 Battery Street, San Francisco, California 94111. I am not a party to this action.

On this 11th day of May, 2005 I caused to be served the following documents:

REAL PARTY IN INTEREST APPLE COMPUTER, INC.'S RESPONSE TO BRIEFS OF *AMICI CURIAE* (1) JACK M. BALKIN *ET AL.*, (2) THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS *ET AL.*, (3) BEAR FLAG LEAGUE, AND (4) UNITED STATES INTERNET INDUSTRY ASSOCIATION AND NETCOALITION;

AND

DECLARATION OF DAVID R. EBERHART IN SUPPORT OF REAL PARTY IN INTEREST APPLE COMPUTER, INC.'S RESPONSE TO *AMICI CURIAE* BRIEFS

by putting a true and correct copy thereof together with a copy of this declaration, in a sealed envelope, with delivery fees paid or provided for, for delivery via United States Mail to:

Nancy Heinen
Apple Computer, Inc.
1 Infinite Loop
Cupertino, California 95014
Telephone: (408) 996-1010

Real Party in Interest
Apple Computer, Inc.

Kurt B. Opsahl
Kevin S. Bankston
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, California 94110
Telephone: (415) 436-9333 x 108
Facsimile: (415) 436-9993

Attorneys for Petitioners Jason O'Grady, Monish Bhatia and Kasper Jade

Richard R. Wiebe
Law Offices of Richard R. Wiebe
425 California Street, Suite 2025
San Francisco, California 94104
Telephone: (415) 433-3200
Facsimile: (415) 433-6382

Attorney for Petitioners Jason O'Grady, Monish Bhatia and Kasper Jade

Thomas E. Moore III
Tomlinson Zisko LLP
200 Page Mill Road, 2nd Floor
Palo Alto, California 94306
Telephone: (650) 325-8666
Facsimile: (650) 324-1808

Attorneys for Petitioners Jason O'Grady, Monish Bhatia and Kasper Jade

Nfox.com, Inc.
C/o of Registered Agent
Charles F. Catania
3187 East Rochelle Avenue
Las Vegas, Nevada 89121

Registered Agent for Nfox.com

Thomas W. Newton
James W. Ewert
1225 8th Street, Suite 260
Sacramento, California 95814
(916) 288-6015

Attorneys for Amicus Curiae
The California Newspaper Publishers Association

David Tomlin
450 W. 33rd Street
New York, New York 10001
(212) 612-1796

Attorney for Amicus Curiae
The Associated Press

Peter Scheer
The California First Amendment Coalition
534 Fourth Street, Suite B
San Rafael, California 94901
(415) 460-5060

Attorney for Amicus Curiae
The California First Amendment Coalition

Harold W. Fuson, Jr.
Judith L. Fanshaw
The Copley Press, inc.
7776 Ivanhoe Avenue
La Jolla, California 92037
(858) 454-0411

Attorneys for Amicus Curiae
The Copley Press, Inc.

Lauren Gelman, ESq.
Center for Internet and Society
Stanford Law School
559 Nathan Abbott Way
Stanford, California 94305-8610

Attorney for Amici Curiae
Jack M. Balkin et al

Lucy A. Dalglish, Esq.
Gregg P. Leslie, Esq.
Grant D. Penrod, ESq.
1101 Wilson Blvd., Suite 1100
Arlington, Virginia 22209-2211
(703) 807-2100

Attorneys for Amicus Curiae
The Reporters Committee for Freedom of the Press

James E. Grossberg
Levine Sullivan Koch & Schulz, LLP
1041 Skyline Drive
Laguna Beach, California 92651
(949) 715-3136

Attorney for Amicus Curiae
Freedom Communications, Inc., dba The Orange County Register

Jonathan R. Donnellan
Justin Peacock
Office of General Counsel
959 Eight Avenue
New York, New York 10019
(212) 649-2000

Attorneys for Amicus Curiae
The Hearst Corporation

Karlene Goller
Los Angeles Times Communications, LLC
202 West 1st Street
Los Angeles, California 90012
(213) 237-3760

Attorney for Amicus Curiae
Los Angeles Times Communications LLC

Karole Morgan-Prager
Stephen J. Burns
The McClatchy Company
2100 Q Street
Sacramento, California 95816
(916) 321-1926

Attorneys for Amicus Curiae
The McClatchy Company

Andy Huntington
General Counsel
San Jose Mercury News
750 Ridder Park Drive
San Jose, California 95190
(408) 920-5000

Attorney for Amicus Curiae
The San Jose Mercury News

Justene Adamec
Pumilia & Adamec LLP
555 W 5th Street, Ste. 3100
Los Angeles, California 90012-1010
Telephone: (213) 622-3006
Fax: (213) 622-3006

Attorney for Amicus Curiae
Bear Flag League

Elizabeth H . Rader
Akin Gump Strauss Hauer & Feld LLP
1950 University Avenue, Suite 505
East Palo Alto, California 94303

Attorneys for Amici Curiae
United States Internet Industry Association and NetCoalition

Steven A. Hirsch
Michael D. Celio
Clement S. Roberts
Keker & Van Nest LLP
710 Sansome Street
San Francisco, California 94111-1704

Attorneys for Amicus Curiae
Genentech, Inc.

Bruce W. Sanford, Esq.
Robert D. Lystad, Esq.
Bruce D. Brown, Esq.
Baker & Hostetler LLP
1050 Connecticut Avenue, Suite 1100
Washington, DC 20036
(202) 861-1500

Attorneys for Amicus Curiae
Society of Professional Journalists

Mark Goodman, Esq.
1101 Wilson Blvd., Suite 1100
Arlington, Virginia 22209-2211
(703) 807-1904

Attorney for Amicus Curiae
The Student Press Law Center

Jeffrey Lewis
Benjamin P. Pugh
Enterprise Counsel Group, ALC
Five Park Plaza, Suite 450
Irvine, California 92614

Attorneys for Amicus Curiae
Bear Flag League

Ann Brick
American Civil Liberties Union Foundation
of Northern California
1663 Mission Street, Suite 460
San Francisco, California 94103
Telephone: (415) 621-2493

Attorney for Amicus Curiae
American Civil Liberties Union Foundation of Northern California

Sonya D. Winner
Covington & Burling
One Front Street
San Francisco, California 94111
Telephone: (415) 591-6000
Facsimile: (415) 591-6091

Attorney for Amicus Curiae the Business Software Alliance

Joel W. Nomkin
Dan L. Bagatell
Perkins Coie Brown & Bain PA
2901 N. Central Ave., Suite 2000
Phoenix, Arizona 85012
Telephone: (602) 351-8000
Facsimile: (602) 648-7000

Attorneys for Amicus Curiae
Intel Corporation

Clerk of the Court (4 copies)
California Supreme Court
350 McAllister Street
San Francisco, California 94102

Also on May 11, 2005, I caused the personal service of the above referenced documents by requesting that an agent or employee of Taylor/Price Attorney Service deliver to the recipient named below, either by handing the documents to the recipient or by leaving the documents with the receptionist or other person authorized to accept courier deliveries on behalf of the addressee:

Clerk of the Court
Santa Clara County Superior Court
for delivery to the Hon. James Kleinberg
191 North First Street
San Jose, California 95113

I declare under penalty of perjury under the laws of the State of California that the above is true and correct. Executed on this 11th day of May, 2005, at San Francisco, California.

SHIVON MEBLIN