

CASE NO. H028579

IN THE COURT OF APPEAL
OF 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
Respondents.

APPLE COMPUTER, INC.

Real Party in Interest

On Writ Review from Santa Clara County Superior Court
Case No. 04-CV-032178, The Hon. James Kleinberg, Judge

BRIEF OF AMICUS CURIAE GENENTECH, INC.

**IN SUPPORT OF REAL PARTY IN INTEREST
APPLE COMPUTER, INC.**

KEKER & VAN NEST, LLP
STEVEN A. HIRSCH - #171825
MICHAEL D. CELIO - #197998
CLEMENT S. ROBERTS - #209203
710 Sansome Street
San Francisco, CA 94111-1704
Telephone: (415) 391-5400
Facsimile: (415) 397-7188

Attorneys for Amici Curiae

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION AND STATEMENT OF INTEREST	1
II. ARGUMENT	5
A. The public has a vital interest in preserving the efficacy of intellectual-property protections, including trade-secret law.....	5
B. The trial court correctly held, on the facts of this case, that allowing limited discovery of the identities of persons who stole trade secrets would not infringe upon any legitimate journalistic activity.	8
1. In this case, the usual justification for the reporter’s privilege—to encourage speech by informants—is not merely absent, but actually negated by the State’s policy against trade-secret theft.	9
2. The federal Stored Communications Act does not apply because Apple seeks to identify the sender of the stored communications, not to obtain the substance of those communications.	13
C. The rule proposed by the petitioners would hobble innovation and massively disrupt the workplace.	15
III. CONCLUSION.....	18

TABLE OF AUTHORITIES

Page(s)

STATE CASES

<i>DVD Copy Control Association, Inc. v. Bunner</i> , 31 Cal. 4th 864 (2003).....	6, 7, 8, 9, 10, 11, 12
<i>Mitchell v. Super. Ct.</i> , 37 Cal. 3d 268 (1984).....	10, 12, 13, 15

FEDERAL CASES

<i>Jessup-Morgan v. America Online, Inc.</i> , 20 F. Supp. 2d 1105 (E.D. Mich. 1998).....	13, 14
<i>Kewanee Oil Co. v. Bicron</i> , 416 U.S. 470 (1974).....	6
<i>Religious Tech. Ctr. v. Lerma</i> , 908 F. Supp. 1362 (E.D. Va. 1995).....	8
<i>San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm.</i> , 483 U.S. 522, 536 (1987).....	7
<i>State Farm Fire & Cas. Co. v. Superior Court</i> , 54 Cal. App. 4th 625, 640 (Cal. Ct. App., 1997).....	14

FEDERAL STATUTES

Digital Millenium Copyright Act, 17 U.S.C. § 512	11
Stored Communications Act, 18 U.S.C. § 2701 <i>et seq.</i>	1, 4, 13, 15

MISCELLANEOUS

Lemley et al., <i>Software and Internet Law</i> , 203 (2d ed. 2003).....	6
Levin et al., <i>Appropriating the Returns from Industrial Research and Development</i> , 1987 BROOKINGS PAPERS ECON. ACTIVITY 783 (1987).....	6
Robert P. Merges et al., <i>Intellectual Property in the New Technological Age</i> 31 (2003).....	6

TABLE OF AUTHORITIES
(cont'd)

Page(s)

Megan M. Sunkel, Comment: And the ISPs Have It . . . But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation, 81 N.C. L. Rev. 1189 (2003)..... 14

Uniform Trade Secrets Act..... 5, 16

I. INTRODUCTION AND STATEMENT OF INTEREST

This case concerns Apple's¹ trade secrets, which were posted to Websites for all the world to see in their raw form—unmediated by any “journalistic” interpretation. The question posed in this writ proceeding is whether the trial court properly allowed Apple to subpoena an Internet Service Provider (“ISP”) to find out who e-mailed this stolen property to the Website operators. There is no dispute that these trade secrets were not independently derived or reverse-engineered, but rather, were purloined—and then published essentially “as is.” The Website operators (“petitioners”) claim that the subpoena is barred by a constitutionally based “reporter’s privilege” and by the federal Stored Communications Act.² For reasons discussed below, Genentech, Inc. urges this Court to reject those assertions and to uphold the trial court’s order.

Genentech has a strong interest in the proper resolution of this question. In this day and age, when a trade secret—indeed, any kind of secret—is never more than a few keystrokes away from global publication, companies that prosper on the strength of their intellectual property must have the ability to take reasonable steps to learn the identities of those who steal that property and arrange for it to be disseminated on the Internet.

Genentech, like Apple, is one such company. A leading biotechnology concern based in South San Francisco, Genentech uses human genetic information to design and develop new biotherapeutic agents to treat unmet medical needs.

¹ “Apple” refers to real party in interest Apple Computer, Inc.

² 18 U.S.C. § 2701 *et seq.*

Genentech currently markets 13 products, with more than 30 ongoing development projects.

Genentech depends on trade-secret law for the intellectual-property protection it needs to safeguard its substantial investments in the research and development of novel biotech drug treatments. Developing these products entails an extremely risky, expensive, and lengthy process. After discovering a viable drug candidate, Genentech spends years analyzing and testing the drug to prove that it is safe and effective. Genentech also must determine how to produce the product in large volumes while preserving the drug's safety and effectiveness. The time between discovery of a drug and market entry routinely exceeds a decade.

A recent example is Genentech's Avastin, which is the first FDA-approved therapy designed to inhibit angiogenesis, the process by which new blood vessels develop and carry vital nutrients to a tumor. The Avastin product-development effort commenced in 1989. Genentech then spent hundreds of millions of dollars developing and testing Avastin, which was approved in 2004. Avastin thus consumed 15 years of concerted effort on the part of dozens of dedicated scientists and technicians. Not until the FDA approved the drug did it become clear that Avastin would be a successful product.

But that massive investment of human effort and ingenuity could have been destroyed by the misappropriation and Internet posting of a few pages from a lab notebook or a manufacturing document. The potential damage to Genentech—both in the short term and the long term—should be obvious. But the potential damage to the public would be, if anything, even greater, if Genentech and similar

companies suddenly found themselves unable to effectively discover and deter those responsible for trade-secret theft.

Below, we offer three principal reasons why no writ relief is warranted here:

First, the public has a vital interest in the continued ability of technology companies to protect their intellectual property through trade-secret law. Trade-secret law is often the tool of choice for companies that cannot risk the cost and uncertainty of obtaining patent protection, especially when a new product is in the development stage. As such, it is the great “equalizer” between established technology companies and fledgling startups. But of perhaps greater importance is the role that trade-secret law plays in maintaining good faith and honesty in commercial dealings—ethical qualities that were sadly absent in this case.

Second, the trial court issued a reasonable and narrow order that properly balanced the fundamental values underlying trade-secret protection against those underlying First Amendment law. The trial court correctly discerned that, on the facts of this case, there was no cognizable First Amendment interest to balance, because California has enacted the Uniform Trade Secrets Act with the express purpose of chilling and suppressing the conduct that occurred here: the theft and circulation of trade-secret material. While bloggers may well be entitled to the rights and status of mainstream journalists, no “journalism” occurred here—merely the reckless global distribution of raw trade secrets that were obviously pilfered from their owner. Because it was quite apparent from the face of the documents that they were trade secrets, the result in this case should be the same regardless of

whether they had been posted on the web or published in the *Wall Street Journal*. No free-speech concern arises from the trial court's order that Nfox must disclose the identities of those who did the pilfering; nor does that order violate the federal Stored Communications Act, which bars ISPs from disclosing the *substance* of stored communications, not the identities of authors.

Third, it would hobble innovation and massively disrupt the workplace to adopt petitioners' view that Apple—which has conducted a thorough if unsuccessful in-house investigation—cannot have the discovery it seeks unless it first deposes scores of its own employees and raids their laptops and home computers. No case endorses this extreme position, which would turn the high-tech workplace into a venue where fear and distrust run rampant, morale and creativity wither, and critical documents are treated like state secrets instead of being freely circulated, criticized, and improved by and amongst employees and other authorized recipients whose work depends on access to such documents. In short, the ironic result of granting the pending petition might be that illegal and harmful conduct—the theft and publication of trade secrets—would be encouraged, while legitimate and socially useful workplace communications would be “chilled.”

For all these reasons, Genentech urges the Court to uphold the trial court's order and to deny writ relief.³

³ Due to the press of time and our inability to predict when the Court may rule on the pending writ petition, our presentation is necessarily brief. But Genentech would be pleased to render any further assistance that the Court might request.

II. ARGUMENT

A. **The public has a vital interest in preserving the efficacy of intellectual-property protections, including trade-secret law.**

The various media-oriented amici who have weighed in on this case would have the Court believe that this case pits narrow commercial interests against venerable First Amendment principles that trump all competing concerns. But their one-sided viewpoint shortchanges the public interest in preserving a system of law that has proven vital to technological progress.

When it comes to protecting the fruit of its research-and-development efforts, trade-secret law is one of the two main arrows in a corporation's intellectual-property quiver—the other being patent law. But patent law alone cannot provide all the protection that firms require when developing new technologies. For many companies, in many situations, the patent process is too costly, too lengthy, and ultimately too uncertain to protect valuable intellectual property.⁴ Trade-secret protection is, if anything, even more vital to startup companies that may have hitched their fortunes to a single product that is not yet ready to patent. For these companies, trade-secret law is an “equalizer” which

⁴ The uncertainty of patent protection stems from the possibility that a court may invalidate a patent after the inventor has disclosed her invention to the world, as patent law requires her to do. As the drafters of the Uniform Trade Secrets Act have noted, “[a] valid patent provides a legal monopoly for seventeen years [now twenty] in exchange for public disclosure of an invention. If, however, the courts ultimately decide that the Patent Office improperly issued a patent, an invention will have been disclosed to competitors with no corresponding benefit. In view of the substantial number of patents that are invalidated by the courts, many businesses now elect to protect commercially valuable information through reliance upon the state law of trade secret protection.” PREFATORY NOTE, UNIF. TRADE SECRETS ACT.

“encourages the development and exploitation of those items of lesser or different invention than might be accorded protection under the patent laws, but which . . . still have an important part to play in the technological and scientific advancement of the Nation.” *DVD Copy Control Assn., Inc. v. Bunner*, 31 Cal. 4th 864, 880 (2003) (quotation marks and citation omitted). Thus, for businesses large and small, established and fledgling, trade-secret law “encourage[s] invention in areas where patent law does not reach, and will prompt the independent innovator to proceed with the discovery and exploitation of his invention.” *Kewanee Oil C.o v. Bicron*, 416 U.S. 470, 481-85 (1974). Accordingly, “many industries rely heavily on trade secret protection to appropriate the value of their research and development.” LEMLEY ET AL., *SOFTWARE AND INTERNET LAW* 203 (2d ed. 2003). Indeed, “many industries value trade secrets *more* highly than patents as an appropriability mechanism[.]” *Id.* (emphasis added) (citing Levin et al., *Appropriating the Returns from Industrial Research and Development*, 1987 BROOKINGS PAPERS ECON. ACTIVITY 783 (1987)).

While trade-secret law has tremendous practical significance to many businesses and to our economy as a whole, it also possesses a moral dimension that is at least equally important. Thus, trade-secret law “emphasizes deterrence of wrongful acts and is therefore sometimes described as a tort theory.” ROBERT P. MERGES ET AL., *INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE* 31 (2003). In this regard, “the aim of trade secret law is to punish and prevent illicit behavior, and even to uphold reasonable standards of commercial behavior.” *Id.*

More succinctly, the California Supreme Court has observed that the primary purposes of California's trade-secret law are "to promote and reward innovation and technological development" and to "maintain commercial ethics." *Bunner*, 31 Cal. 4th at 879 (2003) (citing *San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm.*, 483 U.S. 522, 536 (1987)).

The ethical content of trade-secret law should not be taken lightly. As the *Bunner* court further observed, the basic logic of the common law of trade secrets recognizes that private parties make extensive investments in certain information that "loses its value when published to the world at large." *Id.* at 880 (quotation marks and citation omitted). "Based on this logic, trade secret law creates a property right defined by the extent to which the owner of the secret protects his interest from disclosure to others. . . . In doing so, it allows the trade secret owner to reap the fruits of its labor . . . and protects the owner's moral entitlement to these fruits[.]" *Id.* (quotation marks and citations omitted). "By sanctioning the acquisition, use, and disclosure of another's valuable, proprietary information by improper means, trade secret law minimizes the inevitable cost to the basic decency of society when one steals from another." *Id.* at 881 (quotation marks, ellipses, and citation omitted). Trade-secret law thus "recognizes that good faith and honest, fair dealing is the very life and spirit of the commercial world." *Id.* (quotation marks and citation omitted).

The conduct at issue here—posting raw, stolen, trade-secret material to the Internet—represents a direct assault on the system of trade-secret protection and, more broadly, on the spirit of "good faith and honest, fair dealing" that is "the very

life and spirit of the commercial world.” *Bunner*, 31 Cal. 4th at 881 (quotation marks and citation omitted). “As other courts who have dealt with similar issues have observed, ‘posting works to the Internet makes them generally known’ at least to the relevant people interested in the news group. Once a trade secret is posted on the Internet, it is effectively part of the public domain, impossible to retrieve. Although the person who originally posted a trade secret on the Internet may be liable for trade secret misappropriation, the party who merely downloads Internet information cannot be liable for misappropriation because there is no misconduct involved in interacting with the Internet.” *Religious Tech. Ctr. v. Lerma*, 908 F. Supp. 1362, 1368 (E.D. Va. 1995). “Once the data that constitute a trade secret are disclosed to others, or others are allowed to use those data, the holder of the trade secret has lost his property interest in the data.” *Bunner*, 31 Cal. 4th at 880 (quotation marks and citation omitted).

Thus, posting stolen trade-secret information to the Internet makes it immediately available, without risk of liability, to all of a company’s competitors throughout the world—robbing the owner of its “moral entitlement” to the fruit of its research-and-development efforts. *Id.* (quotation marks and citation omitted). Such conduct brings us closer to a world in which “organized scientific and technological research . . . become[s] fragmented, and society, as whole, would suffer.” *Id.* (quotation marks and citation omitted).

B. The trial court correctly held, on the facts of this case, that allowing limited discovery of the identities of persons who stole trade secrets would not infringe upon any legitimate journalistic activity.

The trial court issued a reasonable and narrow order that appropriately

balanced the practical, economic, and moral concerns that animate trade-secret law against the First Amendment concerns expressed by the petitioners.

1. **In this case, the usual justification for the reporter’s privilege—to encourage speech by informants—is not merely absent, but actually negated by the State’s policy against trade-secret theft.**

Even where the extraordinary remedy of *injunctive* relief has been sought in a trade-secret case—raising, unlike here, the specter of “prior restraint”—the California Supreme Court has held that “[t]he First Amendment does not prohibit courts from incidentally enjoining speech in order to protect a legitimate property right.” *Bunner*, 31 Cal. 4th at 881. *Bunner* held that the free-speech provisions of the federal and state constitutions did not bar an injunction against a Website operator who posted misappropriated trade secrets to his Website despite knowing that the secrets were acquired by improper means. *Id.* at 870. In considering the role that First Amendment values should play in its analysis, the *Bunner* court deemed it significant that the trade secrets in question consisted of “highly technical information” whose “expressive content”—if any—“therefore [did] not substantially relate to a legitimate matter of public concern.” *Id.* at 884. Thus, the appropriate test was whether the trial court’s content-neutral injunction “burden[ed] no more speech than necessary to serve the government’s interest in encouraging innovation and development.” *Id.*

Viewed in that light, the trial court’s application of the five-part *Mitchell* test (relating to the so-called “reporter’s privilege”) cannot be faulted. As the *Mitchell* court observed, the qualified privilege against compelled disclosure of reporters’ sources requires the court to “weigh the fundamental values arguing both for and

against compelled disclosure” and “must be decided on a case-by-case basis, with the trial court examining and balancing the asserted interests in light of the facts of the case before it.” *Mitchell v. Super. Ct.*, 37 Cal. 3d 268, 276 (1984).

The “fundamental value” underlying the privilege is to avoid “the possible ‘chilling effect’ [that] the enforcement of . . . broad subpoenas would have on the flow of information to the press, and so to the public.” *Id.* at 275 n.4 (quotation marks and citation omitted). Again and again, *Mitchell* reminds us that “forced disclosure of journalists’ sources might deter informants from giving their stories to newsmen.” *Id.* at 278. “A confidential source,” we are told, “might well be deterred by the threat that his identity . . . might be made public.” *Id.* at 279. This, in turn, is said to be important because “[t]he investigation and revelation of hidden criminal or unethical conduct is one of the most important roles of the press in a free society—a role that may depend on the ability of the press and the courts to protect sources who may justifiably fear exposure and possible retaliation.” *Id.* at 283.

But the very purpose of trade-secret law is to “chill” the speech of certain “informants.” It is the *avowed public policy* of the State of California to deter, punish, penalize, and generally prevent the unauthorized “flow” of trade-secret information to anyone, including the press. Indeed—as previously discussed—the *Bunner* decision explains that deterring this sort of “flow” will:

- “promote and reward innovation and technological development,”⁵
- protect the trade-secret owner’s “moral entitlement” to the fruits of his

⁵ *Bunner*, 31 Cal. 4th at 878.

efforts,⁶

- “minimize[] the inevitable cost to the basic decency of society when one steals from another,”⁷
- preserve the “good faith and honest, fair dealing” that is “the very life and spirit of the commercial world,”⁸ and
- forestall the day when “organized scientific and technological research could become fragmented, and society, as whole, would suffer.”⁹

Thus, on the facts of this case, the “fundamental value” that typically undergirds the reporter’s privilege must give way to this State’s staunch public policy against the theft of trade secrets. For this reason, the trial court correctly perceived that, when weighing the values at stake here, the scales tipped lopsidedly toward permitting the requested discovery. Critical to the court’s ruling was the fact that the posted materials consisted of a copyrighted rendering of the Asteroid product,¹⁰ technical specifications, manufacturing plans, and competitive analyses—all copied directly from a confidential set of internal Apple slides concerning the Asteroid product. The originals of these slides were prominently labelled “Apple Need-to-Know Confidential.” *See* Apple’s Opposition at 5-7. Thus, the materials in question were, on their face, indisputably, trade secrets consisting of the sort of “highly technical information” whose “expressive content”

⁶ *Id.* at 880 (quotation marks and citation omitted).

⁷ *Id.* at 881 (quotation marks, ellipses, and citation omitted)

⁸ *Id.* (quotation marks and citation omitted).

⁹ *Id.* (quotation marks and citation omitted).

¹⁰ Note that the Digital Millenium Copyright Act expressly permits a copyright owner to subpoena an ISP for identification of an alleged infringer. *See* 17 U.S.C. § 512.

does not “substantially relate to a legitimate matter of public concern.” *Bunner*, 31 Cal. 4th at 884. Indeed, petitioners do not appear to dispute that the posted material consisted of stolen trade secrets. But, like Mr. Bunner, the petitioners utterly fail to explain “how any speech addressing a matter of public concern is inextricably intertwined with and somehow necessitates disclosure of [those] trade secrets.” *Id.* at 884. From Genentech’s perspective, the situation is no different than if someone had posted the manufacturing process for Avastin on the Internet.

Thus, this case—unlike *Mitchell*—is not one in which anything remotely resembling protected “journalism” is at issue.¹¹ Here there was no “great public interest in the truthful revelation of wrongdoing”;¹² rather, the transmission of stolen information was *itself* a species of wrongdoing. Nor does this case involve the public interest in “protecting the ‘whistleblower’ from retaliation”;¹³ those who stole Apple’s trade secrets are anything but whistleblowers. Nor did the petitioners’ “reporting”—if belief may be momentarily suspended—“clearly relate to matters of public importance,” such as “serious wrongdoing by a powerful private organization” and “complicity by public officials.”¹⁴ Rather, the informants themselves—and perhaps the petitioners, who may have knowingly accepted stolen trade secrets from them—are the ones guilty of serious

¹¹ We are not arguing that “bloggers,” if that is what petitioners are, do not qualify as real “journalists.” Rather, we are saying that no “journalism” occurred here—merely the broadcasting of stolen trade secrets through the medium best calculated to utterly destroy their secrecy and thus their value as intellectual property.

¹² *Mitchell*, 37 Cal. 3d at 283.

¹³ *Id.*

¹⁴ *Id.*

malfeasance. And just as the *Mitchell* court acknowledged that “there is very little public interest in protecting the source of false accusations of wrongdoing,”¹⁵ there is very little public interest in protecting the sources of stolen trade secrets. Rather, the public interest is best served by tracking those sources down and enforcing the trade-secret laws against them.

2. The federal Stored Communications Act does not apply because Apple seeks to identify the sender of the stored communications, not to obtain the substance of those communications.

It is a telling sign of the weakness of petitioners’ “privilege” argument that petitioners have now made the federal Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, the centerpiece of their brief. *See* Writ Pet. at 21-24. But that is a mere diversion, because the Act—at most—prevents discovery of the *substance* of a *nonpublic* communication held in electronic storage by an ISP. It does *not* bar a civil litigant from demanding that an ISP disclose the *identity* of the author of a communication that violated the law or that litigant’s rights.¹⁶

Thus, in *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105 (E.D. Mich. 1998), the court held that America Online had not violated the Act by disclosing, in response to a civil subpoena, the identity of a subscriber who had posted a defamatory and harassing message on a public electronic bulletin board. The court reasoned that the Act only “prohibits disclosure of the *contents* of an electronic communication to any person or entity (18 U.S.C. § 2702) or to the

¹⁵ *Id.*

¹⁶ Apple presents compelling arguments, which we need not repeat here, that the Act provides only Fourth Amendment-like protection against governmental searches and that the Act contains exemptions that apply in this case. *See* Apple

government (18 U.S.C. § 2703) without first meeting certain restrictions.” *Id.* at 1108 (emphasis added). The Act defines “contents” as including “any information concerning the *substance, purport, or meaning*” of an electronic communication, but “not information concerning the *identity of the author* of the communication.” *Id.* (emphases added) (quoting 18 U.S.C. § 2510(8)). Thus, the court concluded that “[t]he prohibitions of the [Act] . . . are inapplicable.” *Id.*

Indeed, there is an entire class of so-called “John Doe” lawsuits in which civil litigants have successfully subpoenaed ISPs to obtain the identities of subscribers who posted anonymous defamatory messages on the Internet. These lawsuits simply could not occur if the Act barred the type of discovery sought here. *See* Megan M. Sunkel, *Comment: And the ISPs Have It . . . But How Does One Get It? Examining the Lack of Standards for Ruling on Subpoenas Seeking to Reveal the Identity of Anonymous Internet Users in Claims of Online Defamation*, 81 N.C. L. REV. 1189 (2003).

Here, Apple sought “[a]ll documents relating to *the identity of any person who supplied*” the stolen trade secrets.¹⁷ Apple’s intent obviously was not to discover the *substance* of the stolen trade secrets, as the petitioners already have posted them to the Internet and disclosed their substance to the entire world—just as the defendant in *Jessup-Morgan* “disclosed” the substance of her defamatory and harassing statement to the entire world.¹⁸ Thus, the discovery at issue here

Opp. Br. at 33-35.

¹⁷ March 11, 2005 Order at 3 (emphasis added).

¹⁸ Disclosing the identities of those who transmitted the stolen trade secrets is not equivalent to disclosing the “substance” of the stored communications. As anyone

focuses on the *identity* of the trade-secret suppliers and is not precluded by the Stored Communications Act.¹⁹

In short, the trial court properly balanced the fundamental values at stake here and produced a limited and carefully reasoned order requiring disclosure of the identities of those who supplied stolen trade secrets to the petitioners. And although they invoke a “reporter’s” privilege, petitioners can’t disguise the fact that they did nothing more than to post obviously stolen secrets on a website where the entire planet—including all of Apple’s competitors worldwide—could see and appropriate them. It would be unjust to misread the Stored Communications Act as barring reasonable and limited attempts to address such behavior.

C. The rule proposed by the petitioners would hobble innovation and massively disrupt the workplace.

Relying on *Mitchell*, petitioners contend that Apple cannot obtain the requested discovery because it failed to first exhaust all alternative sources of the desired information. But *Mitchell* does not require this. Rather, it states that discovery of reporters’ sources is “permissible only when the party seeking disclosure has no other *practical* means of obtaining the information.” *Id.* at 282 (emphasis added).

who’s ever compiled a privilege log knows, disclosing facts related to the circumstances of a communication—such as the parties to it—is not the same thing as disclosing the communication itself. See *State Farm Fire & Cas. Co. v. Superior Court*, 54 Cal. App. 4th 625, 640 (Cal. Ct. App., 1997)

¹⁹ Even if this Court were to construe Apple’s subpoena as requiring more than mere disclosure of those identities, the Court could craft its mandate to reform or minimize the order, either by requiring appropriate redaction, or by limiting the required disclosure to a list identifying the relevant persons.

Petitioners' "exhaustion" theory is anything but "practical." Apple has documented its thorough investigatory effort, in which two experienced investigators traced the posted materials back to a confidential set of slides and then interviewed all employees who had access to the slides, warning them that they could be terminated if they concealed the truth. *See* Apple Opp. Br. at 7-8. Regrettably, these efforts failed to ferret out the wrongdoers. But according to the petitioners, even though Apple now knows that Nfox has the information that Apple seeks, Apple cannot subpoena Nfox without first resorting to the extraordinary steps of deposing dozens of its own employees, demanding sworn statements, and seizing and searching employees' laptops and home computers. *See* Writ Pet. at 35-36.

Petitioners' "exhaustion" theory must be rejected for two reasons.

First, adopting that theory would require a company to conduct a needlessly disruptive and demoralizing internal investigation whenever it detects a theft of trade secrets. By subjecting many innocent employees to unpleasant and unnecessary investigatory procedures, petitioners' theory would turn the high-tech workplace into an arena of fear and intimidation, weakening the loyalty and inhibiting the creativity of highly skilled employees whose good will and job satisfaction are crucial to company performance. Employers like Apple and Genentech should not be required to traumatize the workforce to protect their trade secrets. And mandating those methods would effectively rewrite the UTSA, which requires only that an owner's efforts to maintain the confidentiality of its trade secrets be "reasonable under the circumstances." COMMENT TO UNIF. TRADE

SECRETS ACT, § 1.

Second, and more important, petitioners' "exhaustion" requirement would make trade-secret enforcement so onerous that employers would be forced to institute Draconian security measures to ensure that their trade secrets never leave the premises. Possible measures could include banning critical documents from the computer system and restricting them to hard copies stored in heavily policed reading areas protected by sign-in procedures and identity checks. Restricted access to information on a "need to know" basis could become the order of the day. But instituting those procedures would effectively undo the ease and rapidity of communication that two decades of information technology have brought to the modern workplace. It would drastically slow the exchange and refinement of ideas—and thus the pace of innovation. And that is a "chilling effect" worth thinking about.

III. CONCLUSION

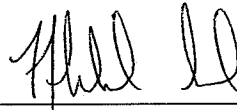
For all the reasons stated here, this Court should deny the pending writ petition.

Respectfully submitted,

Dated: April 25, 2005

KEKER & VAN NEST, LLP

By:



MICHAEL D. CELIO
Attorneys for Amicus Curiae
GENENTECH, INC.

PROOF OF SERVICE

I declare as follows:

I am employed in the City and County of San Francisco, State of California in the office of a member of the bar of this court at whose direction the following service was made. I am over the age of eighteen years and not a party to the within action. My business address is Keker & Van Nest, LLP, 710 Sansome Street, San Francisco, California 94111-1704.

On April 25, 2005, I served the following document(s):

**APPLICATION FOR LEAVE TO FILE BRIEF OF AMICUS
CURIAE GENENTECH, INC. IN SUPPORT OF
REAL PARTY IN INTEREST
APPLE COMPUTER, INC.**

**BRIEF OF AMICUS CURIAE GENENTECH, INC.
IN SUPPORT OF REAL PARTY IN INTEREST
APPLE COMPUTER, INC.**

by **COURIER**, by placing a true and correct copy in a sealed envelope addressed as shown below, and dispatching a messenger from Worldwide Network, whose address is 75 Lily Street, 3rd Floor, San Francisco, California 94102, with instructions to hand-carry the above and make delivery to the following during normal business hours, by leaving the package with the person whose name is shown or the person authorized to accept courier deliveries on behalf of the addressee.

Clerk of the Court
Court of Appeal of the
State of California (4 copies)
Sixth Appellate District
333 West Santa Clara Street, Suite 1060
San Jose, CA 95113

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

Clerk of the Court (4 copies)
California Supreme Court
350 McAllister Street
San Francisco, CA 94102-4783

by **FEDERAL EXPRESS**, by placing a true and correct copy in a sealed envelope addressed as shown below. I am readily familiar with the practice of Kecker & Van Nest, LLP for correspondence for delivery by FedEx Corporation. According to that practice, items are retrieved daily by a FedEx Corporation employee for overnight delivery.

Party Attorney Jason O'Grady, et al.: Petitioners

Thomas E. Moore
Tomlinson Zisko LLP
200 Page Mill Road, 2nd Floor
Palo Alto, CA 94306

Richard R. Wiebe
Berman DeValerio
Law Office of Richard R. Wiebe
425 California Street, Suite 2025
San Francisco, CA 94104

Kurt B. Opshal
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

Apple Computer, Inc.: Real party in interest

George A. Riley
O'Melveny & Myers LLP
Embarcadero Center West
275 Battery Street
San Francisco, CA 94111

California Newspapers Publishers Assoc.: Amicus curiae for petitioner

Thomas Newton
California Newspapers Publishers Assoc.
1225 8th Street, Suite 260
Sacramento, CA 95814

Center for Internet & Society : Amicus curiae for petitioner

Lauren Gelman
Center for Internet & Society
Stanford Law School
559 Nathan Abbott Way
Stanford, CA 94305

Bear Flag League : Amicus curiae for petitioner

Justene Adamec
Paumilia & Adamec LLP
555 W. 5th Street, Suite 3100
Los Angeles, CA 90013

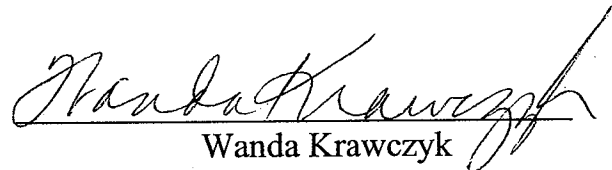
Jeffrey Lewis
Enterprise Counsel Group, ALC
Five Park Plaza, Suite 450
Irvine, CA 92614

United States Internet Society, et al. : Amicus curiae for petitioner

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

I declare under penalty of perjury under the laws of the State of California that the above is true and correct.

Executed on April 25, 2005, at San Francisco, California.


Wanda Krawczyk