Filed 5/26/06

CERTIFIED FOR PUBLICATION

IN THE COURT OF APPEAL OF THE STATE OF CALIFORNIA

SIXTH APPELLATE DISTRICT

JASON O'GRADY et al., Petitioners, v. THE SUPERIOR COURT OF SANTA CLARA COUNTY, Respondent; APPLE COMPUTER, INC., Real Party in Interest.	H028579 (Santa Clara County Super. Ct. No. CV032178)

Apple Computer, Inc. (Apple), a manufacturer of computer hardware and software, brought this action alleging that persons unknown caused the wrongful publication on the World Wide Web of Apple's secret plans to release a device that would facilitate the creation of digital live sound recordings on Apple computers. In an effort to identify the source of the disclosures, Apple sought and obtained authority to issue civil subpoenas to the publishers of the Web sites where the information appeared and to the email service provider for one of the publishers. The publishers moved for a protective order to prevent any such discovery. The trial court denied the motion on the ground that the publishers had involved themselves in the unlawful misappropriation of a trade secret. We hold that this was error because (1) the subpoena to the email service provider cannot be enforced consistent with the plain terms of the federal Stored Communications Act (18 U.S.C. §§ 2701-2712); (2) any subpoenas seeking unpublished

information from petitioners would be unenforceable through contempt proceedings in light of the California reporter's shield (Cal. Const., art. I, § 2, subd (b); Evid. Code, § 1070); and (3) discovery of petitioners' sources is also barred on this record by the conditional constitutional privilege against compulsory disclosure of confidential sources (see *Mitchell v. Superior Court* (1984) 37 Cal.3d 268 (*Mitchell*)). Accordingly, we will issue a writ of mandate directing the trial court to grant the motion for a protective order.

FACTUAL AND PROCEDURAL BACKGROUND

Petitioner Jason O'Grady declared below that he owns and operates "O'Grady's PowerPage" an "online news magazine" devoted to news and information about Apple Macintosh computers and compatible software and hardware. PowerPage has its principal place of business in Abington, Pennsylvania, and has been published daily since 1995. O'Grady acts as its publisher and one of nine editors and reporters. Since 2002 the site has occupied its present address on the World Wide Web, where it publishes 15 to 20 items per week. Over the two years preceding the execution of the declaration, the Web site received an average of 300,000 unique visits per month.[1]

Under the pseudonym " 'Kasper Jade,' " a person identifying himself as "primary publisher, editor and reporter" for Apple Insider declared that Apple Insider is an "online news magazine" devoted to Apple Macintosh computers and related products.[2] He identified petitioner Monish Bhatia as the publisher of "Mac News Network," which provides hosting services to a number of Web sites, including "Apple Insider." Apple

[1] "Unique visits" apparently refers to visits from different internet addresses, and thus corresponds to "unique visitors," which in turn corresponds roughly to the circulation of a newspaper or periodical. (See Search Engine Positioning <http://www.positioning-search-engines.com/glossary.htm#U> (as of May 23, 2006) [defining "unique visits" as "[i]ndividuals who have visited a Web site (or network) at least once in a fixed time frame, typically a 30 day period"].)

[2] Apple has not objected to this declaration on the ground that it was executed anonymously, or on any ground.

Insider has published "daily or near-daily technology news" at the same web address since 1998 at an average rate of seven to 15 articles per week. In July 2004, it received 438,000 unique visitors.

Over a period of several days in November 2004, PowerPage and Apple Insider published several articles concerning a rumored new Apple product known as Asteroid or Q97. The first article appeared on PowerPage on November 19, 2004, with O'Grady's byline. It stated that PowerPage had "got[ten] it's [*sic*] hands on this juicy little nugget about a new FireWire breakout box for GarageBand that Apple plans to announce at MacWorld Expo SF 2005 in January."[3] The article described a device that permitted the user of an Apple computer to record analog audio sources, such as microphones or guitars, using an existing Apple application known as GarageBand, the primary function of which is to facilitate the production of digital audio recordings.[4] The article included a drawing of a smallish box with a few input/output connectors. Next to the drawing was a list of further details: "FW [i.e., FireWire] based audio input device," "[t]wo inputs, two outputs," "powered from FireWire," "[s]oftware driven input gain control," and "[l]imiter circuit to automatically prevent 'clipping.' "

On the following Monday, November 22, 2004, PowerPage published an article entitled "Apple's Asteroid Breakout Box Part II: Product Details," also with O'Grady's byline. It gave additional product details plus a "[t]arget price," "[t]arget intro date," and

---

[3] As with many of the concepts in this opinion, the most authoritative and current sources of information may themselves be found on the web. Thus FireWire is described by a well-known cooperative encyclopedia as a type of serial bus interface used to connect external devices to a computer. (Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Firewire> (as of May 23, 2006).) A "breakout box" is a device "in which a compound electrical connector is separated or 'broken out' into its component connectors." (*Id*. at <http://en.wikipedia.org/ wiki/Breakout_box> (as of May 23, 2006).)

[4] See Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/ GarageBand> (as of May 23, 2006).

"[t]arget intro q[uanti]ty." Also included was a "concept drawing," attributed to "Bob Borries," which diverged substantially from the simple box depicted in the first article, more nearly resembling a small audio mixing board.

On November 23, 2004, PowerPage ran another article by O'Grady addressing Asteroid's integration into GarageBand. The article said, "Today we have some juice on new GarageBand functionality for extremely easy setup, recording and playback through Asteroid." It listed a number of details concerning the anticipated integration.

Also on November 23, 2004, an article appeared on the Apple Insider site, authored by "Kasper Jade," entitled, "Apple developing FireWire audio interface for GarageBand." It stated that the device would "allow users to directly record audio using any Mac and Apple's GarageBand music studio application," and that "[a]ccording to reputable sources, the company is on track to begin manufacturing the device overseas next month." Included was an "[a]rtist rendition" of the device "based on Apple prototype design and . . . likely [to] change." The illustration was attributed to "Paul Scates," whose email address was provided. The article recapitulated the technical details noted on the PowerPage site, adding that "a more advanced version" of the device had been "recently seen floating around the [*sic*] Apple's Cupertino campus" with an additional output port of a stated type. The article stated that it was "unclear which version the company will ultimately send to manufacturing." It noted that the device, "code-named 'Q97' or 'Asteroid,' " had been "under development" for "the better part of a year." It reported some details concerning the history of the product, identified a named Apple subsidiary as having participated in its design, and named a company with whom Apple had already contracted for its manufacture. The article stated that a production run of a specified number of units was to occur in a matter of weeks and that the product would probably be announced at an upcoming trade show. It specified a price range for the product and stated that it would "aggressively target similar products," examples of which were provided. Even at the upper end of its anticipated price range,

the article opined, the product would "represent one of the lowest priced FireWire breakout boxes on the market . . . ." Allusion was also made to "internal company estimates" concerning expected quarterly earnings from the product.

On November 26, 2004, PowerPage ran "Part IV" of its series on Asteroid, entitled "What's it all mean?" The article was bylined "Dr. Teeth and the Electric Mayhem." It alluded to an "article at createddigitalmusic," to which a hypertext link was provided, which had gone "further into the rumored Apple audio interface Asteroid, as reported here on PowerPage." Readers were advised not to "get too excited, as this hardware is similar to hardware already available, though you can probably expect a very cool box and some new software integration features . . . that may ultimately benefit even competitive audio interfaces . . . ." "Dr. Teeth" wrote that the device reflected in the "concept" drawing in the November 22, 2004 article was "probably more interesting than the product that's actually coming," as to which "[i]nside reports suggest . . . a simple 2-in, 2-out box, NOT a control surface with knobs and faders . . . ." The image shown in Apple Insider was said to be "probably dead-on" in making the product "Apple white," and "appears to be adapted from the same prototype image posted on the PowerPage," though it got one detail wrong, i.e., it showed one type of connector while "rumored specs" pointed to another, more adaptable connector type. "Dr. Teeth" observed that the product might "pave the way for future interfaces," but "only if Apple decides it wants to compete in an already-oversaturated pro market. At the entry level, Apple has one major advantage: there's nothing pretty or particularly friendly to new users, meaning this is in fact a ripe opportunity for the company's ongoing push to make Mac THE computer of music-making." Finally, "Dr. Teeth" endorsed the suggestion by createddigitalmusic that

"the codename here is credible, too: Asteroid is a play on the video game Breakout—as in audio breakout box."[5]

According to declarations later filed by Apple investigators, much of the published information appears to have originated in "an electronic presentation file—or 'slide stack,' " generated by Apple and "conspicuously marked as 'Apple Need-to-Know Confidential.' " The investigators note "striking similarities between the Confidential Slides and the articles posted on PowerPage and AppleInsider," as detailed in a portion of the declarations that remains sealed. Perhaps most telling of these similarities is an image from the presentation file that looks identical to the drawing published on PowerPage on November 19, 2004, except that the latter bears the superimposed legend "www.powerpage.org" and lacks the caption "Apple Need to Know Confidential," which appears under the image in the presentation file. Various other parts of the file are closely paraphrased, and in some cases echoed verbatim, in the articles, particularly the PowerPage articles. However, those articles also contained information not attributed by Apple to the presentation file, notably the alternative more complex design drawing. Nor did the Apple Insider articles appear to contain comparably striking similarities to the presentation file. In particular, the drawing there was designated an "Artist rendition" and attributed to one Paul Scates, whose email address was given. It differed from the

[5] This theory appears to conflate two quite different early video games, one called "Breakout" and another called "Asteroids." Descriptions of the two games in an online encyclopedia reveal no common features beyond their roughly comparable vintage. (See Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Breakout>; cf. <http://en.wikipedia.org/wiki/Asteroids_%28game%29> (as of May 23, 2006).) The author of the theory may have confused Asteroids with Arkanoid, a "clone" of Breakout. (See Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Arkanoid> (as of May 23, 2006).)

drawing in the presentation file in several particulars, i.e., it was a different color, viewed from a different angle, and appeared to have slightly different connectors.[6]

On or about December 8, 2004, O'Grady received an email from an attorney for Apple who referred to the appearance on PowerPage of "references to an unreleased Apple product, namely the [']Asteroid.[']" Citing the four articles described above, he demanded that O'Grady remove "all references to this product." He asserted, "The information in these posts and accompanying comments constitutes trade secrets that you have published without Apple[']s authorization. . . . It appears that you may be engaged in a practice of soliciting and disseminating such trade secrets. Apple also demands that you provide all information available to you regarding the sources for the posting and comments identified above. . . ."

On December 13, 2004, Apple filed a complaint against "Doe 1, an unknown individual," and "Does 2-25," whom it described as unidentified persons or entities. The gist of the claim was that one or more unidentified persons, presumably the defendants, had "misappropriated and disseminated through web sites confidential information about an unreleased product . . . ." Such information, Apple alleged, constitutes a trade secret: It possesses commercial and competitive value that would be impaired by disclosure in that, if it is revealed, "competitors can anticipate and counter Apple's business strategy, and Apple loses control over the timing and publicity for its product launches." Therefore, Apple alleged, it "undertakes rigorous and extensive measures to safeguard information about its unreleased products." All Apple employees sign an agreement acknowledging that product plans are " 'Proprietary Information' " and that " 'employment by Apple requires [employees] to keep all Proprietary Information in

[6] We also note that Apple Insider published its version of the device four days after PowerPage had made the first image public, so even if the Apple Insider version were assumed to be descended ultimately from the image in the presentation file, it would afford little basis to infer that Apple Insider had itself obtained a copy of that file.

confidence and trust for the tenure of [their] employment and thereafter, and that [they] will not use or disclose Proprietary Information without the written consent of Apple . . . .' "

Apple alleged that Doe 1, acting alone or with others, misappropriated a trade secret by "post[ing] technical details and images of an undisclosed future Apple product on publicly accessible areas of the Internet." This information, alleged Apple, "could have been obtained only through a breach of an Apple confidentiality agreement." Apple alleged that the unauthorized use and distribution of the information constituted a violation of California's trade secret statute. It prayed for compensatory and exemplary damages, and other relief.

Along with the complaint Apple filed an ex parte application for commissions and orders empowering it to "serve Subpoenas on Powerpage.org, Appleinsider.com, Thinksecret.com and any Internet service providers or other persons or entities identified in the information and testimony produced by Powerpage.org, Appleinsider.com, and Thinksecret.com." The stated basis for the application was that "the true identities of the defendants in this action cannot be ascertained without these subpoenas." The application was accompanied by a request that it and the supporting declarations be filed under seal. The trial court entered an order sealing the documents. The court then granted the application for discovery, authorizing Apple "to serve subpoenas, whether through use of commissions or in-state process, on Powerpage.com, Appleinsider.com, and Thinksecret.com for documents that may lead to the identification of the proper defendant or defendants in this action."

On February 4, 2005, Apple filed a further ex parte application seeking authorization to direct discovery to Nfox.com and Karl Kraft. Counsel for Apple declared that Kraft had contacted one of Apple's attorneys as a result of news reports about this lawsuit. Kraft said that his company, Nfox.com, hosted the email account for

PowerPage, and that numerous emails in the account contained the word " 'Asteroid.' "[7] He said he would forward copies of these messages, and other relevant documents, to counsel. Apple sought to subpoena the materials, declared counsel, because Kraft had failed to send them voluntarily. Apple sought leave to subpoena "those materials and any other documents revealing the identities of the defendants in this case."

The trial court granted the application, authorizing issuance of subpoenas requiring Nfox.com and Karl Kraft to produce "[a]ll documents relating to the identity of any person or entity who supplied information regarding an unreleased Apple product code-named 'Asteroid' or 'Q97,' " all documents identifying any such disclosing persons, all communications to or from them relating to the product, and all images received from or sent to them. The clerk duly issued a commission for such subpoenas. Counsel for Apple caused subpoenas and deposition notices to issue against Nfox and Kraft under both California and Nevada law. The parties later stipulated that these instruments were served on Nfox and Kraft on February 4 and 10, 2005, commanding compliance on February 24 and 25, 2004.

On February 14, 2005, petitioners Monish Bhatia, Jason O'Grady, and "Kasper Jade" moved for a protective order to prevent the discovery sought by Apple on the grounds that (1) their "sources and unpublished information" were "protected under the reporter's shield embodied in both Article I, section 2(b) of the California Constitution and in California Evidence Code Section 1070"; (2) the information was also protected by "the reporter's privilege under the First Amendment of the United States

[7] The significance of this report is debatable. Email stored in the account presumably includes messages between and among staff members who prepared the Asteroid pieces for publication, as well as any relevant messages that may have been received from members of the public after publication of the articles. Indeed, the email sent to O'Grady by Apple's own attorney contained the word "Asteroid" and was therefore presumably among those counted by Kraft.

Constitution," which excused petitioners "from disclosing the source of any information procured in connection with [their] journalistic endeavors"; and (3) the subpoenas already issued against Nfox and Kraft could not be enforced without violating the Stored Communications Act (18 U.S.C. § 2702(a)(1)). In support of the motion, O'Grady and Jade each declared that he had "received information about Asteroid contained in my article from a confidential source or sources."

Apple opposed the motion on the grounds that (1) the newsgatherer's privilege does not apply to trade secret misappropriation as described in the complaint; (2) if the privilege applies, it is overcome by Apple's compelling need for the information; (3) the California reporter's shield provides only an immunity from contempt, not a ground for opposing discovery; (4) petitioners are not protected by the California shield law in any event; (5) there was no right to anonymous speech under the circumstances; and (6) insofar as petitioners' motion concerned discovery other than the subpoenas to Kraft and Nfox, it was premature, and sought an advisory opinion, because no other discovery had actually been undertaken.

The court denied petitioners' motion for a protective order. In a written statement of reasons, the court first declined to reach the merits with respect to any discovery other than the subpoena served on Nfox and Kraft. It noted that no other discovery was "currently outstanding," and opined that any determination as to the propriety of such discovery would constitute an " 'advisory ruling.' " With respect to the Nfox/Kraft subpoenas, the court found that much of the information posted on PowerPage had been "taken from a confidential set of slides clearly labeled 'Apple Need-to-Know Confidential,' " and that therefore, "this action has passed the thresholds necessary for discovery to proceed." The court found petitioners' assertion of a constitutional privilege "overstated" because "[r]eporters and their sources do not have a license to violate

criminal laws such as Penal Code [section] 499c [(§ 499c)]."[8] The court assumed petitioners to be journalists, but wrote that "this is not the equivalent of a free pass" and that they could still be compelled to reveal information relating to a crime. The court repeatedly alluded to the supposed presence of criminal or larcenous conduct. The court also faulted petitioners for failing to establish "what public interest was served" by the publications in question. While acknowledging evidence that thousands of people were interested in the information in question, the court opined that "an *interested public* is not the same as the *public interest*." The court implied that the publications in question were not " 'protected speech.' "

Petitioners brought this proceeding for a writ of mandate or prohibition to compel the trial court to set aside its denial of the motion for protective order. After receiving preliminary opposition and numerous amicus curiae briefs on behalf of both sides, we issued an order to show cause.

DISCUSSION

I. *Appropriateness of Writ Review*

Rulings on discovery matters are rarely the subject of review by extraordinary writ. Such rulings are typically vested in the trial court's discretion, and even if an abuse can be shown it is often impossible for the aggrieved party to establish grounds for interlocutory intervention. At the same time, discovery issues are often vigorously

[8] Section 499c criminalizes the misappropriation or attempted misappropriation of trade secrets under specified circumstances. Although Apple alluded to this statute in its memorandum below, and does so again before us, it has never demonstrated that the facts here could establish a criminal theft of trade secrets. That offense requires proof of, among other things, "intent to deprive or withhold the control of [the] trade secret from its owner, or . . . to appropriate [the] trade secret to [the defendant's] own use or to the use of another . . . ." (§ 499c, subd. (b).) Since Apple has never argued the point, no occasion is presented to consider whether the inferred circumstances of the disclosure here could be found to constitute a crime. For present purposes we are concerned only with an allegedly *tortious* disclosure of a trade secret presumably by an Apple employee.

contested, raising a well-grounded concern that too great a willingness to grant extraordinary review would quickly magnify appellate caseloads beyond any level that could be justified by corresponding benefits. Accordingly, the review of discovery rulings by extraordinary writ is disfavored. (*Raytheon Co. v. Superior Court* (1989) 208 Cal.App.3d 683, 686; see *Oceanside Union School Dist. v. Superior Court* (1962) 58 Cal.2d 180, 185-186, fn. 4.)

Extraordinary review will be granted, however, when a discovery ruling plainly threatens immediate harm, such as loss of a privilege against disclosure, for which there is no other adequate remedy (e.g., *Raytheon Co. v. Superior Court*, *supra*, 208 Cal.App.3d at p. 686), or where the case presents an opportunity to resolve unsettled issues of law and furnish guidance applicable to other pending or anticipated cases (*Oceanside Union School Dist. v. Superior Court*, *supra*, 58 Cal.2d at pp. 185-186, fn. 4; see *Toshiba America Electronics Components v. Superior Court* (2004) 124 Cal.App.4th 762, 767).

Both of these principles appear applicable here. This case raises several novel and important issues affecting the rights of web publishers to resist discovery of unpublished material, and the showing required of an employer who seeks to compel a newsgatherer to identify employees alleged by the employer to have wrongfully disclosed its trade secrets. In part because of these issues and their implications for the privacy of internet communications, the First Amendment status of internet news sites, and the protection of trade secrets, the case has generated widespread interest within the technology sector, the digital information industry, internet content providers, and web and email users. The case also involves an attempt to undermine a claimed constitutional privilege, threatening a harm for which petitioners, if entitled to the privilege, have no adequate remedy at law. (See *Rancho Publications v. Superior Court* (1999) 68 Cal.App. 4th 1538, 1542 (*Rancho Publications*).) Accordingly, review by extraordinary writ is proper and warranted.

II. *Stored Communications Act*

A. Applicability

We first consider whether the trial court should have quashed, or granted a protective order against, the subpoenas Apple served on Nfox and Kraft, the email service providers for petitioners O'Grady and PowerPage. The dispositive issue is whether the disclosures sought by those subpoenas are prohibited by the Electronic Communications Privacy Act (Pub. Law 99-508 (Oct. 21, 1986) 100 Statutes 1860 et seq.), and specifically the chapter thereof entitled Stored Wire and Electronic Communications and Transactional Records Access (Pub. Law 99-108 (Oct. 21, 1986) 100 Stats. 1848, 1860-1868, § 201; 18 U.S.C. §§ 2701-2712), often known as the Stored Communications Act (SCA or Act). (See Stuckey, Internet and Online Law (2005) § 5.03[1][a], pp. 5-24 - 5-24.1 (rel. 18).)

The SCA declares that, subject to certain conditions and exceptions, "a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service . . . ." (18 U.S.C. § 2702(a)(1).) Similarly, but subject to certain additional conditions, "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service . . . ." (18 U.S.C. § 2702(a)(2).)

Petitioners contend that these provisions invalidate the subpoena to Nfox and Kraft under the Supremacy Clause (U. S. Const., art. VI, cl. 2). It seems plain, and Apple does not appear to dispute, that the basic conditions for application of the SCA are present: Kraft is a person, and Nfox is an entity, "providing an electronic communication service to the public." (18 U.S.C. § 2702(a)(1); see 18 U.S.C. 2510(15).) Nor has Apple tried to show that the contents of PowerPage's email account were not

"communication[s] . . . in electronic storage by" Nfox and Kraft.[9] (18 U.S.C. § 2701(a)(1); see 18 U.S.C. § 2510(17).) We therefore turn to Apple's contentions that the disclosures sought here come within enumerated exceptions to the SCA, and that the Act should be understood not to apply to civil discovery, which it was not intended to impede.

Because the issues thus joined are entirely ones of law, we exercise our independent judgment in addressing them, and accord no deference to the trial court's ruling. (*People ex rel. Lockyer v. Sun Pacific Farming Co.* (2000) 77 Cal.App.4th 619, 632; see *Enea v. Superior Court* (2005) 132 Cal.App.4th 1559, 1563.)

B. Protection of Service Provider's Interests

The SCA enumerates several exceptions to the rule that service providers may not disclose the contents of stored messages. Among the disclosures authorized are those that are incidental to the provision of the intended service (see 18 U.S.C. § 2702(b)(1), (4), (5)); incidental to the protection of the rights or property of the service provider (18 U.S.C. § 2702(b)(5)); made with the consent of a party to the communication or, in some cases, the consent of the subscriber (see 18 U.S.C. 2702(b)(3)); related to child

---

[9] The SCA defines " 'electronic storage' " to mean "temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" (18 U.S.C. § 2510(17)(A)) or "storage of such communication by an electronic communication service for purposes of backup protection of such communication" (18 U.S.C. § 2510(17)(B)). It is unclear here whether the messages in question were available to Kraft and Nfox only in backups they had made, or whether some messages had been left on the server by O'Grady or other users of the PowerPage email account. The latter possibility raises a potential issue concerning the status of messages deliberately left on the server after having been viewed by the account holder. The Ninth Circuit has held that messages are in storage for purposes of the Act even if they have already been delivered to the account holder. (*Theofel v. Farey-Jones* (9th Cir. 2004) 359 F.3d 1066, 1077; see *Quon v. Arch Wireless Operating Co., Inc.* (C.D.Cal. 2004) 309 F.Supp.2d 1204, 1207-1209; but see *In re DoubleClick Inc. Privacy Litigation* (S.D.N.Y. 2001) 154 F.Supp.2d 497, 512; *Fraser v. Nationwide Mut. Ins. Co.* (E.D.Pa. 2001) 135 F.Supp.2d 623, 636.)

abuse (18 U.S.C. § 2702(b)(6)); made to public agents or entities under certain conditions (18 U.S.C. § 2702(b)(7)), (8)); related to authorized wiretaps (18 U.S.C §§ 2702(b)(2), 2517, 2511(2)(a)(ii)); or made in compliance with certain criminal or administrative subpoenas issued in compliance with federal procedures (18 U.S.C. §§ 2702(b)(2), 2703)).

Apple contends that compliance with a civil discovery subpoena falls within the SCA's exception for disclosures that "may be necessarily incident . . . to the protection of the rights or property of the provider of that service . . . ." (18 U.S.C. § 2702(b)(5).) The argument apparently proceeds as follows: (1) Noncompliance with a subpoena would expose the service provider to contempt or other sanctions; (2) such exposure is a threat to the provider's rights or property; (3) therefore, compliance with a subpoena tends to protect the provider's rights or property. The first premise introduces a circularity by supposing that noncompliance with the subpoena can support legal sanctions. This premise is sound only where the subpoena is enforceable. A subpoena is not enforceable if compliance would violate the SCA. Any disclosure violates the SCA unless it falls within an enumerated exception to general prohibition. The exception posited by Apple necessarily presupposes that the disclosure falls within an exception. In logical terms, the antecedent assumes the consequents.

Ironically, Apple accuses petitioners of circular reasoning when they point out that if a contemplated disclosure is not authorized by the Act, the refusal to disclose cannot subject Nfox and Kraft to sanctions, and the disclosure cannot be incidental to the protection of their interests. This is at best a "tu quoque" argument, seeking to excuse the circularity in Apple's argument by accusing petitioners of the same vice. But in fact petitioners' argument is sound, while Apple's is not.

The most that could be said in Apple's support is that a service provider might incur *costs* in defending against an invalid subpoena, and that compliance might be viewed as "necessarily incident" to protecting the provider's "property" by avoiding such

costs. (18 U.S.C. § 2702(b)(5).) We seriously doubt that the language of the statute could support such a reading, which is nowhere expressly urged by Apple or its amici. The effect of such an interpretation would be to permit disclosure whenever someone threatened the service provider with litigation. Arguably even a subpoena would be unnecessary; the mere threat would be enough. Further, it is far from apparent that compliance with an invalid subpoena would save the provider any money, since it might expose the provider to a civil suit by an aggrieved user. (See 18 U.S.C. § 2707(e).) There is no reason to suppose that the defense of such a suit would be less expensive than resistance to an invalid subpoena.

C. Safe Harbor

Apple also invokes the safe harbor provisions of the SCA, under which a service provider's "good faith reliance on . . . [¶] a court warrant or order . . . [¶] is a complete defense to any civil or criminal action brought under" the SCA. (18 U.S.C. § 2707.) This provision is obviously intended to protect service providers who would otherwise find themselves between the Scylla of seemingly valid coercive process and the Charybdis of liability under the Act. It does not make compliance with such process lawful; it excuses the provider from the consequences of an unlawful act taken in good faith. In light of the legal uncertainties we here address, this provision might have afforded Nfox and Kraft a defense had they voluntarily complied with the subpoenas and then been charged with a violation of the Act. That hypothesis does not entitle Apple to invoke this provision to compel disclosures otherwise prohibited by the Act.

D. Implied Exception for Civil Discovery

Apple's primary argument for enforcing the subpoenas appears to be that Congress did not intend to "preempt" civil discovery of stored communications, and the Act should not be given that effect. Such commentary as we have found supports a

contrary conclusion.[10] However, there appears to be no judicial authority squarely addressing the issue.[11]

Apple makes no attempt to persuade us that the language of the SCA can be read to expressly authorize disclosure pursuant to civil subpoenas like those served on Nfox and Kraft. This omission is telling, because "[t]he starting point in discerning congressional intent is the existing statutory text [citation] . . . . '[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms.' [Citations]." (*Lamie v. U. S. Trustee* (2004) 540 U.S. 526, 534; see *Helvering v. N. Y. Trust Co.* (1934) 292 U.S. 455, 464 [in general, "where the statute contains no ambiguity, it must be taken literally and given effect according to its language"].)

Here there is no pertinent ambiguity in the language of the statute. It clearly prohibits any disclosure of stored email other than as authorized by enumerated exceptions. Apple would apparently have us declare an *implicit* exception for civil discovery subpoenas. But by enacting a number of quite particular exceptions to the rule

---

[10] One treatise describes the situations in which the statute authorizes disclosure and states, "All other disclosures—including disclosures of content pursuant to a third party subpoena in civil litigation—are prohibited." (Stuckey, Internet and Online Law, *supra*, § 5.03[1][a][ii], p. 5-24.2.) An internet providers' industry guide notes the absence of any express provision for compliance with such subpoenas and states, "This issue has not been litigated to our knowledge . . . . [T]he federal prohibition against divulging e-mail contents remains stark, and there is no obvious exemption for a civil discovery order on behalf of a private party." (U.S. Internet Service Providers Assn., Electronic Evidence Compliance—A Guide for Internet Service Providers (2003) 18 Berkeley Tech. L.J. 945, 965.)

[11] Apple cites *Theofel v. Farey-Jones*, *supra*, 359 F.3d 1066, 1073, for its analytical *assumption* that a civil subpoena narrowly drawn—as the one there was not—might be enforceable. The court's willingness to bypass the issue we address in order to reach a less difficult ground of decision hardly furnishes compelling support for Apple's position.

of non-disclosure, Congress demonstrated that it knew quite well how to make exceptions to that rule. The treatment of rapidly developing new technologies profoundly affecting not only commerce but countless other aspects of individual and collective life is not a matter on which courts should lightly engraft exceptions to plain statutory language without a clear warrant to do so. We should instead stand aside and let the representative branch of government do its job. Few cases have provided a more appropriate occasion to apply the maxim *expressio unius exclusio alterius est*, under which the enumeration of things to which a statute applies is presumed to exclude things not mentioned. This principle was applied to a similar issue in *F.T.C. v. Netscape Communications Corp.* (N.D.Cal. 2000) 196 F.R.D. 559, 561, where the court held that the Act's authorization for the disclosure of certain information to government agencies under a *trial* subpoena did not permit disclosure under a civil *discovery* subpoena. Noting the well-recognized distinctions between trial and discovery subpoenas, the court found "no reason . . . to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to. See *Leatherman v. Tarrant County Narcotics Intelligence and Coordination Unit*, 507 U.S. 163, 168, 113 S.Ct. 1160, 122 L.Ed.2d 517 (1993) (applying maxim of *expressio unius est exclusio alterius*)." (*Ibid*.)

Of course, a statute must be read as a whole and in light of its " 'objects and policy' " so as to " 'carry into execution the will of the Legislature, as thus ascertained, according to its true intent and meaning.' " (*Helvering v. N. Y. Trust Co.*, *supra*, 292 U.S. at p. 464.) If giving the statutory terms their " 'natural significance' " produces " 'an unreasonable result plainly at variance with the policy of the legislation as a whole,' " then courts will " 'examine the matter further,' " " 'look[ing] to the reason of the enactment and inquir[ing] into its antecedent history and giv[ing] it effect in accordance

with its design and purpose, sacrificing, if necessary, the literal meaning in order that the purpose may not fail.' " (*Id*. at pp. 464-465.)[12]

Apple provides no persuasive basis to conclude that the refusal of civil discovery would constitute an " 'unreasonable result plainly at variance with the policy of the legislation as a whole.' " (*Helvering v. N. Y. Trust Co., supra*, 292 U.S. at p. 464.) Apple asserts that the denial of civil discovery will not further the purpose of the SCA, which according to Apple is to "regulate governmental searches of email communications." But this is an unduly narrow reading of the legislative history. Apple quotes Congress's expressed intention "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." (Sen. Rep. No. 99-541, 2d Sess. (1986) reprinted in 1986 U.S. Code Cong. & Admin. News at p. 3557.) But the concluding phrase does not condition the opening one; on the contrary, it suggests an intent to protect the privacy of stored electronic communications *except where* legitimate law enforcement needs justify its infringement. The same report noted the desirability of inhibiting the "possible wrongful use and public disclosure [of stored information] by law enforcement authorities *as well as unauthorized private parties*." (*Ibid*., italics added.)

The report indicated that a fundamental purpose of the SCA is to lessen the disparities between the protections given to established modes of private communication and those accorded new communications media. It observed that while mail and telephone communications had long enjoyed a variety of legal protections, there were no "comparable Federal statutory standards to protect the privacy and security of communications transmitted by new noncommon carrier communications services or new

[12] California law, of course, is to substantially the same effect; but we are here concerned with a federal enactment, the interpretation of which is a question of federal law, and as to which federal authorities are bound to provide the surest guidance.

forms of telecommunications and computer technology . . . even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services." (Sen. Rep. No. 99-541, Sess. (1986) reprinted in 1986 U.S. Code Cong. & Admin. News at p. 3559.) Among other ill effects, this absence of standards produced "legal uncertainty" and might operate to "unnecessarily discourage potential customers from using innovative communications systems" as well as to "discourage American businesses from developing new innovative forms of telecommunications and computer technology." (*Ibid*.) Congress thus sought not only to shield private electronic communications from government intrusion but also to encourage "innovative forms" of communication by granting them protection against unwanted disclosure *to anyone*. In the absence of a degree of privacy at least roughly comparable to that accompanying more traditional modes of communication, potential users might be deterred from using the new forms merely out of a feared inability to communicate in confidence.

It bears emphasis that the discovery sought here is theoretically possible only because of the ease with which digital data is replicated, stored, and left behind on various servers involved in its delivery, after which it may be retrieved and examined by anyone with the appropriate "privileges" under a host system's security settings. Traditional communications rarely afforded any comparable possibility of discovery. After a letter was delivered, all tangible evidence of the communication remained in the sole possession and control of the recipient or, if the sender retained a copy, the parties. A telephone conversation was even less likely to be discoverable from a third party: in addition to its intrinsic privacy, it was as ephemeral as a conversation on a street corner; no facsimile of it existed unless a party recorded it—itself an illegal act in some jurisdictions, including California. (See Pen. Code, § 632.)

If an employee wished to disclose his employer's trade secrets in the days before digital communications, he would have to either convey the secret orally, or cause the

delivery, by mail or otherwise, of written documents. In the case of oral communications there would be no facsimile to discover; in the case of written communication, the original and any copies would remain in the hands of the recipient, and perhaps the sender, unless destroyed or otherwise disposed of. In order to obtain them, a civil litigant in Apple's position would have had to identify the parties to the communication and seek copies directly from them. Only in unusual circumstances would there be any third party from whom such discovery might be sought.

Given these inherent traits of the traditional media of private communication, it would be far from irrational for Congress to conclude that one seeking disclosure of the contents of email, like one seeking old-fashioned written correspondence, should direct his or her effort to the parties to the communication and not to a third party who served only as a medium and neutral repository for the message. Nor is such a regime as restrictive as Apple would make it sound. Copies may still be sought from the intermediary if the discovery can be brought within one of the statutory exceptions—most obviously, a disclosure with the consent of a party to the communication. (18 U.S.C. § 2702(b)(3).) Where a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions. (See U.S. Internet Service Providers Assn., Electronic Evidence Compliance—A Guide for Internet Service Providers, *supra*, 18 Berkeley Tech. L.J. 945, 965; *Miranda v. 21st Century Ins. Co.* (2004) 117 Cal.App.4th 913, 929 [judgment of dismissal affirmed after claimant refused discovery order to sign authorization for release of medical records]; *Emerson Electric Co. v. Superior Court* (1997) 16 Cal.4th 1101, 1112 [sanctions available against deponent who refuses to comply with order requiring him to perform demonstration or reenactment of accident].)

We also note the assertion by amicus United States Internet Industry Association (USIIA) that civil subpoenas are often served on service providers and that compliance with them would impose severe administrative burdens, interfering with the manifest

congressional intent to encourage development and use of digital communications. The severity of this burden cannot be determined from this record, but the threat of routine discovery requests seems inherent in the implied exception sought by Apple, which would seemingly permit civil discovery from the service provider whenever its server is thought to contain messages relevant to a civil suit. Thus if a plaintiff had sent email to family members about injuries that later became the subject of a negligence case, the defendant could subpoena copies of the messages from not only the service provider for the plaintiff (who might be compelled to consent) but from those of the various family members. Responding to such routine subpoenas would indeed be likely to impose a substantial new burden on service providers. Resistance would likely entail legal expense, and compliance would require devoting some number of person-hours to responding in a lawful and prudent manner. Further, routine compliance might deter users from using the new media to discuss any matter that could conceivably be implicated in litigation—or indeed, corresponding with any person who might appear likely to become a party to litigation.

It would hardly be irrational of Congress to deflect such hazards by denying civil discovery of stored messages and relegating civil litigants to such discovery as they can obtain from or through their adversaries. On the contrary, Congress could reasonably conclude that to permit civil discovery of stored messages from service providers without the consent of subscribers would provide an informational windfall to civil litigants at too great a cost to digital media and their users. Prohibiting such discovery imposes no new burden on litigants, but shields these modes of communication from encroachments that threaten to impair their utility and discourage their development. The denial of discovery here makes Apple no worse off than it would be if an employee had printed the presentation file onto paper, placed it in an envelope, and handed it to petitioners.

In other words, Congress could quite reasonably decide that an email service provider is a kind of data bailee to whom email is entrusted for delivery and secure

storage, and who should be legally disabled from disclosing such data in response to a civil subpoena without the subscriber's consent. This does not render the data wholly unavailable; it only means that the discovery must be directed to the owner of the data, not the bailee to whom it was entrusted.

Since the Act makes no exception for civil discovery and no repugnancy has been shown between a denial of such discovery and congressional intent or purpose, the Act must be applied, in accordance with its plain terms, to render unenforceable the subpoenas seeking to compel Kraft and Nfox to disclose the contents of emails stored on their facilities.

E. Disclosure Limited to Sender's Identity

Amicus Genentech argues that the SCA does not impede enforcement of the subpoenas to Kraft and Nfox because it prohibits only the disclosure of "contents of a communication" (18 U.S.C. § 2702(a)(1)) and explicitly permits a service provider to disclose, to a non-governmental entity, "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) . . ." (18 U.S.C. § 2703(c)(1)). According to Genentech, the subpoenas here do not offend the Act's prohibitions because (1) they seek only the identity of an author of a stored communication and (2) the Act expressly authorizes such disclosure.

Both premises are incorrect. Apple seeks much more than the identity of the author or authors of specified emails. Its subpoenas to Nfox and Kraft demand "[a]ll *documents relating to* the identity of any person or entity who supplied information regarding an unreleased Apple product code-named 'Asteroid' or 'Q97' . . . ," including not only "documents identifying . . . individuals who provided information relating to the

Product ('Disclosing Person(s)')," but also "*all communications from or to any Disclosing Person(s)* relating to the Product."[13]

Moreover, the logical effect of *any* affirmative response to Apple's subpoena would be to disclose the contents of communications by confirming that there are in fact stored messages on the system relating to Asteroid. Conceptually the situation resembles one in which an attorney is asked to identify all persons who sought advice on a specified legal issue, or a doctor to identify all patients who sought treatment for a specified affliction. Compliance with such an inquiry operates by simple logic to disclose the contents of privileged communications. (See *Rosso, Johnson, Rosso & Ebersold v. Superior Court* (1987) 191 Cal.App.3d 1514, 1519 [although client's identity usually not considered privileged, list of persons who contacted the firm about particular medical device was shielded from disclosure because it "would reveal the nature of a medical problem, ordinarily considered a confidential communication"].) Here, any identification of senders of messages concerning Asteroid would necessarily tend to disclose the "contents" of messages authored by those senders. (See 18 U.S.C. § 2510(8) [" 'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"].)

Further, the Act does not authorize the disclosure of the identity of the *author* of a stored message; it authorizes the disclosure of "a record or other information pertaining to a *subscriber to or customer of such service* (not including the contents of communications) . . . ." (18 U.S.C. § 2703(c)(1), italics added.) Apple already knows the identities of the subscribers to the Nfox accounts: O'Grady and PowerPage. By

---

[13] Indeed there is no way under our code to subpoena *information* as such; a subpoena can require the party served to produce documents, to appear and give testimony, or both. It is not an interrogatory.

seeking to identify the sender of communications *to* the subscriber, or the addressee of communications *from* the subscriber, Apple steps well outside the statutory authorization.

Genentech's misreading of the Act is reflected in its attempt to analogize this case to *Jessup-Morgan v. America Online, Inc.* (E.D. Mich. 1998) 20 F.Supp.2d 1105 (*Jessup-Morgan*), where the court held that the SCA did not prevent a service provider from disclosing the identity of a *subscriber* who had "post[ed] publicly on the Internet" a malicious message about another person. (*Id.* at p. 1106, italics added.) Relying on the plain statutory language, the court distinguished between "[t]he 'content' of a communication" and "information identifying an . . . account customer," which is what was disclosed there. (*Id.* at p. 1108.) The case differs starkly from this one. The party seeking disclosure there already knew the content of the stored message, which an unidentified subscriber had broadcast to the world. The only information sought was the offending subscriber's identity. Here the situation is reversed. Apple already knows the identity of the *subscriber* whose messages are at issue. What it seeks to discover are the *contents* of *private messages* stored on Nfox/Kraft's facilities. Its main target may well be the *identities of correspondents* who discussed a particular subject, but that information cannot be disclosed without disclosing contents in violation of the Act.

Genentech again overlooks this crucial distinction when it alludes to "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," stating "[t]hese lawsuits simply could not occur if the Act barred the type of discovery sought here." We need not consider the weight to be given this *argumentum ad consequentiam* because its conclusion is a non sequitur. The subpoenas before us do *not* concern a "subscriber" who "posted anonymously" on the internet, but the stored private communications of known persons who openly posted news reports based on information from confidential sources.

Indeed, Genentech's assertions on this point, as well as Apple's pleadings and argument, betray a crucial confusion of terminology. In the world of digital communications, to "post" is "[t]o *send* (a message or data) to a mailing list, newsgroup, or other *online forum* on which it *will be* displayed; to *display or make available* online."[14] Posting thus consists of directly placing material on or in a Web site, bulletin board, discussion group, newsgroup, or similar internet site or "forum," where it will appear automatically and more or less immediately to be seen by anyone with access to that forum. In short, to "post" is to *directly publish content*. If the host system is accessible to the public, the act of "posting" constitutes publication to the world.[15]

To merely supply information to someone else, who may use it or not as he chooses, is not to "post." Thus if I give someone information about an unannounced new product, and he places that information on a Web site for the public to read, it is *he* who posts it. It would be no more accurate to say *I* "posted" that information than it would be

---

[14] Online Oxford English Dictionary, Draft Additions Jun. 2003 <http://dictionary.oed.com/cgi/entry/50184816?query_type=word&queryword=post&first=1&max_to_show=10&sort_type=alpha&search_id=9sQW-SfTuBM-433&result_place=2> (as of May 23, 2006); some italics added.

[15] To be sure, there can be grey areas. Some newsgroups, discussion groups, and email discussion lists may be "moderated," meaning that one or more participants has the power either to screen content before it is posted or to "kill" it afterwards. (See Netlingo <http://www.netlingo.com/lookup.cfm?term=moderated%20mailing%20list>, as of May 23, 2006 [in "moderated mailing list," "[t]he messages are sent to the list owner first, so the moderator can review and approve them before they're distributed to subscribers."]; Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Moderator_%28communications%29>, as of May 23, 2006 [defining "forum moderator" as person with "special powers to enforce the rules of an Internet forum," which may include power to edit or delete posts].) In the latter case, which appears to be the more common, the user still "posts" a message, though subject to the moderator's power to delete it. In the former case, though some might loosely say that the user "posts" a message, the statement would blur a critical distinction. It would be more accurate to say that the user submits the message to the moderator for posting.

to say that Daniel Ellsberg "published" the Pentagon Papers or that Deep Throat "published" reports of the Watergate break-in.

News sites such as petitioners' reflect a kind and degree of editorial control that makes them resemble a newspaper or magazine far more closely than they do the primordial discussion systems that gave birth to the term "post" by analogy to the physical bulletin boards they were named and patterned after. (See *It's In the Cards, Inc. v. Fuschetto* (Wis.App. 1995) 193 Wis.2d 429, 436, 535 N.W.2d 11, 14 [noting that posting a message to a computerized bulletin board was "analogous to posting a written notice on a public bulletin board"].)[16] The ability to post the articles at issue here rested entirely in petitioners and their fellow staff members. It was they, and no one else, who "posted" the content of which Apple complains. Apple's attempt to secure copies of their correspondence thus bears no resemblance to the disclosures sought in *Jessup-Morgan*, which sought only the *identity* of a *subscriber* who had in fact *posted* offending material for the public to read.

Apple's complaint reflects a similar misapprehension in its allegation that Doe defendants, meaning *persons unknown*, "posted technical details and images of an undisclosed future Apple product on publicly accessible areas of the Internet" and "posted trade secret information about Apple's unannounced and undisclosed product prior to the date Apple intended to disclose that product to the public." The undisputed facts of record contradict any claim that *unknown* persons *posted* material on PowerPage. Five days before Apple filed the complaint, its attorney emailed petitioner O'Grady, alluding to the articles in question as "[y]our . . . post[s]." This characterization is, so far as this record shows, quite correct. Apple's subpoena to Nfox/Kraft therefore cannot be understood to seek the identify of anyone who *posted* anything on PowerPage—let alone

[16] See also Wikipedia, The Free Encyclopedia, <http://en.wikipedia.org/wiki/Bulletin_board_system> (as of May 23, 2006).

a *subscriber* who posted—because those matters are already known to Apple. What it seeks is the identities of the *sources* of content posted by O'Grady and PowerPage, information Apple believes is contained in messages in the PowerPage email account. Nothing in the SCA or in *Jessup-Morgan* suggests that such discovery is permissible.

We conclude that the outstanding subpoenas to Nfox and Kraft cannot be enforced without compelling them to violate the SCA. Since this would offend the principle of federal supremacy, the subpoenas are unenforceable, and should be quashed.

III. *Ripeness*

A. The Rule and Its Reasons

We next turn to the question whether the trial court properly refused to issue a protective order barring Apple from obtaining discovery directly from petitioners. The trial court refused to rule on the propriety of such discovery, holding that since no discovery had yet been propounded to petitioners, any ruling would constitute an advisory opinion. We consider the correctness of this ruling anew, without deference to the trial court's determination. (*Standard Alaska Production Co. v. Schaible* (9th Cir. 1989) 874 F.2d 624, 625.)

A controversy is not deemed ripe for adjudication unless it arises from a genuine present clash of interests and the operative facts are sufficiently definite to permit a particularistic determination rather than a broad pronouncement rooted in abstractions. (See *Pacific Legal Foundation v. California Coastal Com.* (1982) 33 Cal.3d 158, 169.) " 'A controversy is "ripe" when it has reached, but has not passed, the point that the facts have sufficiently congealed to permit an intelligent and useful decision to be made.' " (*Id*. at p. 171, quoting *California Water & Telephone Co. v. County of Los Angeles* (1967) 253 Cal.App.2d 16, 22.)

The doctrine arises from several considerations. The requirement of a *genuine* controversy reflects the desirability of avoiding not only collusive litigation, but cases in which one or both parties lack a real motive to diligently contest the issues. If the

competing considerations are not adequately explored and presented, the court may reach a less-than-circumspect result, potentially sending the law down a wrong precedential trail. The rule also reflects an aversion to the needless burden that courts and the public would assume if judicial resources could be diverted to resolving academic or inconsequential controversies.

The ripeness doctrine also reflects a conception that the lawmaking function of courts should generally be confined to narrow interstitial questions, questions the political branches have failed or refused to resolve, or questions (such as matters of procedure) peculiarly within the judicial bailiwick. The broader and more abstract the issues presented for adjudication, the greater is the risk of encroachment onto legislative prerogatives. Such encroachment is to be avoided not only because it offends abstract conceptions of the separation of powers, but because it provides legislators with an escape route from controversial issues for the resolution of which they ought to be responsible to the electorate.

The ripeness requirement reflects an even more fundamental recognition, i.e., that human judgment is fallible and that the risk of error increases with the level of abstraction at which a legal question is considered. The broadest holdings carry the greatest risk that details, nuances, and potential variations may be obliterated which, if naturally absorbed into the law during the incremental evolution of precedent, would lead to a different rule. In the famous words of Oliver Wendell Holmes, "The life of the law has not been logic; it has been experience. The felt necessities of the time, the prevalent moral and political theories, institutions of public policy, avowed or unconscious, even the prejudices which judges share with their fellow men, have had a good deal more to do than the syllogism in determining the rules by which men should be governed. The law embodies the story of a nation's development through many centuries, and it cannot be dealt with as if it contained only the axioms and corollaries of a book of mathematics." (Holmes, The Common Law (1923) p. 1.)

Indeed, a lawsuit resembles less a mathematical problem with a single correct solution than a chemical reaction, the result of which may depend on any number of slight variations in the ingredients used and the conditions under which the reaction occurs. One may theorize endlessly about the likely outcome of a given reaction, but the most reliable result must always come from the test of real experience. Similarly, to yield true results, a lawsuit must present a collision of concrete interests in a particularized factual context; the affected interests may then be tested by a kind of practical logic against the potentially relevant legal principles to ascertain which interests shall prevail. Depending on the nature of the conflict and the principles, the factual details of the controversy may be critical.

A fundamental goal of legal education is to instill the instinctive recognition that a particular solution to a legal problem, however obvious or indisputably correct as a generality, may appear quite intolerable with the introduction of one or two additional factual details. Justice in particular cases cannot be ensured by blind adherence to broad categorical rules, because the application of rules to particular circumstances often reveals latent defects or ambiguities within the rules themselves, or conflicts with other rules, or contradictions in the common social values on which all legal principles must ultimately rest. Such conflicts must be mediated by a deliberate and careful weighing of the effects a case may have on the values and policies implicated in it. Due attention to the facts may thus produce an exception or modification to a rule that, at a more abstract level, seemed perfectly suited to the dispute at hand.

B. Application

The facts here are sufficiently "congealed" to permit a determination of the parties' respective rights in light of the particular details of their controversy. We know what information Apple seeks, what efforts it has made to secure that information by other means, what objections petitioners raise to disclosure, and what facts they cite in support of those objections.

Apple contends that it may never enforce its rights to discovery against petitioners, as embodied in the orders here under scrutiny. However Apple has already sought to obtain records from PowerPage by serving discovery on a Texas entity, Red Widget, which Apple's attorneys then believed to be the "owner of www.powerpage.org." According to a later declaration, Apple desisted from this attempt only when the owner of Red Widget told an Apple attorney that Red Widget was merely the internet service provider for PowerPage, not its owner, and that the owner was petitioner O'Grady. Apple was apparently diverted from its attempt to seek discovery directly from PowerPage when it learned from Kraft that he and Nfox might have the information Apple sought. We have now foreclosed that avenue by holding that Apple's subpoena to Kraft and Nfox cannot be enforced without violating the Stored Communications Act. (See pt. II, *ante*.) Accordingly there is no reason to suppose that the threat of discovery from petitioners is remote or theoretical. So far as this record shows, it is imminent and concrete.

Apple suggests that, depending on what it learns about petitioners' involvement in the wrongful disclosures alleged in the complaint, it might join one or more petitioners as defendants, changing the complexion of one or more issues before us. But the ripeness doctrine does not require that events be frozen in time, only that they be fixed and specific enough to permit a reliable adjudication of the issues presented. Apple has created the present procedural circumstances; it cannot claim that they should be ignored merely because it may choose to alter them. (See pt. V(B)(1), *post*.)

Apple asserts as a categorical rule that "disputes regarding unserved discovery are premature and not ripe." It is true as a general matter that there is little to recommend an attempted adjudication of the propriety of unpropounded discovery. But this is because in the typical suit, no one can know that he is a target of discovery, or the tenor of such discovery, until it is actually propounded. This flows from the fact that discovery is ordinarily served without leave of court. (See Code Civ. Proc., §§ 2025.210 [deposition

notices], 2030.010 [interrogatories], 2031.020 [inspection of documents], 2033.020 [requests for admissions].)[17] As a result, there is ordinarily no reliable indication that discovery will be sought until it is actually served. A request for a protective order will thus appear premature, because there is nothing to protect against. Adjudication of a preemptive motion brought under such nebulous circumstances could well waste court resources, either because it ultimately proves unnecessary, or because it addresses the pertinent issues at too abstract and hypothetical a level for sound resolution.

It does not follow, however, that a subpoena or other formal discovery device is or should be an invariable precondition for adjudication of a discovery dispute. Such a device is rightly required in the typical case because it confirms the existence of a real controversy and delineates the issues to be determined. It establishes the propounding party's fixed and earnest intention to obtain information the responding party wants not to disclose. It establishes the existence and character of a concrete dispute where before there had been only speculation, and where any ruling would have been hypothetical.

Here, however, Apple made petitioners into targets of discovery by *securing orders* authorizing it to conduct discovery against them. It was required to secure such orders because, by statute, a plaintiff's power to conduct depositions without leave of court does not arise until "20 days after the service of the summons on, or appearance by, any defendant." (Code Civ. Proc., § 2025.210, subd. (b).) Not having yet named any defendant, and a fortiori having served none, Apple needed leave of court before it could propound discovery to petitioners or anyone else. By seeking and obtaining such leave, Apple ended any speculation about its intention to seek discovery from petitioners and created a concrete dispute concerning its right to do so. At that moment, the prospect of

[17] We cite the discovery statutes as amended effective July 1, 2005, and currently in effect. For present purposes these provisions appear identical in substance to those in effect when the order under review was made.

an intrusion on petitioners' interests passed from apprehensive surmise into concrete expectation.

This circumstance distinguishes the cases cited by Apple. In one of them, an internet service provider brought an action for declaratory relief seeking to establish that certain persons, whom it named as defendants, were not entitled to subpoena certain records from it. (*Pacific Bell Internet Services v. Recording Industry Ass'n of America, Inc.* (N.D.Cal. Nov. 26, 2003, No. C03-3560 SI) 2003 WL 22862662.) Two of the defendants argued that there was no actual controversy because they had merely sent letters notifying the plaintiff of their contention that some of its subscribers were engaged in copyright violations. The court agreed, holding that the case did not present an "actual controversy" under the federal Declaratory Judgment Act. (*Pacific Bell Internet Services v. Recording Industry Ass'n of America, Inc., supra*, 2003 WL 22862662, *4.) The letters did not threaten the plaintiff with litigation, the court observed, and neither of the defendants had "obtained a subpoena that is currently enforceable against" the plaintiff. (*Ibid*.) An actual controversy could not be predicated solely upon "apprehension" that the defendants "may at some future date obtain a pre-litigation subpoena which may or may not lead to a lawsuit . . . ." (*Id.* at p. *5.)

In *Morgan v. Roberts* (11th Cir. 1983) 702 F.2d 945, the court considered whether an objection to discovery had been rendered *moot* for purposes of appellate review when the objectors complied, so far as was possible, with the challenged subpoena. (*Id.* at p. 946.) The court held that the lack of any "remaining subpoenaed materials which could be produced pursuant to the district court's order," meant that "there is no issue still in litigation on which the district court could act." (*Ibid*.) Nor could the objectors invoke the exception to the mootness rule for issues likely to recur but tending to evade review, because they had failed to show a "reasonable likelihood of future subpoenas requiring them to produce similar videotapes." (*Id.* at p. 947.)

In neither of these cases was there any pending effort to obtain discovery from the complaining party. As a result, questions about the propriety of discovery were necessarily hypothetical and academic. Here, Apple has done more than give petitioners cause for "apprehension" about discovery. It has sought and obtained an order authorizing discovery against them. This moved the prospect of discovery out of the realm of the speculative and into the imminent. Apple has never abandoned the power thus acquired. On the contrary, it has impliedly reserved that power by stating that if it obtains the information it seeks from Nfox and Kraft, it "*may* have no need to send discovery directly to Petitioners at all." (Italics added.) As we have held, Apple cannot obtain the information it seeks from Nfox and Kraft. In any event, the mere possibility that it might not exercise the authority it deliberately sought and obtained does not render the dispute too ethereal for adjudication.

Again, one objective of the doctrine of ripeness is to use judicial resources efficiently. We have held that Apple may not obtain the discovery it seeks from Nfox and Kraft without causing them to violate federal law. To now hold that there is no ripe controversy concerning Apple's rights against petitioners would simply produce a multiplicity of proceedings as it returned to the trial court, subpoenaed petitioners directly, and forced them to bring a second motion for a protective order. We discern no reason to reserve half of this controversy for later adjudication.

We conclude that Apple's discovery rights against petitioners are ripe for adjudication.

IV. *California Reporter's Shield*

A. Introduction

Article I, section 2, subdivision (b), of the California Constitution provides, "A publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication . . . shall not be adjudged in contempt . . . for refusing to disclose the source of any information procured while so

connected or employed for publication in a newspaper, magazine or other periodical publication, or for refusing to disclose any unpublished information obtained or prepared in gathering, receiving or processing of information for communication to the public." Evidence Code section 1070, subdivision (a), is to substantially the same effect. Petitioners assert that these provisions, sometimes known as the California reporter's shield, preclude compelled disclosure of their sources or any other unpublished material in their possession. Apple argues that petitioners may not avail themselves of the shield because (1) they were not engaged in legitimate journalistic activities when they acquired the offending information; and (2) they are not among the classes of persons protected by the statute.[18]

Since this controversy turns on questions of statutory interpretation, it is subject to review entirely independent of the trial court's ruling. (*City of Saratoga v. Hinz* (2004) 115 Cal.App.4th 1202, 1212.) In addition, because it implicates interests in freedom of expression, we review *all* subsidiary issues, including factual ones, independently in light of the whole record. (*People v. Jackson* (2005) 128 Cal.App.4th 1009, 1021.) While this standard does not permit an original evaluation of controverted live testimony, it is the equivalent of de novo review where, as here, the trial court decided the case on a paper record fully duplicated, as this one is, before the reviewing court. (*Ibid*.)

B. "Legitimate" Journalism

Apple contends that petitioners failed to carry their burden of showing that they are entitled to invoke the shield. (See *Rancho Publications, supra,* 68 Cal.App.4th at

[18] Apple also notes that the shield has been described as only a defense to a contempt judgment and not a substantive privilege. (See *KSDO v. Superior Court* (1982) 136 Cal.App.3d 375, 379-380; *Rancho Publications, supra,* 68 Cal.App.4th at p. 1543; *Mitchell v. Superior Court* (1984) 37 Cal.3d 268, 274.) Apple offers this point, however, only with respect to the subpoenas already served on Nfox and Kraft, not those threatened against petitioners.

p. 1546, quoting *Delaney v. Superior Court* (1990) 50 Cal.3d 785, 806, fn. 20 (*Delaney*), italics omitted [burden is on journalist asserting immunity to " 'prove [that] all the requirements of the shield law have been met' "].) In particular, Apple asserts, petitioners failed to establish that they acquired the information in question while "engag[ing] in legitimate journalistic purposes," or "exercis[ing] judgmental discretion in such activities." (*Rancho Publications*, *supra*, at p. 1545.) According to Apple, petitioners were engaged not in "legitimate journalism or news," but only in "trade secret misappropriation" and copyright violations. The trial court seemed to adopt this view, writing that "Mr. O'Grady took the information and turned around and put it on the PowerPage site with essentially no added value."

We decline the implicit invitation to embroil ourselves in questions of what constitutes "legitimate journalis[m]." The shield law is intended to protect the gathering and dissemination of *news*, and that is what petitioners did here. We can think of no workable test or principle that would distinguish "legitimate" from "illegitimate" news. Any attempt by courts to draw such a distinction would imperil a fundamental purpose of the First Amendment, which is to identify the best, most important, and most valuable ideas not by any sociological or economic formula, rule of law, or process of government, but through the rough and tumble competition of the memetic marketplace.

Nor does Apple supply any colorable ground for declaring petitioners' activities not to be legitimate newsgathering and dissemination. Apple asserts that petitioners merely reprinted "verbatim copies" of Apple's internal information while exercising "no editorial oversight at all." But this characterization, if accepted, furnishes no basis for denying petitioners the protection of the statute. A reporter who uncovers newsworthy documents cannot rationally be denied the protection of the law because the publication for which he works chooses to publish facsimiles of the documents rather than editorial summaries. The shield exists not only to protect editors but equally if not more to protect

newsgatherers. The primacy Apple would grant to editorial function cannot be justified by any rationale known to us.

Moreover, an absence of editorial judgment cannot be inferred merely from the fact that some source material is published verbatim. It may once have been unusual to reproduce source materials at length, but that fact appears attributable to the constraints of pre-digital publishing technology, which compelled an editor to decide how to use the limited space afforded by a particular publication. This required decisions not only about what information to include but about how to compress source materials to fit. In short, editors were forced to summarize, paraphrase, and rewrite because there was not room on their pages to do otherwise.

Digital communication and storage, especially when coupled with hypertext linking, make it possible to present readers with an unlimited amount of information in connection with a given subject, story, or report. The only real constraint now is time—the publisher's and the reader's. From the reader's perspective, the ideal presentation probably consists of a top-level summary with the ability to "drill down" to source materials through hypertext links. The decision whether to take this approach, or to present original information at the top level of an article, is itself an occasion for editorial judgment. Courts ought not to cling too fiercely to traditional preconceptions, especially when they may operate to discourage the seemingly salutary practice of providing readers with source materials rather than subjecting them to the editors' own "spin" on a story.

This view is entirely consistent with *Rancho Publications*, *supra*, 68 Cal.App.4th 1538, on which Apple relies heavily. The court there held that the publisher of an "advertorial," i.e., a paid advertisement in the form of editorial content (*id*. at p. 1541, fn. 1), could not claim the newsgatherer's shield where there was no evidence that the publisher had done anything more than *sell space* on its pages to the anonymous originators of an allegedly tortious publication (*id.* at pp. 1545-1546). The court did not find a categorical exemption from the privilege, but held instead that the publisher had

failed to carry its burden of showing that it had acquired the information sought while engaged in activities related to newsgathering. (*Id*. at p. 1546.)Apple's attempt to bring the present case within this holding must fail because there is no basis to conclude, and it does not appear, that petitioners simply opened their Web sites to anonymous tortfeasors, for a fee or otherwise. Rather it appears that petitioners came into possession of, and conveyed to their readers, information those readers would find of considerable interest.

The result in *Rancho Publications* turns on the fact not that the publisher set out source material verbatim, but that it relinquished *any* newsgathering function, sold its editorial prerogatives to another, and acted as nothing more than a paid mouthpiece. This record contains no suggestion that petitioners provided such a service. Rather, like any newspaper or magazine, they operated enterprises whose *raison d'etre* was the dissemination of a particular kind of information to an interested readership. Toward that end, they gathered information by a variety of means including the solicitation of submissions by confidential sources. In no relevant respect do they appear to differ from a reporter or editor for a traditional business-oriented periodical who solicits or otherwise comes into possession of confidential internal information about a company. Disclosure of that information may expose them to liability, but that is not the question immediately of concern; the point here is that such conduct constitutes the gathering and dissemination of news, as that phrase must be understood and applied under our shield law.

C. Covered Persons

Apple contends that petitioners have failed to show that they are among "the types of persons enumerated in the [shield] law." (*Delaney*, *supra*, 50 Cal.3d at p. 805, fn. 17.) The law extends to "[a] publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication . . . ." (Cal. Const., art. I, § 2, subd. (b).) In seeking to place petitioners outside this description, Apple does not address the actual language of the statute. It simply asserts that (1) the shield law has been "repeatedly amended to include new forms of media," but "has never

been enlarged to cover posting information on a website"; (2) "[p]ersons who post such information . . . are not members of any professional community governed by ethical and professional standards"; and (3) "if Petitioners' arguments were accepted, anyone with a computer and Internet access could claim protection under the California Shield and conceal his own misconduct."

These arguments all rest on the dismissive characterization of petitioners' conduct as "posting information on a website." We have already noted the pervasive misuse of the verb "post" by Apple and allied amici. (See pt. II(E), *ante*.) Here they compound the problem by conflating what occurred here—the open and deliberate publication on a news-oriented Web site of news gathered for that purpose by the site's operators—with the deposit of information, opinion, or fabrication by a casual visitor to an open forum such as a newsgroup, chatroom, bulletin board system, or discussion group. Posting of the latter type, where it involves "confidential" or otherwise actionable information, may indeed constitute something other than the publication of news. But posting of the former type appears conceptually indistinguishable from publishing a newspaper, and we see no theoretical basis for treating it differently.

Beyond casting aspersions on the legitimacy of petitioners' enterprise, Apple offers no cogent reason to conclude that they fall outside the shield law's protection. Certainly it makes no attempt to ground an argument in the language of the law, which, we reiterate, extends to every "publisher, editor, reporter, or other person connected with or employed upon a newspaper, magazine, or other periodical publication." (Cal. Const., art. I, § 2, subd. (b).) We can think of no reason to doubt that the operator of a public Web site is a "publisher" for purposes of this language; the primary and core meaning of "to publish" is "[t]o make publicly or generally known; to declare or report openly or publicly; to announce; to tell or noise abroad; also, to propagate, disseminate (a creed or system)." (12 Oxford English Dict. (2d ed. 1989) pp. 784-785.) Of course the term "publisher" also possesses a somewhat narrower sense: "One whose business is the

issuing of books, newspapers, music, engravings, *or the like*, as the agent of the author or owner; one who undertakes the printing or production of copies of such works, and their distribution to the booksellers and other dealers, or to the public. (Without qualification generally understood to mean a *book-publisher* or (in the *U.S.*) also a newspaper proprietor.)" (*Id*. at p. 785, first italics added.) News-oriented Web sites like petitioners' are surely "like" a newspaper or magazine for these purposes. Moreover, even if petitioners' status as "publishers" is debatable, O'Grady and Jade have flatly declared that they are also editors and reporters, and Apple offers no basis to question that characterization.

D. Covered Publications

We come now to the difficult issue, which is whether the phrase "newspaper, magazine, or other periodical publication" (Cal. Const., art. I, § 2, subd. (b)) applies to Web sites such as petitioners'. Again, Apple offers little if any argument concerning the construction to be given this language, beyond the general notion that it should not extend to petitioners.

As potentially applicable here, the phrase, "newspaper, magazine, or other periodical publication" (Cal. Const., art. I, § 2, subd. (b); Evid. Code, § 1070, subd. (a)) is ambiguous. The term "newspaper" presents little difficulty; it has always meant, and continues to mean, a regularly appearing publication printed on large format, inexpensive paper. The term "magazine" is more difficult. Petitioners describe their own sites as "magazines," and Apple offers no reason to take issue with that characterization. The term "magazine" is now widely used in reference to Web sites or other digital publications of the type produced by petitioners. Thus a draft entry in the Oxford English Dictionary defines "e-zine" as "[a] magazine published in electronic form on a computer network, esp. the Internet. [¶] Although most strongly associated with special-interest fanzines only available online, *e-zine* has been widely applied: to regularly updated general-interest web sites, to electronic counterparts of print titles (general and

specialist), and to subscription-only e-mail newsletters."[19] Similarly, an online dictionary of library science defines "electronic magazine" as "[a] digital version of a print magazine, or a magazine-like electronic publication with no print counterpart (*example: Slate*), made available via the Web, e-mail, or other means of Internet access."[20] And a legal encyclopedia notes that "[a]s with newspapers, the nature of magazines has changed because of the internet. Magazines may be published solely on the internet, or as electronic adjuncts of a print magazine." (58 Am.Jur.2d (2002) Newspapers, Periodicals, and Press Associations, § 5, p. 11, fn. omitted.)

Of course, in construing an ambiguous statute, courts will "attempt to ascertain the Legislature's purpose by taking its words ' " 'in the sense in which they were understood *at the time the statute was enacted*.' " ' " (*Resure, Inc. v. Superior Court* (1996) 42 Cal.App.4th 156, 164, quoting *People v. Fair* (1967) 254 Cal.App.2d 890, 893, italics added; see *People v. Williams* (2001) 26 Cal.4th 779, 785.) The term "magazine" was added to Evidence Code section 1070 in 1974, as was "or other periodical publication." (Stats. 1974, ch. 1456, § 2, p. 3184.) Presumably the Legislature was not prescient enough to have consciously intended to include digital magazines within the sweep of the term. By the same token, however, it cannot have meant to *ex*clude them. It could not advert to them at all because they did not yet exist and the potential for their existence is not likely to have come within its contemplation.

However, even were we to decide—which we do not—that Web sites such as petitioners' cannot properly be considered "magazines" for purposes of the shield law,

---

[19] Oxford English Dictionary (Draft Entry Sept. 2001) <http://dictionary.oed.com/cgi/entry/00305686?single=1&query_type=word&queryword=e-zine&first=1&max_to_show=10> (as of May 23, 2006).

[20] Reitz, ODLIS—Online Dictionary for Library and Information Science, <http://lu.com/odlis/odlis_e.cfm#electronicmagazine> (as of May 23, 2006).

we would still have to address the question whether they fall within the phrase "other periodical publications." That phrase is obviously intended to extend the reach of the statute beyond the things enumerated (newspapers and magazines). The question is how to delineate the class of *unspecified* things thus included within the sweep of the law.

The canon of interpretation known as *ejusdem generis* is supposedly suited to just such questions. Under this doctrine, " 'where general words follow the enumeration of particular classes of persons or things, the general words will be construed as applicable only to persons or things of the same general nature or class as those enumerated.' " (*Sears, Roebuck & Co. v. San Diego County Dist. Council of Carpenters* (1979) 25 Cal.3d 317, 331, fn. 10; *Scally v. Pacific Gas & Electric Co.* (1972) 23 Cal.App.3d 806, 819.) The doctrine is said to rest on the supposition that " 'if the Legislature had intended the general words to be used in their unrestricted sense, it would not have mentioned the particular things or classes of things which would in that event become mere surplusage.' " (*Ibid*.) This may seem a tortuous and uncertain route to an inference about legislative intent, grounded as it seems to be in facile abstractions drawn from dubious semantic generalities. (See 2A Singer, Statutory Construction (6th ed. 2000), § 47.18, p. 289, fn. omitted ["The doctrine of ejusdem generis calls for more than merely an abstract exercise in semantics and formal logic. It rests on practical insights about everyday language usage . . . . The problem is to determine what unmentioned particulars are sufficiently like those mentioned to be made subject to the act's provisions by force of the general reference. In most instances there is a wide range of ways in which classes could be defined, any one of which would embrace all of the members in an enumeration. Germaneness to the subject and purpose of the statute, viewed in terms of legislative intent or meaning to others, is the basis for determining which among various semantically correct definitions of the class should be given effect"].)

The rule of *ejusdem generis* assumes that the general term chosen by the Legislature conveys a relatively "unrestricted sense." Sometimes this is so; sometimes it

is not. The rule also supposes that the operative characteristics of the enumerated things may be readily discerned from the face of the statute, but that is not necessarily the case. With or without *ejusdem generis*, the real intent of an inclusive or expansive clause must ordinarily be derived from the statutory context and, if necessary, other permissible indicia of intent. *Ejusdem generis*, with its emphasis on abstract semantical suppositions, may do more to obscure than disclose the intended scope of the clause.

Here it might be suggested that the shield law only applies to "periodical publications" *in print*, because that was a common feature of newspapers and magazines at the time the law was enacted. Yet there is no apparent link between the core purpose of the law, which is to shield the gathering of news for dissemination to the public, and the characteristic of appearing in traditional print, on traditional paper. Indeed, the shield law manifests a clear intention *not* to limit its reach to print publications by also protecting "person[s] connected with or employed by a radio or television station." (Cal. Const., art. I, § 2, subd. (b); Evid. Code, § 1070, subd. (b).) Apple alludes to the absence of any similar explicit extension to digital publications such as petitioners', but this consideration is far from compelling. No one would say that the evening news on television, or an hourly news report on radio, is a "newspaper, magazine, or other periodical publication." The broadcast media represent a radical departure from the preexisting paradigm for news sources. Because no one thought of those media as "publications," an explicit extension was necessary to ensure their inclusion. Petitioners' Web sites are not only "publications" under various sources we have noted but also bear far closer resemblance to traditional print media than do television and radio. They consist primary of text, sometimes accompanied by pictures, and perhaps occasionally by multimedia content. Radio consists entirely of sounds, and television consists almost entirely of sounds and pictures. While television could be used to deliver text, it almost never is.

For these reasons the explicit inclusion of television and radio in the shield law does not imply an exclusion of digital media such as petitioners'. As we have noted, the electorate cannot have intended to exclude those media because they did not exist when the law was enacted. The surest guide to the applicability of the law is thus its purpose and history.

As we have noted, the words "magazine, or other periodical publication" were added to the shield law in 1974. (Stats. 1974, ch. 1323, § 2, p. 2877; Stats. 1974, ch. 1456, § 2, p. 3184.) The purpose of the amendment, obviously, was to extend the statute's protections to persons gathering news for these additional publications. (Sen. Com. on Judiciary, Bill Digest of Assem. Bill No. 3148 (1973-1974 Reg. Sess.) hrg. date Apr. 16, 1974, p. 1 ["This bill broadens the scope of the privilege to include individuals connected with a magazine or other periodical"].) A senate committee report explained the bill and its potential effects as follows (see *In re J.W.* (2002) 29 Cal.4th 200, 211 ["To determine the purpose of legislation, a court may consult contemporary legislative committee analyses of that legislation, which are subject to judicial notice"]): "One effect of this bill is to clear up one ambiguity in existing law and create another. The word, 'newspaper' is not defined in the existing statute. As a result it is not clear whether the law covers periodic newsletters and other such publications. Under this bill these kinds of publications would clearly be covered. If they are technically not newspapers, they are at least periodical publications. On the other hand, it is not clear how far the words 'magazine, or other periodical publication' will stretch. For instance, would it cover legislators' occasional newsletters?" (*Id.* at p. 1.)

It is "technically" debatable whether petitioners' Web sites constitute "periodical publication[s]" within the contemplation of the statute.[21] In its narrowest sense the term

[21] Neither of the parties has directly addressed the question whether petitioners' Web sites may properly be viewed as "periodical publications." Amicus Bear Flag League, an association of "bloggers," comes nearest to the point by citing judicial

"publication" has tended to carry the connotation of printed matter. But petitioners' Web sites are highly analogous to printed publications: they consist predominantly of text on "pages" which the reader "opens," reads at his own pace, and "closes." The chief distinction between these pages and those of traditional print media is that the reader generally gains access to their content not by taking physical possession of sheets of paper bearing ink, but by retrieving electromagnetic impulses that cause images to appear on an electronic display.[22] Thus, even if there were evidence that the Legislature

---

authority defining "periodical publication" to mean a publication appearing at regular intervals. (*Houghton v. Payne* (1904) 194 U.S. 88, 96-97 [holding literary series to constitute books and not periodical publications, for purposes of postal regulations, due to lack of "continuity of literary character, a connection between the different numbers of the series in the nature of the articles appearing in them"]; *Fifeld v. American Auto. Ass'n* (D.C. Mont. 1967) 262 F.Supp. 253, 257 [annual tour guide was "book," not "periodical," so as to require notice of claimed defamation to publisher under state law].)

Amicus Bear Flag League asserts that nothing in these definitions "exclude[s] Bloggers who publish (i.e. post) fairly regularly." However, we have avoided the term "blog" here because of its rapidly evolving and currently amorphous meaning. It was apparently derived from "we blog," a whimsical deconstruction of "weblog," a compounding of "web log," which originally described a kind of online public diary in which an early web user would provide links to, and commentary on, interesting Web sites he or she had discovered. (See Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Blog> (as of May 23, 2006).) The term may now be applied to any Web site sharing some of the characteristics of these early journals. (See *ibid*.) It is at least arguable that PowerPage and Apple Insider, by virtue of their multiple staff members and other factors, are less properly considered blogs than they are "e-magazines," "ezines," or "webzines." (See Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Webzine> (as of May 23, 2006) ["A distinguishing characteristic from blogs is that webzines bypass the strict adherence to the reverse-chronological format; the front page is mostly clickable headlines and is laid out either manually on a periodic basis, or automatically based on the story type."].) However, the meanings ultimately to be given these neologisms, as well as their prospects for survival, remain unsettled.

[22] Even this distinction is permeable. A web page may readily become printed matter by sending it to the printer typically attached to a reader's computer. The distinction may be still further blurred in the near future by the development of electronic

intended the term "publication" in this narrower sense, it would be far from clear that it does not apply to petitioners' Web sites. Thus the online library science dictionary to which we have previously adverted defines "electronic publication" to include Web sites.[23]

Ambiguities also attend the term "periodical" as a modifier of "publication" in the present context. In general usage the adjective "periodical" is roughly synonymous with "recurring" or "repeating." Although it sometimes connotes a degree of regularity, it may also be applied where the recurrence lacks an inflexible frequency. Thus a leading

---

or "smart" paper, permitting the display of text and other content on a device resembling a piece of paper. (See Wikipedia, The Free Encyclopedia <http://en.wikipedia.org/wiki/Electronic_paper (as of May 23, 2006) ["There are many approaches to electronic paper, with many companies developing technology in this area."].) In a decade or two, a traveler may pull a sheet from his briefcase and use it to retrieve and read that morning's news, then mark up a draft agenda for an upcoming meeting, then work on a crossword puzzle, then resume a novel he was reading the night before. Only a sophist could relish the question whether content so displayed is "printed" matter.

[23] See ODLIS, *supra*, at <http://lu.com/odlis/odlis_e.cfm#elecpublication> (as of May 23, 2006).

In several important respects, petitioners' websites more nearly resemble traditional printed "publications" than they do the older electronic media commonly distinguished from printed matter by the generic term "broadcasting." As we have noted, radio cannot convey anything resembling printed matter, and while television can convey text it only does so incidentally, as captions or subtitles for the pictures (mostly moving) which are its raison d'être. Moreover, the recipient of broadcast content was, traditionally, almost entirely passive. He did not read, but listened or watched. He might change stations or channels, or adjust the sound or the picture, but he could not navigate within a given presentation—could not skip to the next program or go back to the previous one. It is not surprising that these media were not brought within the term "publication," which had always been applied to media that were textual, persistent, and redistributable. In these respects broadcasting more nearly resembled ephemeral productions such as plays, lectures, and concerts, whereas petitioners' Web sites have much more in common with traditional "publications" than they do with broadcasting.

dictionary defines "periodical" as "[r]ecurring after *more or less* regular periods of time . . . ." (11 Oxford English Dict., *supra*, p. 560, italics added.)

The term "periodical" is also commonly understood to apply to recurring *publications*, most notably magazines. (See 11 Oxford English Dict., *supra*, p. 560.) In the world of publishing, "periodical" refers specifically to a type of "serial" distinguished mainly by its appearance at regular intervals. (See Merriam-Webster's Collegiate Dict. (10th ed. 1999) p. 864 ["published with a fixed interval between the issues or numbers"]; American Heritage College Dict. (3d ed. 1997), p. 1016 ["[p]ublished at regular intervals of more than one day"].)[24]

It does not appear that petitioners' Web sites are published in distinct issues at regular, stated, or fixed intervals. Rather, individual articles are added as and when they become ready for publication, so that the home page at a given time may include links to articles posted over the preceding several days. This kind of constant updating is characteristic of online publications but is difficult to characterize as publication at

---

[24] See also ODLIS, *supra*, at <http://lu.com/odlis/odlis_s.cfm#serial> (as of May 23, 2006) [defining "serial" as "[a] publication in any medium issued under the same title in a succession of discrete parts, usually numbered (or dated) and appearing at regular or irregular intervals with no predetermined conclusion."]; *id*. at <http://lu.com/odlis/odlis_p.cfm#periodical> (as of May 23, 2006) ["periodical" as "[a] serial publication . . . issued . . . more than once, generally at regular stated intervals of less than a year"].

In *It's In the Cards, Inc. v. Fuschetto*, *supra*, 535 N.W.2d 11, an intermediate appellate court held that messages posted on a bulletin board system were not a "periodical" for purposes of Wisconsin's law requiring a demand for retraction of allegedly libelous matter. We certainly agree with this holding, though we take issue with some of the court's reasoning, including its refusal to analogize online text to the printed matter constituting pre-digital "periodicals."

"regular intervals." That fact, however, has not kept an online dictionary of library science from referring to such a Web site as a "periodical."[25]

Moreover, many familiar print publications universally viewed as "periodicals" (or "periodical publications") do not appear with absolute regularity. The New Yorker Magazine is considered a periodical and a magazine (a subset of periodicals) even though it publishes 47, not 52, issues a year. (*The New Yorker* (March 6, 2006), p. 93 ["published weekly (except for five combined issues . . .)"].) Similarly, the New York Review of Books is "[p]ublished 20 times a year, biweekly except in January, August, and September, when monthly." (*New York Review of Books* (Feb. 23, 2006), p. 3.)

Given the numerous ambiguities presented by "periodical publication" in this context, its applicability must ultimately depend on the purpose of the statute. (See *McGarity v. Department of Transportation* (1992) 8 Cal.App.4th 677, 682-683 [purpose of statute limiting cross-examination of experts warranted broad construction of "similar publication" and justified its application to crash impact study although it "was apparently not published for mass consumption"].) It seems likely that the Legislature intended the phrase "periodical publication" to include all ongoing, recurring news publications while excluding non-recurring publications such as books, pamphlets, flyers, and monographs. The Legislature was aware that the inclusion of this language could extend the statute's protections to something as occasional as a legislator's newsletter. (See Sen. Com. on Judiciary, Bill Digest of Assem. Bill No. 3148 (1973-1974 Reg. Sess.) hrg. date Apr. 16, 1974, p. 1.) If the Legislature was prepared to sweep that broadly, it must have intended that the statute protect publications like petitioners', which differ

[25] ODLIS, *supra*, at <http://lu.com/odlis/odlis_p.cfm#periodical> (as of May 23, 2006) ["Some periodicals are born digital and never issued in print (example: *Slate*)"].

from traditional periodicals only in their tendency, which flows directly from the advanced technology they employ, to continuously update their content.[26]

We conclude that petitioners are entitled to the protection of the shield law, which precludes punishing as contempt a refusal by them to disclose unpublished information.

V. Constitutional Privilege

A. Availability to Online Journalists

Petitioners also assert that the discovery sought by Apple is barred, on the present record, by a conditional privilege arising from the state and federal guarantees of a free press. The gist of the privilege is that a newsgatherer cannot to be compelled to divulge the identities of confidential sources without a showing of need sufficient to overbalance the inhibitory effect of such disclosure upon the free flow of ideas and information which is the core object of our guarantees of free speech and press. This argument raises two subsidiary questions: (1) Is such a privilege available to petitioners? (2) If so, has Apple made a sufficient showing to overcome it?

Because a constitutional privilege is implicated, we must subject the trial court's order to the relatively searching standards of " 'constitutional fact review.' " (*DVD Copy Control Association v. Bunner* (2003) 31 Cal.4th 864, 889 (*Bunner*), quoting *Rankin v. McPherson* (1987) 483 U.S. 378, 385, fn. 8.) " '[W]here a Federal right has been denied as the result of a [factual] finding . . . or where a conclusion of law as to a Federal right and a finding of fact are so intermingled as to make it necessary, in order to pass upon the

---

[26] The nearest analogue in traditional print media is probably the specialized looseleaf services familiar to lawyers and, we presume, other professions. We have no occasion to consider whether such publications should be deemed "periodical," but if they are not it is because they are books, which the Legislature pointedly *omitted* from the statute. The device of continuously updating with looseleaf inserts was devised not as a way not of publishing wholly new content in the manner of a magazine, but of keeping an existing *book* current by a means less costly than printing and binding a whole new volume.

Federal question, to analyze the facts,' the reviewing court must independently review these findings. [Citation.] '[F]acts that are germane to' the First Amendment analysis 'must be sorted out and reviewed de novo, independently of any previous determinations by the trier of fact.' [Citation.] And 'the reviewing court must " 'examine for [itself] the statements in issue and the circumstances under which they were made to see . . . whether they are of a character which the principles of the First Amendment . . . protect.' " ' [Citations.]" (*Bunner*, *supra*, 31 Cal.4th at pp. 889-890.) We must therefore " 'make an independent examination of the entire record' [citation], and determine whether the evidence in the record supports the factual findings necessary" to sustain the trial court's order denying a protective order. (*Id.* at p. 890.)[27]

The leading exposition of this privilege as applied in this state appears in *Mitchell*, *supra*, 37 Cal.3d 268, a libel action in which the defendant newsmagazine and its reporters sought to avoid compelled disclosure of confidential sources by asserting "a nonstatutory privilege based on the broad protections for freedom of the press enshrined in the United States Constitution and the correlative provision (art. I, § 2, subd. (a)) of the California Constitution." (*Id.* at p. 274.) The court held that "in a civil action a reporter, editor, or publisher has a qualified privilege to withhold disclosure of the identity of confidential sources and of unpublished information supplied by such sources. The scope of that privilege in each particular case will depend upon the consideration and weighing of a number of interrelated factors." (*Id.* at p. 279.)

Before turning to the relevant factors we must of course decide whether petitioners are reporters, editors, or publishers for purposes of this privilege. Our answer to this question is anticipated by the preceding discussion of the California reporter's shield.

---

[27] Although the court spoke in terms of the standard of review applicable to claimed infringements on the *federal* right to free speech, we have little doubt that the same standard applies to infringements of our state constitutional guarantee.

Whereas we there had to construe relatively specific statutory language, we are concerned here with broad constitutional principles. In that light, we can see no sustainable basis to distinguish petitioners from the reporters, editors, and publishers who provide news to the public through traditional print and broadcast media. It is established without contradiction that they gather, select, and prepare, for purposes of publication to a mass audience, information about current events of interest and concern to that audience.

Indeed, we do not understand Apple to contend that the constitutional privilege is inapplicable to petitioners. Its argument seems to assume that petitioners are within the zone of the privilege's protection and that the pivotal question is whether the weighing process discussed in *Mitchell* supports disclosure. Similarly, the brief of amici Intel Corporation and Business Software Alliance "assumes (without taking the position) that petitioners qualify in this instance as 'media' and 'reporters.' " Amicus Internet Technology Industry Council (ITIC) does not contest the point either, but contends that our weighing of the relevant factors should be colored by the unique dangers the internet poses to the preservation of trade secrets.[28] We agree with these implied concessions, and with petitioners' arguments, that petitioners are reporters, editors, or publishers entitled to the protections of the constitutional privilege.[29] If their activities and social

[28] ITIC notes that the internet has "contribute[d] to dramatic increases in business productivity. Accordingly, ITIC and its members strongly favor policies that protect the flow of free speech across the Internet." It then goes on to suggest that the supposedly unique hazard posed by the internet to trade secrets warrants special restrictions on the constitutional privilege in this context.

[29] Although the point is not argued, the record may leave some uncertainty as to the role and status of petitioner Bhatia. He is declared by "Kasper Jade" to be the "publisher" of another Macintosh-related Web site and the provider of hosting services, including "systems administration [and] bandwidth allocation," to Apple Insider. We assume, without deciding, that he is a "publisher" of Apple Insider for purposes of the privilege.

function differ at all from those of traditional print and broadcast journalists, the distinctions are minute, subtle, and constitutionally immaterial.

B. Application of Mitchell Factors

1. Nature of, and Role in, Litigation

We turn then to the balancing process outlined in *Mitchell*. The first factor identified there was "the nature of the litigation and whether the reporter is a party." (*Mitchell*, *supra*, 37 Cal.3d at p. 279.) Discovery is peculiarly appropriate when the reporter is a defendant in a libel action, because successful assertion of the privilege may shield the reporter himself from a liability he ought to bear. (*Ibid*.) This danger arises from the requirement, in many libel cases, that the plaintiff prove the reporter's publication of the challenged statements with knowledge of their falsity or reckless disregard for the truth. (*Id.* at pp. 279-280.) That burden may be impossible to carry if the statements can only be attributed to an unidentified source whose reliability cannot be evaluated. (*Ibid*.) Even in those cases, however, " 'disclosure should by no means be automatic.' " (*Id.* at p. 280, quoting *Zerilli v. Smith* (D.C.Cir. 1981) 656 F.2d 705, 714.)

Here this factor obviously favors nondisclosure. Of course this is not a libel action, but more fundamentally, petitioners are not defendants. If they were defendants, an analogy might be drawn between the requirement of a knowing and reckless falsehood in libel, and the various mental states that may be elements of a claim for violation of the trade secret laws. (See Civ. Code, § 3426.1, subd. (b).) But so long as petitioners are not parties, the validity of such a comparison is academic.

Apple argues that ". . . Petitioners may, in fact, be one or more of the Doe Defendants named in the complaint." This assertion is worse than speculative; it contradicts Apple's own allegations that the Doe defendants are persons unknown to Apple. Petitioner O'Grady, at least, is not unknown to Apple, and was not unknown when the complaint was filed. Moreover Apple has repeatedly accused petitioners, if somewhat obliquely, of misappropriating trade secrets. Thus Apple asserted below that

"illegal misappropriations occurred not only when [the trade secret] information was taken from Apple, but when it was disseminated by a person who had reason to know that it was a trade secret. The clear markings on the slides—'Apple Need-To-Know Confidential'—as well as the text of the postings themselves—describing the unreleased Asteroid product by its internal code name—establish that the dissemination was caused by a person who knew, or had reason to know, that the information was a trade secret." The concluding clause of that sentence echoes the provisions of the Uniform Trade Secrets Act defining "misappropriation" to include disclosure of a trade secret by one who, "[a]t the time of disclosure . . ., knew or had reason to know that his or her knowledge of the trade secret was: [¶] (i) Derived from or through a person who had utilized improper means to acquire it; [¶] (ii) Acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use; or [¶] (iii) Derived from or through a person who owed a duty to the person seeking relief to maintain its secrecy or limit its use . . . ." (Civ. Code, § 3426.1, subd. (b)(2)(B).)

Apple quotes this statutory language in its opposition to the petition, but then asserts only that the persons liable for misappropriation of the Asteroid trade secrets "*potentially* include[e] Petitioners." (Italics added.) Apple cannot have it both ways. If it is unprepared to charge petitioners with liability for trade secret misappropriation, it cannot count in its favor their status vis à vis the litigation, however culpable it may claim them to be.

We reach this conclusion not by merely taking the comments in *Mitchell* at face value, but by considering several factors bearing on the wisdom of Apple's proposed departure from those comments. First, the plaintiff in litigation has complete control over whom to join as defendants and when to do so. If the plaintiff elects not to join a journalist as a defendant, it will hardly lie in the plaintiff's mouth to insist that the journalist should be viewed and treated as if he *had* been joined. A plaintiff cannot

decline to exercise the power to bring a person into the action, and then ask to be granted the fruits that would flow from an exercise of that power.

Further, the discovery process is intended as a device to facilitate adjudication, not as an end in itself. To accept Apple's position on the present point would empower betrayed employers to clothe themselves with the subpoena power merely by suing fictitious defendants, and then to use that power solely to identify treacherous employees for purposes of discipline, all without any intent of pursuing the underlying case to judgment. An employer pursuing such an objective might prefer not to join any defendants lest it expose itself to negative consequences up to and including a countersuit for malicious prosecution or abuse of process. Our sympathy for employers in such a position cannot blind us to the gross impropriety of using the courts and their powers of compulsory process as a tool and adjunct of an employer's personnel department.

Finally, viewing petitioners as if they were defendants when they have not in fact been joined would permit a plaintiff in Apple's position to subvert the usual prerogative of civil defendants to propound discovery first. (See Code Civ. Proc., § 2025.220; *California Shellfish Inc. v. United Shellfish Co.* (1997) 56 Cal.App.4th 16, 22, italics removed ["Every section of the Discovery Act . . . requires that at least one defendant ha[ve] been served with the summons and complaint, and . . . subject[s] [the plaintiff] to a holding period after service on a defendant, or requires that the party to whom the discovery is propounded ha[ve] been served with the summons and complaint"].) Plaintiffs could easily circumvent this prerogative if they were allowed to obtain documents and testimony from a prospective defendant while refusing, without explanation, to join that person as a party.

Since petitioners are not parties, the first factor weighs against disclosure.

2. Cruciality of Information

The second factor noted in *Mitchell* is "the relevance of the information sought to plaintiff's cause of action." (*Mitchell, supra*, 37 Cal.3d at p. 280.) The court adopted the

"majority view" that "mere relevance is insufficient to compel discovery; disclosure should be denied unless the information goes 'to the heart of the plaintiff's claim.' " (*Ibid*., citing *Garland v. Torre* (2d Cir. 1958) 259 F.2d 545, cert. den.)

Here this factor favors disclosure. It seems plain enough that when a plaintiff alleges a misappropriation of its trade secrets, the identity of the misappropriator goes to the heart of its claim. Such information is crucial to the plaintiff's cause of action. The force of this point is somewhat reduced, however, by the possibility that Apple might not identify the putative malefactor even if it obtains the discovery it seeks. Most obviously, the information may have provided to petitioners *anonymously*.[30] In other words, there is no assurance that the discovery sought by Apple will, in and of itself, permit Apple to name the original source of the posited leak. It may only supply further clues, pursuit of which may or may not enable Apple to learn what it seeks to know.

3. Exhaustion of Alternative Sources

The third *Mitchell* factor—the extent to which the party seeking disclosure of confidential sources has "exhausted all alternative sources of obtaining the needed information" (*Mitchell*, *supra*, 37 Cal.3d at p. 282)—weighs decisively against disclosure. "Compulsory disclosure of sources is the 'last resort' [citation], permissible only when the party seeking disclosure has no other practical means of obtaining the information." (*Ibid*., quoting *Senear v. Daily Journal-American, etc.* (1982) 97 Wash.2d 148, 641 P.2d 1180, 1184.) Discovery was denied in *Mitchell* because the plaintiffs there had failed to "reduce[] their discovery" to the "irreducible core of information which [could not] be discovered" except from the journalists. (*Mitchell*, *supra*, 37 Cal.3d at

[30] Although both O'Grady and Jade declared that they relied on confidential sources in preparing the Asteroid articles, neither indicated that he knew the actual identity of these sources. Jade declared that PowerPage relies heavily on "confidential and anonymous sources."

p. 282.) The same is true here: Apple has failed to establish that there is *any* information that it cannot obtain by means other than the present discovery.

So far as the record shows, Apple's attempt to identify the source of the posited leak consisted largely of questioning employees who were known to have had access to the Asteroid presentation file. Apple's investigators declared that they had identified, by our count, 29 employees known to have had knowledge of the file, including its creator, 25 employees to whom he distributed copies, one to whom a copy was forwarded, one who "accessed" the file on a secure server where another had placed it, and one with whom the matter was "verbally discussed." Each of these employees was interviewed, and each denied sharing the contents of the file, in whole or part, with anyone outside this group.

As petitioners point out, Apple made no attempt to question any of its employees under oath, even though it could readily have done so by obtaining permission to depose them instead of seeking to obtain unpublished information from petitioners. (See *Zerilli v. Smith, supra,* 656 F.2d 705, 714-715 [exhaustion not shown where plaintiffs had made no attempt to depose government employees most likely to lead to source of leaked wiretap transcripts]; *In re Petroleum Products Antitrust Litig.* (2d Cir. 1982) 680 F.2d 5, 8-9 [exhaustion not shown where pertinent questions not asked in hundreds of depositions already taken; citing authorities to the effect that 60 to 65 depositions might not be too many to require].)

Apple states that it did "everything possible" to trace the leak because "[t]he interviewed employees were all obligated to tell the truth to the investigators or risk losing their jobs." But people who are willing to take risks of one type may yet be very reluctant to lie under oath. Moreover an Apple employee who admitted disclosing trade secrets would presumably fear loss of his job anyway. Apple alleges in its complaint that "all Apple employees are required to agree to and sign a confidentiality agreement" prohibiting them from disclosing product plans "to anyone outside Apple at any time."

Although Apple avoids saying so, there can be little doubt that a violation of this agreement would constitute grounds for termination. This would seem to take the teeth out of any threat to terminate an employee who misleads an investigator about his role in the posited leak. Deception might save the employee's job, or at least delay the day or reckoning, while a confession might be expected to produce prompt if not immediate termination.

Questioning under oath exposes the person questioned to *criminal prosecution* for any willful falsehoods. (See Pen. Code, § 118.) That is no guarantee of truthful answers, but it certainly provides a stronger incentive to tell the truth than the mere risk of discharge—a risk which, as we have noted, was not obviated by truthful answers. An employee involved in a possibly criminal theft of trade secrets (see Pen. Code, § 499c) might invoke the privilege against self-incrimination rather than answer questions under oath, but even that would provide Apple with an extremely valuable investigative lead, to say the least.

Amicus Genentech asserts that an employer in Apple's situation should be excused from "conduct[ing] a needlessly disruptive and demoralizing internal investigation whenever it detects a theft of trade secrets." Such employers, continues Genentech, "should not be required to traumatize the workforce to protect their trade secrets." Of course no one is requiring Apple to traumatize its employees. It is entirely for Apple to decide what risks and costs to incur in pursuing the source of the leak. This choice is no different from one that may confront any employer who believes one or more unidentified employees have engaged in conduct harmful to its interests. Such an employer may have to decide how far to incommode innocent employees in order to identify guilty ones. Genentech would have us relieve the employer of this dilemma by shifting its burdens onto third party journalists. Such a shifting, however, would impair interests of constitutional magnitude. There is no countervailing constitutional interest in identifying faithless employees without inconveniencing their fellow workers.

Moreover, Apple has failed to establish that it adequately pursued other possible means to identify the source of the information in question. Beyond questioning its employees, as described above, one investigator declared that he had "requested a broad search of Apple's e-mail servers for communications regarding the Confidential Slides, the Confidential Drawing, or details regarding Aseteroid and/or Q97." He "reviewed the results of that search and found no evidence that the trade secret information had been transmitted outside Apple or to anyone other than the persons [the investigators] had interviewed." After one employee told investigators that he had "placed a copy of the Confidential Slides on a secure server," they conducted a review of "all available data regarding the identity of users who had accessed that file on the Secure Server," which led them to two additional Apple employees, who denied passing the information on.

Apple's account is conspicuously vague with respect to what evidence might have existed on its own facilities concerning further copying or dissemination of the presentation file. The ambiguities begin with the statement that the file was "distributed . . . electronically" to the initial 25 recipients. We are left to guess at what this means. Was the file emailed? Placed on an intranet server? Handed to the recipients on a CD-ROM or other portable medium? Each of these possibilities would present its own opportunities for, or obstacles to, further investigation.

Also conspicuously absent from this account is any indication of what network logs or similar resources might be available to show further transfers or other suspicious processing of the file by recipients. (See *Liebert Corp. v. Mazur* (2005) 827 N.E.2d 909, 918, 357 Ill.App.3d 265 [forensic examination of former employee's hard drive showed that he downloaded files, placed them in "zip" file, and probably burned copies to CD]; *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.* (S.D.Fla. 2003) 267 F.Supp.2d 1268, 1299-1300 [forensic expert testified that examination revealed, among other things, that licensee had used examined machine to penetrate licensor's intranet and transfer files]; *id.* at p. 1291 [monitoring of network connections led administrator to

conclusion "that someone else's hardware had been connected to the . . . network"]; *U. S. v. Hay* (9th Cir. 2000) 231 F.3d 630, 632 [examination of file transfer protocol (FTP) log showed direct exchanges of files between defendant's Washington computer and Canadian computer]; *U. S. v. Becht* (8th Cir. 2001) 267 F.3d 767, 769 [analysis of " 'transfer logs' " showed numerous files transferred to or from defendant's computer]; *LeJeune v. Coin Acceptors, Inc.* (2004) 381 Md. 288, 297, 314 [849 A.2d 451, 456, 466] [forensic expert contradicted defecting employee's claim that he inadvertently copied trade secrets to CD-ROM along with personal files; also showed that employee had erased information from laptop in effort to conceal downloads].)

True, Apple investigators referred to a vaguely described examination of its email servers. However, it would hardly be surprising if the culprit avoided that mode of transfer precisely because of the ease with which it could be traced. Apple failed to establish what other modes of transfer were or were not traceable and what efforts were made to investigate the traceable ones. For example, would server or workstation logs show that an employee had copied the file to a CD-ROM? Transferred it to a flash memory device? Printed a copy? Printed it to an image file and transferred that? Uploaded it to an off-site host using any of various file transfer protocols? Attached it to an email sent through a web-based mail server rather than through Apple's own servers? Transferred it directly to a laptop or other portable computer? Without answers to these questions it is impossible to say that Apple "exhausted" other means of identifying the source of the leak. Yet Apple's showing was entirely silent on these points even though petitioners asserted in the trial court that Apple had not "fully exploited internal computer forensics." Indeed, as we have noted, Apple did not even plainly describe in what form and by what means the file was originally distributed.

In oral argument Apple exposed another weakness in its showing when counsel suggested that the Asteroid information might have been acquired through "electronic espionage" by someone other than an employee. If this means that someone might have

"hacked" Apple's network from outside, then Apple was required under *Mitchell* to demonstrate that it had investigated that possibility to the extent practicable. This it failed entirely to do. (See *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, *supra*, 267 F.Supp.2d at p. 1301 [plaintiff's network included firewall/gateway, "a security device which is designed to prevent unauthorized access in a variety of dimensions, and to keep track of any attempts at unauthorized access when they occur"]; *ibid*. [attempts at unauthorized access were recorded "in a variety of different logs that are generated automatically"]; *id.* at p. 1302 [logs permitted generation of an "activity report, which would display all the traffic that was going through the . . . gateway/firewall"]; *id.* at p. 1306 [computer scientist confirmed that logs reflected "computer hacking"].)

The record shows at least one other avenue of investigation that Apple has apparently neglected to pursue. Petitioners point out that Apple has apparently done nothing to seek information from Paul Scates and Bob Borries, two publicly identified contributors to the drawings in the challenged articles. Apple responds by conjuring a false inconsistency between petitioners' reliance on this omission and their supposed assertion elsewhere that "any discovery regarding these two individuals is insufficiently related to Apple's trade secret claims." We can find no such assertion by petitioners. At the cited page of the petition, they object to Apple's attempt to obtain discovery *from petitioners* about these persons, on the ground that Apple has not shown that the drawings were based on the disclosure of trade secret information to the artists. This objection is entirely consistent with petitioners' argument here that Apple's failure to "directly contact[] or conduct[] discovery against Bob Borries and Paul Scates" constituted a failure to pursue potential alternative sources of information.

In sum, Apple has failed to demonstrate that it cannot identify the sources of the challenged information by means other than compelling petitioners to disclose

unpublished information. This fact weighs heavily against disclosure, and on this record is dispositive. We nonetheless comment upon the remaining two factors.

4. Importance of Preserving Confidentiality

The fourth consideration is "the importance of protecting confidentiality in the case at hand . . . ." (*Mitchell, supra*, 37 Cal.3d at p. 283.) "[W]hen the information relates to matters of great public importance, and when the risk of harm to the source is a substantial one, the court may refuse to require disclosure even though the plaintiff has no other way of obtaining essential information." (*Ibid*.)

Apple first contends that there is and can be no public interest in the disclosures here because "the public has no right to know a company's trade secrets." Surely this statement cannot stand as a categorical proposition. As recent history illustrates, business entities may adopt secret practices that threaten not only their own survival and the investments of their shareholders but the welfare of a whole industry, sector, or community. Labeling such matters "confidential" and "proprietary" cannot drain them of compelling public interest. Timely disclosure might avert the infliction of unmeasured harm on many thousands of individuals, following in the noblest traditions, and serving the highest functions, of a free and vigilant press. It therefore cannot be declared that publication of "trade secrets" is ipso facto outside the sphere of matters appropriately deemed of "great public importance."

Apple alludes repeatedly to the notion that the publication of trade secrets cannot be found to serve the public interest because of the policy embodied in trade secret law itself, which presupposes that trade secrets possess social utility justifying special protections against wrongful disclosure. This is, of course, a false dichotomy. It is true that trade secrets law reflects a judgment that providing legal protections for commercial secrets may provide a net public benefit. But the Legislature's general recognition of a property-like right in such information cannot blind courts to the more fundamental judgment, embodied in the state and federal guarantees of expressional freedom, that free

and open disclosure of ideas and information serves the public good. When two public interests collide, it is no answer to simply point to one and ignore the other. This case involves not a purely private theft of secrets for venal advantage, but a journalistic disclosure to, in the trial court's words, "an interested public." In such a setting, whatever is given to trade secrets law is taken away from the freedom of speech. In the abstract, at least, it seems plain that where both cannot be accommodated, it is the statutory quasi-property right that must give way, not the deeply rooted constitutional right to share and acquire information.

It might be suggested that the challenged reports do not come within the core of expressional liberty because they concern technical developments of interest only to a narrow readership, i.e., persons interested in the digital home recording of music. Such an implication pervades the brief of amicus Genentech Corp., which compares this matter to *Bunner, supra*, 31 Cal.4th 864, which held that an injunction could issue, on a proper showing, against the online publication of programming code that would permit computer users to circumvent the copy-protection system for commercially produced digital versatile disks. The court concluded that the plaintiffs' interest in preventing the disclosure of trade secrets overcame the publisher's expressional rights. In doing so, however, the court emphasized that the publication "convey[ed] only technical information about the method used by specific private entities to protect their intellectual property." (*Id.* at p. 883, italics in original.)

The publication here bears little resemblance to that in *Bunner*, which disclosed a sort of meta-secret, the whole purpose of which was to protect the plaintiff's members' products from unauthorized distribution. Here, no proprietary technology was exposed or compromised. There is no suggestion that anything in petitioners' articles could help anyone to build a product competing with Asteroid. Indeed there is no indication that Asteroid embodied any new technology that *could* be compromised. Apple's own slide stack, as disclosed in sealed declarations which we have examined, included a table

comparing Asteroid to existing, competing products; there is no suggestion that it embodies any particular technical innovation, except perhaps in the fact that it would integrate closely with Apple's own home recording software—a feature reflecting less a technical advance than a prerogative of one who markets both hardware and software. The newsworthiness of petitioners' articles thus resided not in any technical disclosures about the product but in the fact that Apple was planning to release such a product, thereby moving into the market for home recording hardware.

The case also differs from *Bunner* in that the alleged trade secret here was of greater public interest, and closer to the heart of First Amendment protection, than the information at issue there. The *Bunner* court declared computer code worthy of First Amendment protection, quoting with approval a statement that it was " 'a means of expressing ideas.' " (*Bunner*, *supra*, 31 Cal.4th at p. 877, quoting *Universal City Studios, Inc. v. Reimerdes* (S.D.N.Y. 2000) 111 F.Supp.2d 294, 327.) But a computer is fundamentally a set of switches mediating the interaction between input and output devices. Computer code is a set of instructions for turning those switches on and off in a prescribed pattern in order to carry out some desired set of functions. Such code bears more resemblance to a blueprint, recipe, or schematic diagram than to a news report. Like these other representations, it reflects and incidentally expresses the ideas of its author, and thus merits First Amendment protection. But its primary function, as with these other representations, is directory or *imperative*, not declarative. It is intended to *instruct* someone (or something), not in the sense of teaching, but in the sense of *ordaining* a practical objective, or a process for bringing such objective about.

Publishing a computer manufacturer's proprietary code may thus be compared to publishing a miller's secret recipe for a breakfast cereal. What occurred here was more like publicizing a secret *plan to release* a new cereal. Such a secret plan may possess the legal attributes of a trade secret; that is a question we are not here required to decide. But it is of a different order than a secret recipe for a product. And more to the point, the fact

of its impending release carries a legitimate interest to the public that a recipe is unlikely to possess.

Genentech thus goes astray when it attempts to compare this case to one in which an employee causes the publication of a technical secret such as a new design or process. The *Bunner* court declared the primary purposes of California trade secret law to be "to promote and reward innovation and technological development and maintain commercial ethics." (*Bunner*, *supra*, 31 Cal.4th at p. 878.) Whether or not confidential marketing plans constitute trade secrets under the governing statutory language, it cannot be seriously held that their protection has any direct and obvious tendency to serve the central purposes of the law.

More generally, we believe courts must be extremely wary about declaring what information is worthy of publication and what information is not. At first glance it might seem that Asteroid is nothing more than a hobbyist's gadget with no ponderable bearing on the great issues of the day. But such an impression would be, in our view, erroneous. With the release of this product, one of the world's leading manufacturers of personal computing products would be throwing its considerable muscle behind the development of sophisticated devices for creating high-quality audio recordings on a home computer. Such a development would inevitably contribute to blurring the line between professional and amateur audio production, and hence between professional and amateur composing and performing, in much the same way that the personal computer coupled with telecommunications technology has blurred the distinction between commercial and amateur publishing. The decentralization of expressive capacity represented by such developments is unquestionably one of the most significant cultural developments since the invention of the printing press.

While it may be tempting to think of Asteroid as a mere gizmo for nerds, such a device may also be the means by which the next Bob Dylan, Julia Ward Howe, or Chuck D conveys his or her message to the larger world. Music is of course a form of speech,

from the stirring hymns of Charles Wesley to the soaring meditations of John Coltrane. Who knows what latter day Woody Guthries may be lifted from obscurity by this new technology, in defiance of the considered judgment of recording executives that once might have condemned them to obscurity? Apple's commitment to such a product could prove to be an important step in democratizing the production and publication of music, as other digital technologies have democratized the publication of news and commentary.

These observations are intended not to demonstrate the innate newsworthiness of petitioners' articles but rather to illustrate the peril posed to First Amendment values when courts or other authorities assume the power to declare what technological disclosures are newsworthy and what are not. The digital revolution has been compared to the Industrial Revolution in terms of its potential impact on society and citizens. Apple is widely seen as a central figure in this cultural sea change. The online version of a leading business magazine has quoted a securities analyst's descriptions of Apple as " 'the nexus of [the] digital lifestyle revolution' " whose products "frequently incorporate disruptive changes in technology" and whose innovations "fundamentally alter the way we li[v]e."[31] The dry technical detail that pervaded petitioners' articles should not be permitted to obscure the fact that any movement by such a cultural leader into a whole new area of expression—as was promised by the Asteroid product—is newsworthy.

It is often impossible to predict with confidence which technological changes will affect individual and collective life dramatically, and which will come and go without lasting effects. Any of them may revolutionize society in ways we can only guess at. The lawful acquisition of information necessary to anticipate and respond to such changes is the birthright of every human, formally enshrined for Americans in our state

[31] Forbes.com <http://www.forbes.com/2006/01/26/apple-ipod-hdtv-0126markets09.html> (as of May 23, 2006).

and federal constitutions. The publications at issue here fully implicated that birthright and the interests protected by those constitutional guarantees.

5. Prima Facie Case

The fifth and final consideration noted in *Mitchell* was whether the plaintiff had made a prima facie case that the challenged statements were false. (*Mitchell*, *supra*, 37 Cal.3d at p. 283.) As extrapolated to actions not sounding in defamation, this factor translates into consideration of the demonstrated strength of the plaintiff's case on the merits. Again, however, the first factor—the journalist's relationship to the litigation—is implicated. In the libel case at issue in *Mitchell*, the prima facie case under scrutiny was the one alleged in the complaint *against the journalist* from whom disclosure was sought. Obviously the journalist's interest in withholding information should merit less protection if it appears likely that the journalist has indeed committed a tort against the plaintiff. Here, however, the plaintiff has not alleged that petitioners committed any tort; this fact alone tends to reduce the weight to be given this factor.

Still the factor should be given some weight if only because a strong showing of probable liability strengthens the plaintiff's interest in obtaining the information sought. More precisely, a *weak* showing of ultimate success tends to militate *against* disclosure because it increases the likelihood that any disclosure, and the accompanying violence to expressional interests, will prove to have been needless.

Here it can be reasonably inferred from the circumstances shown by Apple that someone violated a duty not to disclose the information in question, and that the information constituted a trade secret. Apple has thus presented enough evidence to support a reasoned inference of wrongdoing on someone's part. Therefore this factor favors disclosure, or more precisely, does not weigh against it. On balance however, neither this factor nor the other factors favoring disclosure possess sufficient weight on this record to overbalance the countervailing factors, particularly the inadequacy of Apple's showing that it exhausted alternative avenues of investigation.

DISPOSITION

Let a writ of mandate issue directing the court below to set aside its order denying petitioners' motion for a protective order and to enter a new order granting that motion.

_____
RUSHING, P.J.

WE CONCUR:

_____
PREMO, J.

_____
ELIA, J.

O'Grady et al. v. Superior Court (Apple)
H028579

Trial Court:	Santa Clara County Superior Court Court No.: CV032178
Trial Judge:	The Honorable James Kleinberg
Attorneys for Petitioner Jason O'Grady et al.:	Law Offices of Richard R. Wiebe Richard R. Wiebe Berman DeValerio Tomlinson Zisko Thomas E. Moore, III Electronic Frontier Foundation Kurt B. Opsahl Kevin S. Bankston
Attorneys for Real Party in Interest Apple Computer Inc.:	O'Melveny & Myers George A. Riley David R. Eberhart Dhaivat H. Shah James A. Bowman Ian N. Ramage
Attorneys for Amicus Curiae for Petitioner California Newspaper Publishers Assoc.:	Thomas W. Newton James W. Ewert
Attorneys for Amicus Curiae for Petitioner Reporters Committee for Freedom of the Press:	Lucy D. Dalglish Gregg P. Leslie Grant D. Penord
Attorneys for Amicus Curiae for Petitioner Center for Internet & Society:	Center for Internet & Society Lauren Gelman

Attorneys for Amicus Curiae for Petitioner Bear Flag League:	Paumilia & Adamec Justene Adamec WLF The Williams Law Firm J. Craig Williams Enterprise Counsel Group Jeffrey Lewis Benjamin P. Pugh
Attorney for Amicus Curiae for Petitioner United States Internet Society et al.:	Akin Gump Strauss Hart & Feld Elizabeth H. Rader
Attorney for Amicus Curiae for Real Party in Interest Genetech, Inc.:	Keker & Van Nest Michael D. Celio Steven A. Hirsch Clement S. Roberts
Attorney for Amiucs Curiae for Real Party in Interest ACLU:	Ann Brick
Attorneys for Amicus Curiae for Real Party in Interest Intel Corp., et al.:	Perkins Coie Brown & Bain Dan L. Bagatell Joel W. Nomkin Covington & Burling Sonja D. Winner
Attorneys for Amicus Curiae for Real Party in Interest Information Technology Industry Council:	Quinn Emanuel Urquhart, etc. Robert W. Stone Kathleen M. Sullivan

O'Grady et al. v. Superior Court (Apple)
H028579