read, it is *he* who posts it. It would be no more accurate to say *I* "posted" that information than it would be 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 **92 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 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.

*1451 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

[9] 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.)

[10] 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, 188 Cal.Rptr. 104, 655 P.2d 306.) " '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 **93 decision to be made.' " (*Id.* at p. 171, 188 Cal.Rptr. 104, 655 P.2d 306, quoting *California Water & Telephone Co. v. County of Los Angeles* (1967) 253 Cal.App.2d 16, 22, 61 Cal.Rptr. 618.)

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 *1452 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 ****94** 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 ***1453** 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. VB.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 ***1454** notices], 2030.010 [interrogatories], 2031.020 [inspection of documents], 2033.020 [requests for admissions].)[17] As a result, there is ****95** 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 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 ***1455** 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, p. *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 ****96** 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.

***1456** We conclude that Apple's discovery rights against petitioners are ripe for adjudication.

IV. *California Reporter's Shield*

A. Introduction

[11] 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]

****97 [12]** 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, 9 Cal.Rptr.3d 791.) 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, 27 Cal.Rptr.3d 596.) 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 ***1457** *Rancho Publications, supra,* 68 Cal.App.4th at p. 1546, 81 Cal.Rptr.2d 274, quoting *Delaney v. Superior Court* (1990) 50 Cal.3d 785, 806, fn. 20, 268 Cal.Rptr. 753, 789 P.2d 934(*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, 81 Cal.Rptr.2d 274.) 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 **98 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.

*1458 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, 81 Cal.Rptr.2d 274, 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, 81 Cal.Rptr.2d 274), 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, 81 Cal.Rptr.2d 274). 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, 81 Cal.Rptr.2d 274.) 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.

**99 *1459 *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, 268 Cal.Rptr. 753, 789 P.2d 934.) 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 ***1460** 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

[13] We come now to the difficult issue, which is whether the phrase "newspaper, ****100** 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.)

[14] ***1461** 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, 49 Cal.Rptr.2d 354, quoting *People v. Fair* (1967) 254 Cal.App.2d 890, 893, 62 Cal.Rptr. 632, italics added; see *People v. Williams* (2001) 26 Cal.4th 779, 785, 111

Cal.Rptr.2d 114, 29 P.3d 197.) 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, 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 ****101** (newspapers and magazines). The question is how to delineate the class of *unspecified* things thus included within the sweep of the law.

[15] 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, 158 Cal.Rptr. 370, 599 P.2d 676;*Scally v. Pacific Gas & Electric Co.* (1972) 23 Cal.App.3d 806, 819, 100 Cal.Rptr. 501.) 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 ***1462** 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. ****102** 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.

***1463** 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.) hearing 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, 126 Cal.Rptr.2d 897, 57 P.3d 363 ["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 ***1464** narrowest sense ****103** the term "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 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 dictionary defines "periodical" as ****104** "[r]ecurring after *more or less* regular periods of time...." (11 Oxford English Dict., *supra,* p. 560, italics added.)

***1465** 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 "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, 10 Cal.Rptr.2d 344 [purpose of statute limiting ***1466** 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 ****105** 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.) hearing 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 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

[16] 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?

[17] 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, 4 Cal.Rptr.3d 69, 75 P.3d 1(*Bunner*), quoting ***1467** *Rankin v. McPherson* (1987) 483 U.S. 378, 385, fn. 8, 107 S.Ct. 2891, 97 L.Ed.2d 315.) " '[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 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, 4 Cal.Rptr.3d 69, 75 P.3d 1.) 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, 4 Cal.Rptr.3d 69, 75 P.3d 1.) [27]

[18] The leading exposition of this privilege as applied in this state appears in ****106** *Mitchell, supra,* 37 Cal.3d 268, 208 Cal.Rptr. 152, 690 P.2d 625, a libel action in which the defendant news magazine 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, 208 Cal.Rptr. 152, 690 P.2d 625.) 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, 208 Cal.Rptr. 152, 690 P.2d 625.)

[19] 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. 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.

*1468 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 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

[20] We turn then to the balancing process outlined in *Mitchell.* The first **107 factor identified there was "the nature of the litigation and whether the reporter is a party." (*Mitchell, supra,* 37 Cal.3d at p. 279, 208 Cal.Rptr. 152, 690 P.2d 625.) 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, 208 Cal.Rptr. 152, 690 P.2d 625.) 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, 208 Cal.Rptr. 152, 690 P.2d 625, quoting *Zerilli v. Smith* (D.C.Cir.1981) 656 F.2d 705, 714.)

*1469 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 **108 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 ***1470** 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, 64 Cal.Rptr.2d 797 ["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 (italics omitted)"].) 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, 208 Cal.Rptr. 152, 690 P.2d 625.) 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 ***1471** 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 been provided to petitioners *anonymously.* [30] In other words, there is no assurance that the discovery sought by ****109** 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

[21] 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, 208 Cal.Rptr. 152, 690 P.2d 625)—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 p. 282, 208 Cal.Rptr. 152, 690 P.2d 625.) 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 ***1472** 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 ****110** 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. ***1473** 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) 357 Ill.App.3d 265, 293 Ill.Dec. 28, 827 N.E.2d 909, 918 [forensic examination of **111 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 *1474 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, supra,* 37 Cal.3d 268, 208 Cal.Rptr. 152, 690 P.2d 625 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 **112 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 *1475 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.

[22] 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, 208 Cal.Rptr. 152, 690 P.2d 625.) "[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 ***1476** 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." ****113** 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 Inc., which compares this matter to *Bunner, supra,* 31 Cal.4th 864, 4 Cal.Rptr.3d 69, 75 P.3d 1, 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, 4 Cal.Rptr.3d 69, 75 P.3d 1, italics omitted.)

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.

***1477** 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, 4 Cal.Rptr.3d 69, 75 P.3d 1, 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 ****114** 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, 4 Cal.Rptr.3d 69, 75 P.3d 1.) 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, ***1478** 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 ****115** 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.

***1479** 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 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, 208 Cal.Rptr. 152, 690 P.2d 625.) 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.

***1480 DISPOSITION**

Let a writ of mandate issue directing the court below to set aside its order denying ****116** petitioners' motion for a protective order and to enter a new order granting that motion. Costs to petitioners.

WE CONCUR: PREMO and ELIA, JJ.

All Citations

139 Cal.App.4th 1423, 44 Cal.Rptr.3d 72, 79 U.S.P.Q.2d 1398, 34 Media L. Rep. 2089, 06 Cal. Daily Op. Serv. 4509, 2006 Daily Journal D.A.R. 6618

Footnotes

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.

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).

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).)

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.

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.

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.

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.)

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.

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.

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.

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.

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

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.

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, 186 Cal.Rptr. 211;*Rancho Publications, supra,* 68 Cal.App.4th at p. 1543, 81 Cal.Rptr.2d 274;*Mitchell v. Superior Court* (1984) 37 Cal.3d 268, 274, 208 Cal.Rptr. 152, 690 P.2d 625.) Apple offers this point, however, only with respect to the subpoenas already served on Nfox and Kraft, not those threatened against petitioners.

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).

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 authority defining "periodical publication" to mean a publication appearing at regular intervals. (*Houghton v. Payne* (1904) 194 U.S. 88, 96–97, 24 S.Ct. 590, 48 L.Ed. 888 [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"]; *Fifield 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 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' web sites 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.

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,* 193 Wis.2d 429, 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."

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*)"].

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.

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.

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.

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."

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

End of Document

KeyCite Yellow Flag - Negative Treatment
Distinguished by Elcometer, Inc. v. TQC-USA, Inc., E.D.Mich., September 23, 2013

252 F.R.D. 346
United States District Court,
E.D. Michigan,
Southern Division.

Ernest FLAGG, as Next Friend
of Jonathan Bond, Plaintiff,
v.
CITY OF DETROIT, et al., Defendants.

No. 05–74253. | Aug. 22, 2008.

Synopsis

Background: In **civil** action, defendant city and one individual defendant moved to prevent **discovery** of **communications** exchanged among certain officials and employees of the city via city-issued text messaging devices retained by non-party service provider.

[Holding:] The District Court, Gerald E. Rosen, J., held that **Stored Communications Act** (SCA) did not preclude **civil discovery** of city's relevant, nonprivileged electronically **stored communications** that were maintained by a non–party service provider but remained within the city's control.

Motion granted in part and denied in part.

West Headnotes (6)

[1] **Federal Civil Procedure**
Proceedings to obtain

Regardless of whether defendants' motions could be construed as requests for reconsideration of order requiring that **discovery** process go forward, the motions, which were filed more than a month after the court issued opinion and related order, would not be considered forfeited since the motions were expressly contemplated and permitted by the court.

Cases that cite this headnote

[2] **Federal Civil Procedure**
Existence, possession, custody, control and location

Federal Civil Procedure
Particular Subject Matters

Discovery of text messages retained by non-party service provider but remaining within the party's control may be achieved by a request for the production of documents. Fed.Rules Civ.Proc.Rule 34(a)(1), 28 U.S.C.A.

7 Cases that cite this headnote

[3] **Federal Civil Procedure**
Existence, possession, custody, control and location

For purposes of **discovery** rule governing production of documents, city had "control" over text messages preserved by third party service provider pursuant to its contractual relationship with the city; since city could "block" the disclosure of the text messages by withholding its consent, it could permit the disclosure of those **communications** by granting its consent. Fed.Rules Civ.Proc.Rule 34(a)(1), 28 U.S.C.A.

7 Cases that cite this headnote

[4] **Records**
Matters Subject to Disclosure; Exemptions

City's text messages satisfied the definition of "public records" under Michigan's Freedom of Information **Act** (FOIA) insofar as they captured **communications** among city officials or employees in the performance of an official function; thus, for purposes of **discovery** rule governing production of documents, city had "control" over any such "public records" that might be retained by third party service provider under its contract with the city. M.C.L.A. § 15.232(e).

3 Cases that cite this headnote

[5] **Telecommunications**

Computer communications

Stored Communications Act (SCA) did not preclude civil discovery of party's relevant, nonprivileged electronically stored communications that were maintained by a non–party service provider but remained within the party's control; any archive of text messages that service provider maintained on party's behalf constituted the only available record of those communications, and could not possibly serve as a "backup" copy of communications stored elsewhere, and the archive maintained by service provider constituted "computer storage," and provider's maintenance of that archive on behalf of the party was a "remote computing service" as defined under the SCA. 18 U.S.C.A. § 2701 et seq.; Fed.Rules Civ.Proc.Rule 34(a)(1), 28 U.S.C.A.

13 Cases that cite this headnote

[6] Federal Civil Procedure

Grounds and Objections

City employees, who were advised under city's electronic communications policy directive that they should assume that any electronic communication created, received, transmitted, or stored on the city's electronic communication system was public information, and may be read by anyone, impliedly consented to service provider's production of their text messages to city for the limited purpose of enabling the city to fulfill its discovery obligations. Fed.Rules Civ.Proc.Rule 34, 28 U.S.C.A.

8 Cases that cite this headnote

Attorneys and Law Firms

*347 Robert S. Zawideh, Norman N. Yatooma, Ryan D. Bobel, Norman Yatooma Assoc., Howard Y. Lederman, Birmingham, MI, for Plaintiff.

John A. Schapka, Krystal A. Crittendon, Detroit City Law Department, Kenneth L. Lewis, Randal M. Brown, James C. Thomas, Plunkett Cooney, Detroit, MI, Jeffrey B. Morganroth, Morganroth & Morganroth, Southfield, MI, for Defendants.

OPINION AND ORDER REGARDING DEFENDANTS' MOTIONS TO PRECLUDE DISCOVERY OF ELECTRONIC COMMUNICATIONS

GERALD E. ROSEN, District Judge.

I. *INTRODUCTION*

In an opinion and related order issued on March 20, 2008, the Court (i) determined that the communications exchanged among certain officials and employees of the Defendant City of Detroit via city-issued text messaging devices were potentially discoverable under the standards of Fed.R.Civ.P. 26(b)(1), (*see* 3/20/2008 Op. at 10–11), and (ii) established a protocol under which two designated Magistrate Judges would review these communications and make the initial determination as to which of them are discoverable, (*see* 3/20/2008 Order at 3–8). Through the present motions, the Defendant City and one of the individual Defendants, Christine Beatty, seek to prevent this discovery effort from going forward, arguing that the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*,[1] wholly precludes the production in civil litigation of electronic communications stored by a non-party service provider.[2]

As discussed below, the Court rejects this proposed reading of the SCA as establishing a sweeping prohibition against civil discovery of electronic communications. Defendants' position, if accepted, would dramatically alter discovery practice, in a manner clearly not contemplated by the existing rules or law, by permitting a party to defeat the production of electronically stored information created by that party and still within its control—information that plainly is subject to civil discovery, *see* Fed.R.Civ.P. 34(a)(1)—through the simple expedient of storing it with a third party. Because nothing in the plain language of the SCA requires this extraordinary result, and because Defendants have not identified any other support for this proposition, the Court holds that the discovery effort contemplated in its March 20, 2008 opinion and related order may go forward, albeit through a means somewhat different from that employed by Plaintiff to date.

II. *BACKGROUND*

During the time period of relevance to this case, the Defendant City of Detroit entered into a contract for text messaging services with non-party service provider SkyTel, Inc.[3] Under this contract, SkyTel provided text messaging devices and corresponding services to various City officials and employees, including at least some of the individual Defendants in this case. Although the City discontinued its contract with SkyTel in 2004, the company evidently continues to maintain copies of at least some of the text messages sent and received by City officials during the ***348** period when SkyTel provided this service to the City.[4]

Upon learning of SkyTel's apparent retention of such **communications**, Plaintiff issued two broad subpoenas to SkyTel in February of 2008, seeking the disclosure of (i) all text messages sent or received by 34 named individuals, including the individual Defendants, during a number of time periods spanning over 5 years, and (ii) all text messages sent or received by any City official or employee during a four-hour time period in the early morning hours of April 30, 2003, the date that Plaintiff's mother was killed. Defendants promptly moved to quash these subpoenas, arguing (among other things) that none of these **communications**, regardless of their content, satisfied the standard for **discovery** as set forth in Fed.R.Civ.P. 26(b)(1). In an opinion and related order issued on March 20, 2008, the Court rejected this contention —along with Plaintiff's contrary and equally sweeping assertion that all such **communications** were **discoverable**, without regard to their subject matter—and established a protocol under which two designated Magistrate Judges would conduct an initial review of certain subsets of the **communications** retained by SkyTel and determine, subject to Defendants' objections and this Court's review, which of these **communications** should be produced to Plaintiff.

As this court-ordered process was getting under way, the Defendant City and one of the individual Defendants, Christine Beatty, filed the present motions, arguing that the federal **Stored Communications Act** ("SCA"), 18 U.S.C. § 2701 *et seq.*, prevents Plaintiff from obtaining in **civil discovery** any text messages that remain in SkyTel's possession as a result of its role as the City's service provider. Apart from these motions, SkyTel has moved to quash Plaintiff's subpoenas or, alternatively, for entry of an order that would protect the company against liability under the SCA for its production of text messages in accordance with the protocol established in this Court's March 20, 2008 order. Finally, by motion filed on July 23, 2008, the Detroit Free Press seeks leave to file an *amicus* brief in opposition to the motion brought by Defendant Beatty, arguing that the Court's resolution of this motion is likely to have a bearing on a state-court suit in which the newspaper seeks the production of certain text messages from SkyTel pursuant to the Michigan Freedom of Information **Act**.

III. *ANALYSIS*

A. Defendants Have Not Forfeited Their Opportunity to Challenge Plaintiff's Discovery Effort as Precluded by the SCA.

[1] Before turning to the merits of Defendants' SCA-based challenge, the Court first addresses Plaintiff's contention that Defendants' motions should be denied as untimely requests for reconsideration of the Court's March 20, 2008 rulings. As Plaintiff points out, under Local Rule 7.1(g)(1) of this District, such a request for rehearing or reconsideration must be filed within ten days after entry of the ruling at issue, but Defendants brought their present motions more than a month after the Court issued its March 20, 2008 opinion and related order. It follows, in Plaintiff's view, that Defendants' SCA-based challenge is untimely.

Yet, regardless of whether Defendants' motions could be construed as requests for reconsideration, the Court agrees with Defendant Beatty's contention in her reply brief that Defendants filed these motions in accordance with the Court's express authorization. So far as the Court's review of the record has revealed, Defendants first alluded to the possible impact of the SCA in a March 17, 2008 ***349** reply brief in support of Defendants' initial round of motions to quash Plaintiff's SkyTel subpoenas. As the Court observed at a subsequent April 14, 2008 hearing, however, Defendants' passing reference to the SCA was far too "elliptical" to elicit a ruling on the merits of this issue. (*See* 4/14/2008 Hearing Tr. at 22.) Nonetheless, the Court invited defense counsel to properly and squarely raise this challenge through a separate motion. (*See id.* at 22, 34.) Accordingly, because Defendants' present motions were expressly contemplated and permitted by the Court, Plaintiff's claim of forfeiture is not well-taken.

B. The SCA Does Not Preclude Civil Discovery of a Party's Electronically Stored Communications That

Are Maintained by a Non–Party Service Provider But Remain Within the Party's Control.

Turning to the merits, Defendants' motions rest upon a simple yet sweeping proposition: namely, that the SCA "absolutely precludes the production of electronic **communications** in **civil** litigation." (Defendant Beatty's Motion at ¶ 3; *see also* Defendant City of Detroit's Motion at ¶ 5.)[5] In order to properly address this assertion, the Court finds it instructive to first (i) survey the SCA provisions that Defendants contend are pertinent here, (ii) describe the subset of **communications** that the Court envisioned as subject to production in its March 20, 2008 opinion and order, and (iii) review the terms and scope of the Federal Rules that ordinarily govern the **discovery** of a party's electronically **stored** information. Against this backdrop, the Court finds that Defendants' motions are rather easily resolved, without the need for an overly detailed or exhaustive construction of the terms of the SCA.

1. The Potentially Relevant Provisions of the SCA

As pertinent here, the SCA generally prohibits—subject to certain exceptions—a "person or entity providing an electronic **communication** service to the public" from "knowingly divulg[ing] to any person or entity the contents of a **communication** while in electronic storage by that service." 18 U.S.C. § 2702(a)(1). It further prohibits—again, subject to certain exceptions—a "person or entity providing remote computing service to the public" from "knowingly divulg[ing] 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).[6]

As is evident from these provisions, the prohibitions set forth in § 2702(a) govern service providers to the extent that they offer either of two types of services: an "electronic **communications** service" or a "remote computing service." An "electronic **communications** service" ("ECS") is defined as "any service which provides to users thereof the ability to send or receive wire or electronic **communications**." 18 U.S.C. § 2510(15).[7] A "remote computing service" ("RCS"), in contrast, is defined as "the provision to the public of computer storage or processing services by means of an electronic **communications** system." 18 U.S.C. § 2711(2).[8]

The potential importance of distinguishing between an "ECS" and an "RCS" lies in the different criteria for establishing an exception to the general rule against disclosure. ***350** The provider of an RCS may divulge the contents of a **communication** with the "lawful consent" of the subscriber to the service, while the provider of an ECS may divulge such a **communication** only with the "lawful consent of the originator or an addressee or intended recipient of such **communication**." 18 U.S.C. § 2702(b)(3). Apart from this exception for disclosures made with the appropriate consent, the SCA authorizes the provider of either an ECS or an RCS to divulge the contents of a **communication** under several other specified circumstances—e.g., disclosure is permitted "to a person employed or authorized or whose facilities are used to forward such **communication** to its destination," 18 U.S.C. § 2702(b)(4), or "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," 18 U.S.C. § 2702(b)(5).

Yet, as noted by the courts and commentators alike, § 2702 lacks any language that explicitly authorizes a service provider to divulge the contents of a **communication** pursuant to a subpoena or court order. *See, e.g., In re Subpoena Duces Tecum to AOL, LLC,* 550 F.Supp.2d 606, 611 (E.D.Va.2008) (observing that "the statutory language of the [SCA] does not include an exception for the disclosure of electronic **communications** pursuant to **civil discovery** subpoenas"); *see also* U.S. Internet Service Provider Ass'n, *Electronic Evidence Compliance—A Guide for Internet Service Providers,* 18 Berkeley Tech. L.J. 945, 965 (2003) (noting that none of the exceptions set forth in § 2702(b) "expressly permits disclosure pursuant to a **civil discovery** order" obtained by a private party).[9] Seizing upon this absence of express statutory authorization, Defendants contend in their present motions that neither Plaintiff (through a subpoena) nor this Court (through an order) may compel SkyTel to produce the contents of any **communications** it might still retain under its contract to provide text messaging services to the City of Detroit.[10]

2. The Communications That Are Potentially Subject to Production Under the Rulings and Corresponding Protocol Set Forth in the Court's March 20, 2008 Opinion and Related Order

Before returning to the terms of the SCA and their potential impact here, the Court first revisits its rulings in the March 20, 2008 opinion and related order. As discussed earlier, the subpoenas that were addressed in the March 20 opinion sought the production of the contents of (i) all messages that originated from or were received by the SkyTel text messaging devices issued to any of 34 named individuals—most (but not all) of whom were City of Detroit officials

and employees [11] —during several specified time periods spanning over five years, and (ii) all messages sent or received by any City of Detroit official or employee during the hours surrounding the death of Plaintiff's mother, Tamara Greene.

In its March 20 opinion, the Court rejected the extreme positions of Plaintiff and Defendants alike as to the **discoverability** of these **communications**—i.e., Plaintiff's contention that ***all*** of the text messages meeting these broad criteria were subject to production, ***351** without regard to their contents, and Defendants' equally sweeping assertion that ***none*** of these **communications** were relevant to Plaintiff's claims in this case, also without regard to their subject matter. Instead, the Court looked to the standards of Fed.R.Civ.P. 26(b)(1), concluding that Plaintiff was entitled to obtain copies of those **communications** which addressed "any nonprivileged matter that is relevant to any party's claim or defense." The Court then established, through its separate March 20 order, a protocol by which two designated Magistrate Judges would review successive subsets of text messages retained by SkyTel under its contract with the Defendant City and determine—subject to Defendants' objections and assertions of privilege and this Court's final review—which of them met the Rule 26(b)(1) criteria for **discoverability**.

As a result of these rulings, the universe of text messages that will ultimately be produced to Plaintiff is narrowly confined to those that are found to be "relevant" and "nonprivileged" under Rule 26(b)(1). Moreover, and as the Rule itself makes clear, the requisite determination of relevance will be made by reference to the parties' claims and defenses. In this case, then, the Rule 26(b)(1) inquiry will turn upon the relevance of any particular text message to the theory of recovery advanced in Plaintiff's complaint—namely, that Defendants violated his constitutional right of access to the courts by deliberately delaying and obstructing the investigation into his mother's murder, and by ignoring and actively concealing material evidence bearing upon this investigation.

When Plaintiff's **discovery** effort is viewed in this light, the appeals of Defendant Beatty—as well as Defendant Kilpatrick, in his submissions stating his concurrence in his co-Defendants' motions—to notions of "privacy" appear wholly inapposite. As explained, a text message is **discoverable** in this case only if it is relevant to Plaintiff's allegations of deliberate delay, obstruction, and disregard or concealment of evidence in the investigation of his mother's murder. Surely, any text messages exchanged among City of Detroit officials or employees concerning the topic of the Tamara Greene murder investigation are properly characterized as governmental, and not private or personal, **communications**. [12] Thus, to the extent that Defendants rely on case law—principally, the Ninth Circuit's recent decision in *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 903–09 (9th Cir.2008)—that addresses a government employee's reasonable expectation of privacy in his or her personal **communications** using employer-provided equipment, such rulings provide no guidance here. [13]

For similar reasons, the Defendant City's attempts in its motion to interpose claims of privilege are, at best, premature, and have no bearing on the present SCA-based challenge. Contrary to the City's contention, it simply is not possible to meaningfully address such assertions of privilege generically, without first reviewing the text messages sent and received by the pertinent City officials and employees and identifying those which contain relevant subject matter. Consider, for example, a hypothetical text message in ***352** which two City officials are discussing the possibility of concealing evidence that is material to the Tamara Greene murder investigation. The City could not possibly assert a legitimate claim of privilege as to such a **communication**—and, in any event, any such claim would surely be overcome by Plaintiff's need for this information. *See, e.g., Frankenhauser v. Rizzo*, 59 F.R.D. 339, 344 (E.D.Pa.1973) (citing as two factors in a privilege inquiry (i) "whether the information sought is available through other **discovery** or from other sources," and (ii) "the importance of the information sought to the plaintiff's case"). As this example illustrates, the City's appeal to various possible privileges, like Defendant Beatty's appeal to notions of privacy, does not obviate the need for an initial review of the available **communications** of the pertinent City officials and employees to identify those which are relevant to Plaintiff's claims in this case. Only then can any meaningful determination of privilege be made.

To be sure, some of the text messages reviewed by the Magistrate Judges in this process might include personal or private information, and some might be the subject of legitimate claims of privilege. Yet, this was the very purpose of the protocol established in the Court's March 20, 2008 order—to review these **communications** *in camera,* and then to afford Defendants an opportunity to raise objections, as a means of protecting against disclosure to Plaintiff of irrelevant, privileged, or otherwise non-**discoverable** materials. In agreeing to this protocol, Defendants presumably recognized that it was meant to

safeguard their interests in preventing such disclosures, and they have not suggested how it might be inadequate to achieve this objective. [14]

Under these circumstances, Defendants' appeals to notions of privacy and privilege are simply beside the point. What they necessarily must show is far broader—namely, that the SCA prohibits either (i) the submission of SkyTel text messages to the Court for an *in camera* review, or (ii) the production to Plaintiff of the subset of these **communications** that are determined by the Court to be **discoverable** under the standards of Rule 26(b)(1). If the SCA dictates such a result, it must do so despite the absence in this case of any real threat that personal or privileged **communications** might be disclosed to Plaintiff. This bears emphasis as the Court resolves Defendants' motions.

3. The Federal Rules Governing the Discovery of a Party's Electronically Stored Information

One final subject warrants consideration before addressing the merits of Defendants' SCA-based challenge. Although Plaintiff chose third-party subpoenas as the vehicle for seeking the production of SkyTel text messages, the Court finds it instructive to consider whether Plaintiff could have achieved the same objective through an ordinary Fed.R.Civ.P. 34 request for production directed at the Defendant City. As discussed below, the Court answers this question in the affirmative.

[2] Under Rule 34(a), a party may request the production of documents and various other categories of items that are "in the responding party's possession, custody, or control." Fed.R.Civ.P. 34(a)(1). The items that may be sought under the Rule include "electronically **stored** information," Fed.R.Civ.P. 34(a)(1), which plainly encompasses both electronic **communications** and archived copies of such **communications** that are preserved in electronic form, *see* Fed.R.Civ.P. 34, Advisory Committee Note to 2006 Amendments; *Zubulake v. UBS Warburg LLC,* 217 F.R.D. 309, 317 nn. 36–38 (S.D.N.Y.2003). [15] Thus, the archived text ***353** messages under consideration here fit comfortably within the scope of the materials that a party may request under Rule 34.

As the language of the Rule makes clear, and as the courts have confirmed, a request for production need not be confined to documents or other items in a party's possession, but instead may properly extend to items that are in that party's "control." Fed.R.Civ.P. 34(a)(1); *see also Cooper Industries, Inc. v. British Aerospace, Inc.,* 102 F.R.D. 918, 919 (S.D.N.Y.1984) ("Documents need not be in the possession of a party to be **discoverable**, they need only be in its custody or control."). The Sixth Circuit and other courts have held that documents are deemed to be within the "control" of a party if it "has the legal right to obtain the documents on demand." *In re Bankers Trust Co.,* 61 F.3d 465, 469 (6th Cir.1995); *see also Mercy Catholic Medical Center v. Thompson,* 380 F.3d 142, 160 (3d Cir.2004); *Searock v. Stripling,* 736 F.2d 650, 653 (11th Cir.1984). [16] In light of the Rule's language, "[a] party responding to a Rule 34 production request cannot furnish only that information within his immediate knowledge or possession; he is under an affirmative duty to seek that information reasonably available to him from his employees, agents, or others subject to his control." *Gray v. Faulkner,* 148 F.R.D. 220, 223 (N.D.Ind.1992) (internal quotation marks and citation omitted).

The case law illustrates the variety of circumstances under which a party may be deemed to have "control" over materials not in its possession. First, the requisite "legal right to obtain" documents has been found in contractual provisions that confer a right of access to the requested materials. *See, e.g., Anderson v. Cryovac, Inc.,* 862 F.2d 910, 928–29 (1st Cir.1988); *Golden Trade, S.r.L. v. Lee Apparel Co.,* 143 F.R.D. 514, 525 (S.D.N.Y.1992). The courts also have held that documents in the possession of a party's agent—for example, an attorney—are considered to be within the party's control. *See, e.g., Commercial Credit Corp. v. Repper (In re Ruppert),* 309 F.2d 97, 98 (6th Cir.1962); *American Society for the Prevention of Cruelty to Animals v. Ringling Bros. & Barnum & Bailey Circus,* 233 F.R.D. 209, 212 (D.D.C.2006); *Gray,* 148 F.R.D. at 223. As the Sixth Circuit observed, "[i]f this were not so, then the client could always evade his duty to produce by placing the documents with his attorney." *In re Ruppert,* 309 F.2d at 98; *see also Cooper Industries,* 102 F.R.D. at 920 (ordering the production of documents in the possession of the defendant corporation's overseas affiliate, and reasoning that if this party "could so easily evade **discovery**" by "destroying its own copies and relying on ... copies maintained by its affiliate abroad," then "every United States company would have a foreign affiliate for **storing** sensitive documents").

Next, the courts have found that a corporate party may be deemed to have control over documents in the possession of one of its officers or employees. In *Riddell Sports Inc. v.*

Brooks, 158 F.R.D. 555, 558 (S.D.N.Y.1994), for example, the defendant sought to compel the production of tape recordings of his telephone conversations with an officer of the plaintiff corporation, Mr. Wingo, who had not been named a party to the suit. The plaintiff argued that these tapes belonged to Wingo, and not the corporation, "and therefore should have been sought by subpoena served on him personally." *Riddell Sports,* 158 F.R.D. at 558. The court disagreed, explaining that when materials are "created in connection with the officer's functions as a corporate employee, the corporation has a proprietary interest in them and the officer has a fiduciary duty to turn them over on demand." 158 F.R.D. at 559. Accordingly, because Wingo made the recordings at issue "in furtherance of his functions" as an officer of the plaintiff corporation, the court found that the tapes were within the control of this party, and thus "must be disclosed in response to a proper notice for production." 158 F.R.D. at 559.

***354** Indeed, this principle extends not just to documents in the actual possession of a non-party officer or employee of a corporate party, but also to materials that the officer or employee has a legal right to obtain. In *Herbst v. Able,* 63 F.R.D. 135, 136 (S.D.N.Y.1972), for instance, the plaintiffs sought the production of transcripts of testimony given by non-party employees of the defendant corporation, Douglas Aircraft Company, at a private hearing before the Securities and Exchange Commission ("SEC"). Douglas Aircraft objected to this request, stating that it did not have copies of these transcripts in its possession, and citing an SEC policy not to make such transcripts available to private litigants. Under another SEC rule, however, each witness was entitled to a transcript of his or her own testimony. In light of this rule, the court held that the plaintiffs were entitled to the requested transcripts, which Douglas Aircraft could obtain through its employees:

> Rule 34(a) plainly provides that a party may request another party to produce any designated document which is within the possession, custody or control of the party of whom the request is made. Plaintiffs, consequently, may request Douglas to have its non-defendant employees procure copies of their private testimony before the SEC so that Douglas may give same to plaintiffs. Plainly Douglas' employees are persons within its control. The testimony of these employees relates to Douglas' affairs.

Herbst, 63 F.R.D. at 138; see also *In re Domestic Air Transportation Antitrust Litigation,* 142 F.R.D. 354, 356 (N.D.Ga.1992) (ordering the defendant corporations to secure the consent of their employees in order to obtain and produce transcripts of deposition testimony given by these employees in a Department of Justice investigation).

Finally, in a relatively recent decision, a district court found that defendant El Paso Corporation had "control," within the meaning of Rule 34(a)(1), of electronic records maintained by a third party on the company's behalf. *See Tomlinson v. El Paso Corp.,* 245 F.R.D. 474, 477 (D.Colo.2007). In that case, defendant El Paso had a duty under the Employee Retirement Income Security **Act** of 1974 ("ERISA"), 29 U.S.C. § 1001 *et seq.,* and its implementing regulations to ensure that its employee benefit records were "maintained in reasonable order and in a safe and accessible place, and in such manner as they may be readily inspected or examined." *Tomlinson,* 245 F.R.D. at 477 (quoting 29 C.F.R. § 2520.107–1(b)). Although El Paso employed a third party, Mercer Human Resource Consulting, to administer its employee pension plan and maintain the electronic records associated with this plan, the court held that El Paso could not delegate its recordkeeping duties under ERISA to this third party. 245 F.R.D. at 477. Rather, the court held that El Paso retained control over the pension plan data held by Mercer, and thus had the "authority and ability to obtain" and produce the data requested by the plaintiff plan participants. 245 F.R.D. at 477.

[3] Applying Rule 34(a)(1) and its attendant case law here, the Court readily concludes that the Defendant City of Detroit has "control" over the text messages preserved by third party SkyTel pursuant to its contractual relationship with the City. To be sure, and as noted earlier, the Court's inquiry on this point is significantly hindered by the City's failure to produce any meaningful documentation that might reveal the terms of its agreements with SkyTel. In response to the Court's May 6, 2008 order directing it to produce copies of "any and all contracts" pursuant to which SkyTel provided text messaging services to the City and its employees, the City furnished a handful of one-page purchase orders, partial and unsigned SkyTel "Corporate Account Agreement" forms, and the like, none of which discloses the specific nature and extent of the services provided by SkyTel to the City during the course of their contractual relationship. Under this record, it is impossible to make any definitive pronouncements about

the degree of control granted to the City under its agreements with SkyTel.

Nonetheless, the record includes several other indicia of the City's control over the text messages maintained by SkyTel. First and foremost, the City's present motion is **premised** upon such control, first asserting *355 that the City has the ability to consent to SkyTel's production of the text messages at issue, but then stating that it is unwilling to do so. Specifically, in its motion and brief in support, the City affirmatively states that "[p]ursuant to [its] contract" with SkyTel, it was the "customer or subscriber" of the text messaging service provided by SkyTel. (Defendant City's Motion at ¶ 3; Br. in Support at 1.) Quoting the SCA provision permitting the disclosure of the contents of a **communication** "with the lawful consent of ... the subscriber," the City then states that "as subscriber to the subject SkyTel text messages," it "does not consent to the disclosure of these **communications**, as required by the SCA before such **communications** are divulged." (Defendant City's Motion, Br. in Support at 3 (citing 18 U.S.C. § 2702(b)(3)).)

Yet, if the City can ***block*** the disclosure of SkyTel messages by ***withholding*** its consent, it surely follows that it can ***permit*** the disclosure of these **communications** by ***granting*** its consent. This acknowledged power readily qualifies as a "legal right to obtain" the messages held by SkyTel, and hence constitutes "control" within the meaning of Rule 34(a)(1). *See In re Bankers Trust Co.*, 61 F.3d at 469. Indeed, the courts recognized precisely this point in *Herbst, supra*, 63 F.R.D. at 138, and *In re Domestic Air Transportation Antitrust Litigation*, 142 F.R.D. at 356, determining in each case that a party had control over materials in the possession of a third party by virtue of its ability to secure the consent that was necessary to obtain a copy of these materials. [17] Moreover, the above-cited case law confirm the obvious point that it is immaterial whether a party, such as the City here, might prefer not to give the necessary consent—if a party has the requisite control over a requested document, it must exercise this control in order to comply with the mandate of Rule 34. *See, e.g., Gray, supra*, 148 F.R.D. at 223. [18]

[4] The City's control over the SkyTel text messages is further confirmed by the Michigan law governing the maintenance and disclosure of public records. In particular, Michigan's Freedom of Information **Act** ("FOIA") mandates that, subject to various exceptions, a "public body shall furnish a requesting person a reasonable opportunity for inspection and examination of its public records." Mich. Comp. Laws § 15.233(3). There is no question that the Defendant City is a "public body" under the FOIA, *see* Mich. Comp. Laws § 15.232(d)(iii), and that at least some of the SkyTel text messages satisfy the statutory definition of "public records," insofar as they capture **communications** among City officials or employees "in the performance of an official function," *see* Mich. Comp. Laws § 15.232(e); *see also City of Warren v. City of Detroit*, 261 Mich.App. 165, 680 N.W.2d 57, 62 (2004) (confirming that the statutory definition of a "public record" includes information captured in electronic form); *Farrell v. City of Detroit*, 209 Mich.App. 7, 530 N.W.2d 105, 109 (1995) (same). [19] Indeed, the City has acknowledged that at least some of these **communications** are "public records," both through a policy directive promulgated to its employees —a directive which, among other things, cautions "users of the City's electronic **communications** *356 system" to "bear in mind that, whenever creating and sending an electronic **communication**, they are almost always creating a public record which is subject to disclosure," (*see* Plaintiff's Response, Ex. 9, Directive for the Use of the City of Detroit's Electronic **Communications** System at 2) [20] —and through its appeal in its present motion to the deliberative process privilege—a privilege which, as the City recognizes, encompasses only **communications** among City officials and employees pursuant to "their official positions within the City of Detroit government," (Defendant City's Motion at ¶ 7).

Because at least some of the text messages maintained by SkyTel are "public records" within the meaning of Michigan's FOIA, it would be problematic, to say the least, to conclude that the City lacks a legal right to obtain these records as necessary to discharge its statutory duty of disclosure. Such a conclusion also would be contrary to the pertinent Michigan case law. First, the Michigan courts have held that the FOIA duty of disclosure, like the Rule 34 duty of production, extends to public records within the possession ***or control*** of a public body. *See MacKenzie v. Wales Township*, 247 Mich.App. 124, 635 N.W.2d 335, 339 (2001); *Easley v. University of Michigan*, 178 Mich.App. 723, 444 N.W.2d 820, 822 (1989). Next, while there is no obligation under the Michigan FOIA to create public records, the statute does impose a "duty to provide access" to those public records that have been created and are the subject of a proper FOIA request, and this obligation "inherently includes the duty to preserve and maintain such records until access has been provided or a court executes an order finding the record to be exempt from disclosure." *Walloon Lake Water System, Inc. v. Melrose Township*, 163 Mich.App. 726, 415 N.W.2d 292,

295 (1987) (footnote omitted); *see also* Mich. Comp. Laws § 15.233(3) ("A public body shall protect public records from loss, unauthorized alteration, mutilation, or destruction."). In this respect, then, the City here stands on a similar footing to the defendant corporation in *Tomlinson, supra,* 245 F.R.D. at 477, which was found to have control over electronic records in the possession of a third party by virtue of its statutory obligation to maintain these records and make them available for examination or inspection.

Indeed, the decision of the Michigan Court of Appeals in *MacKenzie, supra,* is particularly instructive here. In that case, the defendant townships contracted with a third party, the City of Port Huron, to prepare property tax notices to be issued to township property owners. Under this contract, the townships supplied paper documents to Port Huron, which then "created magnetic computer tapes containing the pertinent tax information on each property owner." *MacKenzie,* 635 N.W.2d at 336. At the conclusion of this process, Port Huron returned the paper documents but retained the computer tapes. The plaintiff real estate broker submitted a FOIA request to the defendant townships seeking a copy of the computer tapes, but the townships resisted this request, contending that the tapes were not in their possession and that they were under no obligation to obtain them from Port Huron.

The Michigan Court of Appeals rejected the townships' arguments and ordered them to disclose the computer tapes to the plaintiffs. In so ruling, the court first ***357** found it immaterial that a third party, and not the townships, had created and retained possession of the tapes. Citing the FOIA's definition of a "public record" as including documents "used" by a public body in the performance of an official function, the court concluded that the townships had "used" the computer tapes, "albeit indirectly," by delegating to a third party, Port Huron, the "clerical task" of "prepar[ing] tax notices for mailing" and providing the information needed to perform this function. *MacKenzie,* 635 N.W.2d at 338. The court reasoned that this delegation did not defeat the townships' duty of disclosure, as public bodies "may not avoid their obligations under the FOIA by contracting for a clerical service that allows them to more efficiently perform an official function." 635 N.W.2d at 338.

Of particular significance here, the court next found that the defendant townships "maintained a measure of control over the tapes," by virtue of having provided the data used to created the tapes, and as evidenced by a letter from one of the townships to the plaintiff stating that Port Huron would not release the tapes without permission and that the township did not intend to give any such permission. 635 N.W.2d at 339. In light of this retained control, the court deemed it legally insignificant that the tapes were not in the townships' possession. 635 N.W.2d at 339 (citing Mich. Comp. Laws § 15.240(4), which authorizes the courts to order the production of "all or a portion of a public record wrongfully withheld, regardless of the location of the public record"). Rather, the court held that the townships were obligated to secure the production of the computer tapes, "whether by signing the release provided by Port Huron or [by] obtaining copies of the tapes and forwarding them to plaintiff." 635 N.W.2d at 339. This decision in *MacKenzie* provides a compelling basis for concluding that the Defendant City has control, within the meaning of Rule 34(a)(1), over any "public records" that might be retained by third party SkyTel under its contract with the City.

Finally, while the record does not disclose the terms of the City's contracts with SkyTel, it simply defies belief that SkyTel would maintain an archive of **communications**—many of which, as discussed, presumably qualify as public records and concern official City business—without providing any sort of contractual mechanism for the City to retrieve these messages. Presumably, a profit-seeking business such as SkyTel would not maintain such an archive unless it was compensated for this service, and the City, in turn, would not pay for this service unless it could gain access to the archive when desired. [21] In the absence of any evidence to the contrary, then, the Court assumes that the City has at least some sort of contractual right of access to the text messages preserved by SkyTel in the course of its contractual relationship with the City.

Given all these indicia of control, the Court finds that the text messages maintained by SkyTel would be an appropriate subject of a Rule 34 request for production directed at the Defendant City of Detroit. Pursuant to such a request, Plaintiff would be entitled to review any and all nonprivileged **communications** that are relevant to his claims, *see* Fed.R.Civ.P. 26(b)(1), absent some basis for concluding that these **communications** are beyond the reach of **civil discovery**. This, of ***358** course, leads the Court back to the proposition advanced in Defendants' motions—namely, that the SCA erects just such a bar to the production of any text messages preserved by SkyTel. Accordingly, the Court turns to this question.

4. The SCA Does Not Override Defendants' Obligation to Produce Relevant, Nonprivileged Electronic Communications Within Their Possession, Custody, or Control.

[5] As noted earlier, Defendants' challenge to Plaintiff's request for disclosure of the SkyTel text messages rests upon what they view as a straightforward reading of the terms of the SCA. In particular, they first point to the SCA provision that generally prohibits a service provider such as SkyTel from (i) "knowingly divulg[ing] to any person or entity the contents of a **communication** while in electronic storage by" an electronic **communication** service ("ECS"), 18 U.S.C. § 2702(a)(1), or (ii) "knowingly divulg[ing] to any person or entity the contents of any **communication** which is carried or maintained on" a remote computing service ("RCS"), 18 U.S.C. § 2702(a)(2). Next, while the SCA recognizes various exceptions to this general rule of non-disclosure, Defendants submit that the only relevant exception is disclosure "with the lawful consent of" the originator or intended recipient of a **communication** or (in the case of an RCS) the subscriber to the service, 18 U.S.C. § 2702(b)(3), and they state their unwillingness to give the requisite consent. It follows, in Defendants' view, that SkyTel may not produce any text messages in this case, whether pursuant to the subpoenas issued by Plaintiff or in accordance with the protocol established in this Court's March 20, 2008 opinion and related order.

In analyzing this contention, the Court initially proceeds under the premise that Plaintiff has sought the production of SkyTel text messages under a Rule 34 document request directed at the Defendant City, rather than a third-party subpoena directed at SkyTel.[22] Under this scenario, SkyTel would not be called upon to produce any text messages directly to Plaintiff. Rather, any such production would pass through an intermediary, the Defendant City, which would be obligated under Rule 34 and the above-cited case law to obtain the text messages from SkyTel and make them available to Plaintiff as materials within its "control."

There is reason to believe that the SCA might apply differently to (i) direct production to an outside party such as Plaintiff and (ii) production to a customer such as the City. First, the Court notes that the provisions upon which Defendants rely here prohibit a service provider from "divulg[ing]" the contents of a **communication**. 18 U.S.C. § 2702(a)(1)-(2). Although disclosure to an outside party plainly would qualify as "divulg[ing]" the contents of a **communication**, it is not self-evident that a service provider "divulge[s]" the contents of a **communication** merely by retrieving the **communication** from an archive and forwarding it to a customer pursuant to a contractual obligation. To "divulge" information ordinarily entails "mak[ing] known" or revealing something which is "private or secret." Webster's Ninth New Collegiate Dictionary at 370 (1986); *see also* Merriam–Webster Online Dictionary, *available at http://www.merriam-webster.com/dictionary/divulge*. By fulfilling a request from its customer, the City, to retrieve and forward **communications** from an archive that has been created and maintained at the customer's request, SkyTel cannot necessarily be characterized as having "divulged" any information to anyone outside the scope of the confidential relationship that exists between SkyTel and its customer.

If the archive and retrieval service provided by SkyTel qualifies as an RCS,[23] it is still more doubtful that this sort of retrieval would run afoul of § 2702(a). Under the pertinent subsection of § 2702(a), a service provider that provides an RCS is prohibited from "divulg[ing]" the "contents of any **communication** which is carried or maintained on ***359** that service ... on behalf of ... a subscriber or customer" only ***if*** the service provider "is not authorized to access the contents of any such **communications** for purposes of providing any services other than storage or computer processing." 18 U.S.C. § 2702(a)(2). Yet, to the extent that the contracts between the City and SkyTel provide a mechanism for the City to request the retrieval of text messages from the archive maintained by SkyTel, such a request presumably would supply the necessary "authoriz[ation]" for SkyTel to "access" the **communications** in this archive "for purposes of providing a [ ] service[ ] other than storage or computer processing"—namely, the service of retrieval. It is not a foregone conclusion, then, that SkyTel necessarily would engage in any activity prohibited under § 2702(a) by fulfilling the City's demand to retrieve text messages from an archive maintained at the behest of this customer.[24]

Next, even assuming that SkyTel were deemed to engage in activity within the scope of § 2702(a) by retrieving text messages from an archive and forwarding them to the City, the Court would not so readily conclude, as Defendants do, that only the "lawful consent" exception is potentially applicable here. Another exception permits the contents of a **communication** to be divulged "as may be necessarily incident to the rendition of the service" being provided. 18 U.S.C. § 2702(b)(5). As discussed earlier, it is difficult

to see how an archive of text messages would be of any use or value to a customer if the service provider did not also offer a mechanism for retrieving messages from this archive. Seemingly, then, SkyTel's retrieval of messages from the archive it has maintained on the City's behalf is "necessarily incident to" its ability to carry out the text message transmission and storage services it has agreed to provide to the City. [25]

In any event, even if Defendants are correct in their contention that SkyTel cannot produce any **communications** in this case without the "lawful consent" called for under § 2702(b)(3), the Court finds that the Defendant City has both the ability and the obligation to secure any such consent that the SCA may require. As observed earlier, the consent that is needed to satisfy § 2702(b)(3) depends upon the sort of service being provided. If this service is deemed to be an RCS, then the consent of the "subscriber" is sufficient to permit the service provider to divulge the contents of a **communication** maintained on this service. 18 U.S.C. § 2702(b)(3). [26] In contrast, if a service is determined to be an ECS, then only the "lawful consent of the originator or an addressee or intended recipient" of a **communication** will suffice to overcome the prohibition against divulging this **communication**. 18 U.S.C. § 2702(b)(3).

This distinction between an ECS and an RCS was central to the rulings of the district and appellate courts in *Quon*, with the district court initially determining that the service at issue in that case was an RCS. *See Quon,* 445 F.Supp.2d at 1137. In that case, the defendant municipality, the City of Ontario, California, entered into a contract with a service provider, Arch Wireless, that called for alphanumeric text-messaging devices and related wireless **communication** services to ***360** be provided to various city employees. In an effort to determine whether and to what extent these devices were being used for personal rather than work-related purposes, the city's chief of police ordered an audit of the text messages sent and received by two police officers over a two-month period. When this audit triggered an internal affairs investigation and other adverse consequences for the subjects of the audit and others whose **communications** were encompassed by the review, one of the police officers and several other city employees brought suit against Arch Wireless, the City of Ontario, and various city officials, asserting federal claims under the SCA and 42 U.S.C. § 1983 as well as claims under California law.

Arch Wireless moved for summary judgment in its favor on the plaintiffs' SCA claim, arguing that the service it provided was an RCS and that the city, by requesting the disclosure of text messages maintained on this service, had provided the subscriber consent necessary to permit these disclosures without violating the prohibitions set forth in § 2702(a). In addressing this question, the district court initially observed that Arch Wireless appeared to have provided a "computer storage" service that was characteristic of an RCS, as the messages it had provided to the city were retrieved from long-term storage after already having been delivered and read by their recipients. *See Quon,* 445 F.Supp.2d at 1130–31. Nonetheless, the court acknowledged that the maintenance of the text message in storage was not enough, standing alone, to distinguish an RCS from an ECS, because the SCA expressly contemplates that an ECS also entails the "electronic storage" of **communications**. *See Quon,* 445 F.Supp.2d at 1134–36; *see also* 18 U.S.C. § 2702(a)(1) (prohibiting a provider of an ECS from divulging "the contents of a **communication** while in electronic storage by that service"). [27] Moreover, while it was clear that Arch Wireless provided an ECS to the city by supplying text messaging devices and associated services that enabled city employees to send and receive electronic **communications**, *see* 18 U.S.C. § 2510(15), the district court construed the SCA and its legislative history as eschewing an "all or nothing" approach to characterizing a service provider's activities, and as instead recognizing that a service provider such as Arch Wireless could provide ***both*** RCSs and ECSs to a single customer. *Quon,* 445 F.Supp.2d at 1136–37; *see also* Orin S. Kerr, *A User's Guide to the **Stored Communications Act**, and a Legislator's Guide to Amending It,* 72 Geo. Wash. L.Rev. 1208, 1215–16 (2004) (noting the "functional nature of the definitions of ECS and RCS," with the result that a "provider can **act** as an RCS with respect to some **communications** [and] an ECS with respect to other **communications**"). [28]

***361** Thus, the key question before the district court was whether the specific service that gave rise to the plaintiffs' SCA claims—*i.e.,* Arch Wireless's retrieval of text messages from storage after they had been transmitted and read by their recipients—should be deemed to be an RCS or an ECS. This, in turn, required the court to distinguish between the "electronic storage" utilized by an ECS and the "computer storage" provided by an RCS. As to the former, the statute defines "electronic storage" as "any temporary, intermediate storage of a wire or electronic **communication** incidental to the electronic transmission thereof," or "any storage of such **communication** by an electronic **communication** service

for purposes of backup protection of such **communication**." 18 U.S.C. § 2510(17). Because the text messages that Arch Wireless had retrieved from storage and forwarded to the city had already been transmitted and read in the past, their continued storage could not be construed as "temporary" or "incidental to" their transmission. Rather, the district court reasoned that the characterization of Arch Wireless's service as an ECS or an RCS turned upon whether the text messages had been **stored** "for purposes of backup protection." *See Quon,* 445 F.Supp.2d at 1136.

The court concluded that this was not the purpose for which Arch Wireless had **stored** the text messages that it subsequently provided to the city. In so ruling, the court relied principally on the Ninth Circuit's observation in an earlier case that a service does not **store** messages "for backup purposes" if it is "the only place a user **stores** his messages." *Quon,* 445 F.Supp.2d at 1136 (quoting *Theofel v. Farey–Jones,* 359 F.3d 1066, 1077 (9th Cir.2004)). The district court reasoned that "Arch Wireless' service would meet this definition," where the storage it provided was "long-term" and was "apparently ... the single place where text messages, after they have been read, are archived for a permanent record-keeping mechanism." *Quon,* 445 F.Supp.2d at 1136; *see also Theofel,* 359 F.3d at 1076 (reasoning that an internet service provider "that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages"). Consequently, the court held that the service provided by Arch Wireless was an RCS, and that any disclosures of **communications** maintained on this service were permissibly made with the consent of the subscriber City of Ontario. *See Quon,* 445 F.Supp.2d at 1137.

In its recent decision, however, the Ninth Circuit reversed this aspect of the district court's ruling, and held that "Arch Wireless provided an 'electronic **communication** service' to the City." *Quon,* 529 F.3d at 903. This decision appears to rest on the "all-or-nothing" approach rejected by the district court, with the Ninth Circuit broadly "categoriz[ing] Arch Wireless" as providing a service for sending and receiving electronic **communications**, as opposed to a "computer storage" service. 529 F.3d at 901. While the court recognized that Arch Wireless did "archiv[e] ... text messages on its server," it noted that both ECSs and RCSs entail some form of "storage," and it found that Arch Wireless did not provide the "virtual filing cabinet" function that was cited in the legislative history of the SCA as characteristic of an RCS. 529 F.3d at 901–02.

The Ninth Circuit then explained that the district court's reliance on its *Theofel* decision was misplaced, and that this prior ruling, properly understood, actually led to the opposite conclusion. As observed in *Quon,* the court in *Theofel* held that an internet service provider ("ISP") had **stored** e-mail messages on its server "for purposes of backup protection," since "[a]n obvious purpose for **storing** a message on an ISP's server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user's own computer." *Theofel,* 359 F.3d at 1075. The court in *Quon* found that this ruling governed the case before it, where "[t]he service provided by [the ISP in *Theofel]* is closely analogous to Arch Wireless's storage of [the plaintiffs'] messages," and where it was "clear that the messages were archived for 'backup protection,' just as they were in *Theofel.*" *Quon,* 529 F.3d at 902.

Finally, the Ninth Circuit addressed certain language in *Theofel* that Arch Wireless ***362** (and the district court) viewed as supporting the conclusion that its storage of messages was ***not*** for "backup protection":

> Arch Wireless contends that our analysis in *Theofel* of the definition of "backup protection" supports its position. There, we noted that "[w]here the underlying message has expired in the normal course, any copy is no longer performing any backup function. An ISP that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages." [*Theofel,* 359 F.3d] at 1070. Thus, the argument goes, Arch Wireless's permanent retention of the [plaintiffs'] text messages could not have been for backup purposes; instead, it must have been for storage purposes, which would require us to classify Arch Wireless as an RCS. This reading is not persuasive. First, there is no indication in the record that Arch Wireless retained a permanent copy of the text messages or **stored** them for the benefit of the City; instead, the [declaration of an Arch Wireless employee] simply states that copies of the messages are "archived" on Arch Wireless's server. More importantly, *Theofel's* holding—that the e-mail messages **stored** on [the ISP's] server after delivery were for "backup protection," and that [the ISP] was undisputedly an ECS—forecloses Arch Wireless's position.

Quon, 529 F.3d at 902–03. Thus, the court held that Arch Wireless provided an ECS to the city, and that it violated the SCA by disclosing transcripts of text messages to the city without first securing the consent of the originator, addressee,

or intended recipient of each such **communication**. 529 F.3d at 903.

Upon carefully reviewing the district and appellate court rulings in *Quon,* this Court finds the lower court's reasoning more persuasive, on a number of grounds. First, the Court reads the Ninth Circuit's decision in that case—and, to some extent, the court's prior ruling in *Theofel*—as resting on a unitary approach, under which service providers contract with their customers to provide either an ECS or an RCS, but not both. Yet, the prohibitions against disclosure set forth in § 2702(a) focus on the specific type of service being provided (an ECS or an RCS) with regard to a particular **communication**, and do not turn upon the classification of the service provider or on broad notions of the service that this entity generally or predominantly provides. Thus, the Court is inclined to agree with the view of the district court in *Quon* that "Congress took a middle course" in enacting the SCA, under which a service provider such as SkyTel may be deemed to provide both an ECS and an RCS to the same customer. *Quon,* 445 F.Supp.2d at 1137; *see also* Kerr, *supra,* at 1215–16.

In light of the SCA's functional, context-specific definitions of an ECS and an RCS, it is not dispositive that SkyTel indisputably did provide an ECS to the City of Detroit in the past, or that it presumably kept text messages in "electronic storage" at times in connection with the ECS that it provided. Rather, the ECS/RCS inquiry in this case turns upon the characterization of the service that SkyTel ***presently*** provides to the City, pursuant to which the company is being called upon to retrieve text messages from an archive of **communications** sent and received by City employees in years past using SkyTel text messaging devices. The resolution of this issue, in turn, depends upon whether SkyTel has maintained this archive "for purposes of backup protection," 18 U.S.C. § 2510(17)(B), so that its contents may be deemed to be held in "electronic storage" by an ECS, 18 U.S.C. § 2702(a)(1), or whether this archive is more properly viewed as "computer storage" offered by an RCS, 18 U.S.C. § 2711(2).

Whatever might be said about the reasoning through which the district and appellate courts in *Quon* determined that the archive of text messages in that case did or did not serve the purpose of "backup protection,"[29] ***363** the circumstances of this case are far clearer. SkyTel is no longer providing, and has long since ceased to provide, a text messaging service to the City of Detroit—the City, by its own admission, discontinued this service in 2004, and the text messaging devices issued by SkyTel are no longer in use. Consequently, any archive of text messages that SkyTel continues to maintain on the City's behalf constitutes the ***only*** available record of these **communications**, and cannot possibly serve as a "backup" copy of **communications** **stored** elsewhere. In this respect, this Court is in complete agreement with the Ninth Circuit's observations in *Theofel,* 359 F.3d at 1076–77, that a service provider "that kept permanent copies of temporary messages could not fairly be described as 'backing up' those messages," and that "messages are not **stored** for backup purposes" if a computer repository is "the only place" where they are **stored**. Regardless of whether these observations applied to the services at issue in *Theofel* and *Quon,* the Court concludes that they apply with full force here—the service provided by SkyTel may properly be characterized as a "virtual filing cabinet" of **communications** sent and received by City employees. *See Quon,* 529 F.3d at 902. The Court finds, therefore, that the archive maintained by SkyTel constitutes "computer storage," and that the company's maintenance of this archive on behalf of the City is a "remote computing service" as defined under the SCA.

It is only a short step from this finding to the conclusion that the Defendant City is both able and obligated to give its consent, as subscriber, to SkyTel's retrieval of text messages so that the City may comply with a Rule 34 request for their production. As previously discussed, a party has an obligation under Rule 34 to produce materials within its control, and this obligation carries with it the attendant duty to take the steps necessary to exercise this control and retrieve the requested documents. Moreover, the Court already has explained that a party's disinclination to exercise this control is immaterial, just as it is immaterial whether a party might prefer not to produce documents in its possession or custody. Because the SkyTel archive includes **communications** that are potentially relevant and otherwise **discoverable** under the standards of Rule 26(b)(1), and because the City has "control" over this archive within the meaning of Rule 34(a)(1) and the case law construing this term, the City must give any consent that might be required under the SCA in order to permit SkyTel to retrieve **communications** from this archive and forward them to the Magistrate Judges in accordance with the protocol established in this Court's March 20, 2008 order.

Contrary to Defendant Kilpatrick's contention in his response to the Detroit Free Press's *amicus* brief, it is not an "oxymoron" to conclude, under the particular circumstances

presented here, that a party may be compelled to give its consent. It is a necessary and routine incident of the rules of **discovery** that a court may order disclosures that a party would prefer not to make. As illustrated by the survey of Rule 34 case law earlier in this opinion, this power of compulsion encompasses such measures as are necessary to secure a party's compliance with its **discovery** obligations. In this case, the particular device that the SCA calls for is "consent," and Defendant Kilpatrick has not cited any authority for the proposition that a court lacks the power to ensure that this necessary authorization is forthcoming from a party with the means to provide it. Were it otherwise, a party could readily avoid its **discovery** obligations by warehousing its documents with a third party under strict instructions to release them only with the party's "consent."

[6] Alternatively, even if the Court is mistaken in its conclusion that the service provided by SkyTel is an RCS, there is ample basis to conclude that the City nonetheless ***364** has an obligation to secure the requisite consent from its employees that would permit SkyTel to proceed with its retrieval of **communications**. This, after all, is precisely what the courts have held in the Rule 34 case law discussed earlier, including *Riddell Sports,* 158 F.R.D. at 559, *Herbst,* 63 F.R.D. at 138, and *In re Domestic Air Transportation Antitrust Litigation,* 142 F.R.D. at 356. In particular, *Riddell Sports,* 158 F.R.D. at 559, holds that a corporate party has control over, and thus may be compelled to produce, documents in the possession of one of its officers or employees, and that the officer or employee has a fiduciary duty to turn such materials over to the corporation on demand. Next, *Herbst,* 63 F.R.D. at 138, and *In re Domestic Air Transportation Antitrust Litigation,* 142 F.R.D. at 356, illustrate the principle that the Rule 34(a) concept of "control" extends to a company's control over its employees, such that a corporate party may be compelled to secure an employee's consent as necessary to gain access to materials that the employee has the right to obtain. In accordance with these authorities, the Court finds that the City of Detroit is both able and obligated to obtain any consent from its employees that would be necessary to permit SkyTel to retrieve the **communications** of City employees from its archive and forward them to the Magistrate Judges for review.

This conclusion is confirmed by the case law construing the same or similar "consent" provisions found in the SCA's close cousin, the federal Wiretap **Act**, 18 U.S.C. § 2510 *et seq.* Under one such provision, the interception of a "wire, oral, or electronic **communication**" is permissible "where one of the parties to the **communication** has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). Another provision, like its counterpart at § 2702(b)(3) of the SCA, permits a "person or entity providing electronic **communication** service" to "divulge the contents of" a **communication** "with the lawful consent of the originator or any addressee or intended recipient of such **communication**." 18 U.S.C. § 2511(3)(b)(ii).

The courts have held that the requisite consent to interception or disclosure may be implied under circumstances analogous to those presented here. In *Griffin v. City of Milwaukee,* 74 F.3d 824 (7th Cir.1996), for example, the plaintiff was employed as a telephone operator for the Milwaukee police department, and she alleged that her employer had illegally monitored and intercepted her personal telephone calls. In affirming the district court's award of summary judgment in the employer's favor, the court noted that the plaintiff had been informed that "workstation telephone calls might be monitored for training, evaluation, and supervision purposes," and that the plaintiff herself had testified that "she knew that her telephone conversations at her workstation could be monitored by supervisors." *Griffin,* 74 F.3d at 827. Moreover, employees were told "that incoming emergency calls would be recorded," and the equipment to do so was "located conspicuously in a glass case in the middle of [the plaintiff's] work area." 74 F.3d at 827. Under this record, the court concluded that the defendant employer's "systematic monitoring of workstation telephones occurred with [the plaintiff's] consent." 74 F.3d at 827; *see also United States v. Rittweger,* 258 F.Supp.2d 345, 354 (S.D.N.Y.2003) (finding that an employee had given his implied consent to his employer's interception of his phone calls where the employer had disseminated a memo and handbooks advising employees that their calls were being recorded and were subject to review); *George v. Carusone,* 849 F.Supp. 159, 164 (D.Conn.1994) (finding implied consent in light of the memoranda circulated to employees informing them that their calls would be recorded and the warning labels to this effect that were affixed to many phones around the workplace).

In this case, City of Detroit employees were similarly advised, under the above-cited electronic **communications** policy directive signed by Defendant Kilpatrick, that they should "assume [as] a 'rule of thumb' that any electronic **communication** created, received, transmitted, or **stored** on the City's electronic **communication** system is public information, and may be read by anyone." (Plaintiff's Response, Ex. 9, Directive for the Use of the City of Detroit's

Electronic **Communications** System at 4.) In addition, this directive states that all such **communications** ***365** are "the property of the City," that they should not be "considered, in whole or in part, as private in nature regardless of the level of security on the **communication**," and that, "in accordance with the applicable law governing access or disclosure, the City reserves the right to access electronic **communications** under certain circumstances and/or to disclose the contents of the **communication** without the consent of" its originator or recipient. (*Id.* at 1–2.) Finally, and as noted earlier, the directive cautions employees to "bear in mind that, whenever creating and sending an electronic **communication**, they are almost always creating a public record which is subject to disclosure" under the Michigan FOIA, regardless of "whether the **communication** is routine or intended to be confidential."

In light of this directive, a strong case can be made that City employees have given their implied consent to SkyTel's production of text messages to the City, at least under the circumstances presented here. First, SkyTel's disclosure here is for the limited purpose of enabling the City to fulfill its **discovery** obligations, which comports with the statements in the directive that employee **communications** are the property of the City and that, as such, the City reserves the right to access or disclose the contents of these **communications** in accordance with applicable law. Next, the Court already has explained that the text messages that are **discoverable** here can by no means be characterized as private or personal, but instead are confined to **communications** concerning official City business. Again, the directive emphasizes precisely this point, advising employees that their **communications** often will be deemed public records which are subject to disclosure.

To be sure, the courts have cautioned that consent under the federal Wiretap **Act** "is not to be cavalierly implied," *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581 (11th Cir.1983), and the case law illustrates that consent may not be implied where, for example, the employer's stated policy of monitoring does not encompass the particular sort of **communication** at issue, *see Watkins*, 704 F.2d at 581–82, or where the employer's actual practices deviate from its written policies, *see Quon*, 529 F.3d at 906–07. Yet, in this case, it is important to recall exactly ***who*** is challenging the efficacy of the City's policy directive as proof of the City's and its employees' consent to the disclosure of electronic **communications**. Out of the several current and former City of Detroit officials and employees who are named as Defendants in this case, only two have challenged SkyTel's retrieval and production of text messages as prohibited under the SCA: Defendant Kwame Kilpatrick, the mayor of Detroit, who signed the City's policy directive, and Defendant Christine Beatty, the mayor's chief of staff at all times relevant to this case. The remaining Defendants have not joined in the SCA-based challenge being pursued by the City and Defendants Kilpatrick and Beatty.

Whatever any given City of Detroit employee might be able to say about his or her awareness of the City's electronic **communications** policy or any lack of rigor or consistency in its enforcement, such arguments are singularly ineffective —and, indeed, give cause for concern—when raised by two of the City's highest-ranking officials, at least one of whom unquestionably has policymaking authority for the City and ***authorized the policy in question.*** It is problematic, to say the least, for someone in Defendant Kilpatrick's position to attempt to deny or diminish the import of the City's electronic **communications** policy as it applies to him, when an important purpose of this policy is to provide notice to rank-and-file employees that their **communications** are subject to access and disclosure as public records and as property of the City. As *Quon* well illustrates, a municipal policy governing city employees may be undermined by a policymaker's or supervisor's inconsistent or contrary practice, *see Quon*, 529 F.3d at 906–07, thereby impairing the city's ability to investigate employee wrongdoing.[30] Perhaps this is why ***366** the remaining individual Defendants in this case—including the City's chief of police, Ella Bully–Cummings—have elected not to join in the SCA-based challenge mounted by the Defendant City and Defendants Beatty and Kilpatrick, where a "victory" on this issue threatens to eliminate an important tool for uncovering government corruption.

Finally, the Court returns to the premise under which it has conducted its SCA analysis—namely, that Plaintiff has sought the disclosure of SkyTel text messages via a Rule 34 request for production, as opposed to a third-party subpoena. As this premise is incorrect, the Court necessarily must address the legal significance of Plaintiff's election to proceed via the latter means of **discovery**. The question, in particular, is whether the Court's analysis and conclusions continue to hold true where production is sought directly from a non-party, rather than from a party that retains control over materials in the nonparty's possession.

The Court finds it best to avoid this question, and to instead insist that Plaintiff reformulate his third-party subpoena as a Rule 34 request for production directed at the Defendant City. If Plaintiff were to continue to proceed via a third-party subpoena, it seems apparent that SkyTel's compliance would

qualify as "divulg[ing]" the contents of **communications** within the meaning of § 2702(a), and that, as Defendants have argued, this disclosure could only be made with the "lawful consent" referred to in § 2702(b)(3). Moreover, while Rule 34 and its attendant case law provide clear authority for insisting that a party consent to the disclosure of materials within its control, there is very little case law that confirms the power of a court to compel a party's consent to the disclosure of materials pursuant to a third-party subpoena. [31]

In an effort to avoid such potentially difficult questions where a more straightforward path is readily available, the Court instructs Plaintiff to prepare and serve a Rule 34 request for production of the relevant text messages maintained by SkyTel on behalf of the Defendant City. The City shall then forward this **discovery** request to SkyTel, and SkyTel, in turn, shall proceed in accordance with the protocol set forth in the Court's March 20, 2008 order. By directing the parties to proceed in this manner, the Court obviates the need to determine what powers it might possess to compel a service provider such as SkyTel to comply with a third-party subpoena, and the Court leaves this question for another day. Rather, because production will be sought under Rule 34, the Court may resort to the usual mechanisms for ensuring the parties' compliance. *See, e.g.,* Fed.R.Civ.P. 37. [32]

*367 IV. *CONCLUSION*

For the reasons set forth above,

NOW, THEREFORE, IT IS HEREBY ORDERED that Defendant Christine Beatty's April 25, 2008 motion to preclude **discovery** of electronic **communications** from SkyTel is GRANTED IN PART and DENIED IN PART, in accordance with the rulings in this opinion and order. Similarly, IT IS HEREBY ORDERED that the Defendant City of Detroit's May 2, 2008 motion to preclude **discovery** of electronic **communications** from SkyTel also is GRANTED IN PART and DENIED IN PART, in accordance with the rulings in this opinion and order. In light of these rulings, Plaintiff is directed to promptly prepare and serve an appropriate Rule 34 request for production directed at the City of Detroit, and the parties are then directed to proceed in accordance with the rulings in this opinion and the protocol established in the Court's March 20, 2008 order.

Next, IT IS HEREBY ORDERED that non-party SkyTel's May 13, 2008 motion to quash is GRANTED IN PART and DENIED IN PART, in accordance with the rulings in this opinion and order. Finally, IT IS HEREBY ORDERED that the July 23, 2008 motion of the Detroit Free Press for leave to file an *amicus* brief is GRANTED.

SO ORDERED.

All Citations

252 F.R.D. 346

Footnotes

1 This statute was enacted as Title II of the Electronic **Communications** Privacy **Act** of 1986, Pub.L. No. 99–508, 100 Stat. 1848, but will be referred to here by its more common name of the **Stored Communications Act**.

2 Defendant Kwame Kilpatrick has since joined in Defendant Beatty's motion.

3 SkyTel recently was acquired by Velocita Wireless, but will be referred to by its former name throughout this opinion.

4 On this point—as with so many others relating to the City's use of SkyTel as its text messaging service provider—the record is devoid of helpful information. In particular, the City has not divulged, and the record does not otherwise reveal, the nature and extent of SkyTel's obligation under the parties' contract to maintain copies of **communications** sent or received via SkyTel text messaging devices during the period when the company provided these services to the City. More generally, the record discloses virtually nothing about the precise services provided by SkyTel to the City or the underlying technological means by which these services were performed. The Court revisits these evidentiary deficiencies below, as relevant to the issues presented in the motions now under consideration.

5 As discussed below, Defendants retreat somewhat from this broad proposition in the briefs in support of their motions, and instead argue that such **communications** cannot be obtained from an outside service provider in **civil** litigation.

6 The SCA also prohibits a service provider from divulging subscriber or customer information or records "to any governmental entity." 18 U.S.C. § 2702(a)(3). As discussed in the Court's prior May 6, 2008 order in this case, this provision is not applicable here, where any such subscriber or customer information is being sought by a private party, Plaintiff.

7 The SCA incorporates by reference this definition (and others) found in the federal Wiretap **Act**. *See* 18 U.S.C. § 2711(1).

8 An "electronic **communications** system," in turn, is defined as encompassing "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic **communications**, and any computer facilities or related electronic equipment for the electronic storage of such **communications**." 18 U.S.C. § 2510(14).

9 In contrast to § 2702, a separate SCA provision permits a "governmental entity" to compel the disclosure of the contents of an electronic **communication** through such means as a warrant or an administrative subpoena. 18 U.S.C. § 2703(a)-(b). This provision does not apply here, however, where production of electronic **communications** is sought by a private party. Accordingly, this case presents no occasion to decide how a governmental entity could properly secure the disclosure of any text messages maintained by SkyTel.

10 As SkyTel points out in its motion to quash, while § 2702 lacks any language explicitly authorizing the disclosure of the contents of an electronic **communication** pursuant to a court order, a service provider's "good faith reliance" on such an order operates as a "complete defense to any **civil** or criminal action brought under [the SCA] or any other law." 18 U.S.C. § 2707(e); *see also McCready v. eBay, Inc.*, 453 F.3d 882, 892 (7th Cir.2006). Not surprisingly, then, in the event that the Court permits the **discovery** of text messages maintained by SkyTel, the company requests that the Court issue an order compelling its participation in this effort.

11 This list included, for example, Carlita Kilpatrick, the wife of Detroit mayor (and Defendant) Kwame Kilpatrick. The record does not disclose whether a SkyTel text messaging device was issued to Carlita Kilpatrick under the company's contract with the City of Detroit.

12 If, after the Magistrate Judges' threshold determination of relevance, any Defendant wishes to oppose the production of one or more text messages on the ground that they should be deemed "private" **communications**, the Court certainly would entertain such a challenge at that time. As indicated, however, such a claim of privacy seems unlikely to succeed under the circumstances presented here.

13 More generally, the Court notes that *Quon* addresses a government employee's reasonable expectation of privacy in the context of a Fourth Amendment claim asserted by the plaintiff employees in that case against their municipal employer. *See Quon*, 529 F.3d at 903. Here, in contrast, the **discovery** efforts of the private Plaintiff do not implicate the Fourth Amendment protection against unreasonable searches and seizures. *See United States v. Jacobsen*, 466 U.S. 109, 113, 104 S.Ct. 1652, 1656, 80 L.Ed.2d 85 (1984) (confirming that the Fourth Amendment "proscrib[es] only governmental action," and does not apply to searches conducted by private individuals); *see also United States v. International Business Machines Corp.*, 83 F.R.D. 97, 102 (S.D.N.Y.1979) ("It strains common sense and constitutional analysis to conclude that the fourth amendment was meant to protect against unreasonable **discovery** demands made by a private litigant in the course of **civil** litigation."). As to the possible relevance of other aspects of the *Quon* decision, the Court addresses this subject below.

14 Notably, in finding that the review of text messages by the defendant city officials in *Quon* violated the plaintiff employees' Fourth Amendment rights, the Ninth Circuit cited various ways that this review could have been conducted differently in order to minimize the intrusion upon the plaintiffs' privacy interests. *See Quon*, 529 F.3d at 908–09. In this respect, *Quon* seems to support, rather than call into question, this Court's efforts to implement a protocol that protects against overbroad disclosure of **communications** to Plaintiff.

15 Indeed, one of the principal objectives of the 2006 amendments to the Rule was to explicitly extend the Rule's coverage to electronically **stored** information. *See* Fed.R.Civ.P. 34, Advisory Committee Note to 2006 Amendments.

16 Some courts have adopted a more expansive notion of "control," finding that it extends to circumstances where a party has the "practical ability to obtain the documents from a nonparty to the action." *Bank of New York v. Meridien BIAO Bank Tanzania Ltd.*, 171 F.R.D. 135, 146 (S.D.N.Y.1997).

17 These cases go farther, in fact, holding that a corporate party has the obligation to secure any necessary consent from its non-party employees. The Court returns below to this aspect of the case law.

18 The **discovery** process would undoubtedly be more streamlined if a party's duty of disclosure were limited solely to the information it was willing to part with voluntarily. It is well established, however, that the Federal Rules governing **discovery** "often allow extensive intrusion into the affairs of both litigants and third parties." *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 30, 104 S.Ct. 2199, 2206, 81 L.Ed.2d 17 (1984) (footnote omitted).

19 The Court is aware, of course, of a suit pending in the Michigan courts in which two Detroit newspapers are pursuing disclosure under the FOIA of a different subset of text messages maintained by SkyTel under its contract with the City of Detroit. In its limited discussion here of the terms of the FOIA, the Court does not seek or intend to express any view as to whether any of the SkyTel text messages might be subject to disclosure under this Michigan statute, or whether any of the

statutory exceptions to disclosure might apply. Rather, it is enough, for present purposes, to confirm that at least some of the text messages maintained by SkyTel surely qualify as "public records" within the meaning of Michigan's FOIA.

20 In her reply brief in support of her motion, Defendant Beatty challenges the authenticity of this directive submitted by Plaintiff, observing that it is signed by Defendant Kilpatrick, and yet bears a date (June 26, 2000) prior to the date that he took office as the mayor of Detroit. Yet, this is surely a mere typographical error, as evidenced by the absence of any claim by either Defendant Kilpatrick or the City that this directive does not accurately reflect the City's policy regarding electronic **communications**. Plainly, these parties are in the best position to address this question, and yet neither has done so, despite ample opportunity. In any event, it appears that Defendant Kilpatrick recently issued a revised directive with similar language, stating that "electronic **communications** may be deemed under the law to be public records," and that "users of the City's electronic **communications** system must bear in mind that, whenever creating and sending an electronic **communication**, the information may be subject to court-ordered disclosure." (4/15/2008 Directive for the Use of the City of Detroit's Electronic **Communications** System at 2, *available at* http://info.detnews. com/pix/2008/pdf/citydirective.pdf.)

21 The only evidence in the record that has any bearing upon this question is a printout of a SkyTel web page attached as an exhibit to Plaintiff's response to the City's motion. This web page describes a "Message Archiving" service that SkyTel apparently offers to its customers, under which a customer may retrieve messages **stored** by SkyTel by faxing a request to the company. (*See* Plaintiff's Response, Ex. 8.) Unfortunately, the record does not indicate whether SkyTel provided this or some comparable service under its contracts with the City.

Nonetheless, SkyTel seemingly has confirmed, albeit only in a general way, that it provided some sort of archiving service to the City. In its brief in support of its motion to quash, SkyTel quotes a passage from the district court's decision in *Quon* characterizing the service provider in that case as having "archived" the defendant municipality's text messages as "a permanent record-keeping mechanism." (SkyTel's Motion, Br. in Support at 7 (quoting *Quon v. Arch Wireless Operating Co.*, 445 F.Supp.2d 1116, 1136 (C.D.Cal.2006)).) SkyTel then states that "[t]his description applies squarely to" the service it provided to the City of Detroit. (*Id.*)

22 The Court recognizes, of course, that this premise is inaccurate, and will return below to the legal significance of Plaintiff's election to proceed via subpoena.

23 The Court addresses this question in greater detail below.

24 The Court recognizes that the defendant service provider in *Quon* engaged in similar activity, and that the Ninth Circuit held in its recent decision that the service provider had violated § 2702(a) as a matter of law. *See Quon*, 529 F.3d at 903. It does not appear from the published decisions in that case, however, that any party raised the question whether the service provider "divulge[d]" any **communications** within the meaning of § 2702(a), nor whether such "divulg[ing]" might be permissible if done in the course of providing an authorized service other than storage or computer processing. In addition, the Ninth Circuit's ruling in *Quon* rested in large part upon the court's determination that the service provider in that case was providing an ECS, and not an RCS. *See Quon*, 529 F.3d at 903. Again, the Court addresses this question below.

25 Again, it does not appear that the parties in *Quon* raised this issue, and the published decisions in that case do not address it.

26 The parties agree that the City is the "subscriber" of SkyTel's text messaging services within the meaning of § 2702. Thus, if the relevant service provided by SkyTel to the City is properly characterized as an RCS, SkyTel need only secure the City's consent in order to divulge the contents of any **communications** it has archived under its contracts with the City.

27 As the district court pointed out, this common feature of "storage" shared by both an ECS and an RCS serves to distinguish the types of activities covered by the SCA from the types of activities covered by the federal Wiretap **Act**. *See Quon*, 445 F.Supp.2d at 1134–35 (citing *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876–79 (9th Cir.2002)).

28 The Kerr article, the legislative history of the SCA, and other relevant authorities are discussed extensively in an *amicus* brief that the Detroit Free Press seeks to file in this case. Prior to this submission, neither Plaintiff nor Defendants had provided much discussion or analysis of the terms of the SCA, and they had cited very little case law or other pertinent authorities, apart from the *Quon* decisions, that might assist the Court in interpreting this statute. Spurred by the Free Press's submission, however, Defendants Beatty and Kilpatrick have filed briefs that give more extensive treatment to this subject.

Under these circumstances, the Court finds that leave should be granted for the Detroit Free Press to file its proposed *amicus* brief in this suit. First, the Free Press points out that this Court's interpretation of the SCA—to the extent that this is necessary to resolve Defendants' motions—is likely to have at least some impact upon the interests that the newspaper seeks to vindicate in its pending state court FOIA suit against the City of Detroit. There is undeniably

some overlap in the legal issues raised in that case and in Defendants' motions, where the Free Press is seeking disclosure of a different subset of the text messages maintained by SkyTel on behalf of the City of Detroit, and where the newspaper faces an SCA-based challenge to this effort that is quite similar to the SCA-based challenge advanced in Defendants' present motions. Moreover, and as noted above, the *amicus* brief submitted by the Free Press offers a unique perspective and analysis of the terms of the SCA which the parties' submissions did not supply, at least prior to the Free Press's filing. The Court welcomes this assistance in resolving the issues before it, and thus has considered the Free Press's *amicus* brief in preparing this opinion.

29 The Court confesses that it is puzzled by the Ninth Circuit's observation that there was "no indication in the record" in that case that "Arch Wireless retained a permanent copy of the text messages or **stored** them for the benefit of the City," and that the evidence "instead" showed "that copies of the messages are 'archived' on Arch Wireless's server." *Quon,* 529 F.3d at 902–03. In this Court's view, an "archive" is commonly understood as a permanent record, and the district court in *Quon* characterized Arch Wireless's repository in that case as "the single place where text messages, after they have been read, are archived for a permanent record-keeping mechanism." *Quon,* 445 F.Supp.2d at 1136. Moreover, once a service provider has successfully delivered a given text message to its intended recipient and the message has been opened and read, it would appear that any retention of a copy of this message in an "archive" could only be intended "for the benefit of" the customer, because this practice would serve no apparent purpose, whether backup or otherwise, for the service provider in its role as ECS.

30 Notably, while the defendant City of Ontario's review of text messages in *Quon* was primarily intended to ascertain the extent to which employees were using city-issued pagers for personal **communications**, these text messages also were reviewed in connection with an internal affairs investigation into police dispatchers who had tipped off Hell's Angels motorcycle gang members about an ongoing sting operation. *See Quon,* 445 F.Supp.2d at 1121–22.

31 While there are cases in which, for example, a party is ordered to execute a release authorizing the production of medical records from a non-party physician, these cases tend to rest upon notions of waiver rather than control over non-party materials. *See, e.g., Vartinelli v. Caruso,* No. 07–12388, 2008 WL 2397666, at *2–3 (E.D.Mich. June 10, 2008).

32 In light of the Court's rulings, it would appear that the issues raised in SkyTel's May 13, 2008 motion to quash have now been resolved. In particular, the Court has elected to proceed in accordance with one of the alternatives suggested in SkyTel's motion—namely, that the City be ordered to request and obtain the relevant text messages from SkyTel, thereby supplying the requisite "consent" for SkyTel's disclosure of these messages. (*See* SkyTel's Motion to Quash, Br. in Support at 7–8.) The Court trusts, then, that SkyTel no longer has any objection to the procedure established by the Court.

The Court remains extremely troubled, however, by a letter attached as an exhibit to SkyTel's motion. In this letter, dated March 12, 2008, an attorney who represents Defendant Kilpatrick in other matters (but not this case), Dan Webb, requests SkyTel's "immediate assurance that going forward it will not produce records regarding the contents of any text messages sent by or to [Defendant Kilpatrick] in response to **civil discovery**." (SkyTel's Motion, Ex. A, 3/12/2008 Letter at 2.) Yet, at the very time this letter was sent, Defendants (including Defendant Kilpatrick) had a motion pending before this Court seeking to quash subpoenas Plaintiff had served on SkyTel.

This apparent extra-judicial attempt to circumvent the usual (and obviously available) procedures for challenging a third-party subpoena is wholly inappropriate and will not be tolerated. Defendant Kilpatrick is a party to this case, and is represented by counsel who have proven fully capable of challenging **discovery** efforts that are believed to be inconsistent with or contrary to the applicable rules and law. Once this Court rules on such a challenge, it expects Defendant Kilpatrick (like any other party) to abide by this ruling. It is simply unacceptable that another attorney for Defendant Kilpatrick, who has not appeared in this case, would send a letter demanding SkyTel's "assurance" that it will not comply with a **discovery** request made and presently under challenge in this case, without any apparent regard for how this Court might rule on this pending challenge. The Court trusts and expects that no further such **communications** will come to light in this case, whether from Defendant Kilpatrick's attorneys or the representatives of any other party.

End of Document

1 Internet Law and Practice § 24:45

Internet Law and Practice
Database updated November 2015
Part V. General Legal Issues
Chapter 24. Free Speech on the Internet

John B. Morris, Jr., Julie M. Carpenter [*]

Correlation Table References

§ 24:45. Other significant First Amendment issues on the Internet—The right to speak anonymously—The standard when the anonymous/pseudonymous individuals are direct participants in the litigation

A common fact pattern in anonymous speech cases involves anonymous speakers sued as John Doe defendants. In such cases, a plaintiff typically sues the John Doe and subpoenas the John Doe's Internet service provider ("ISP") to obtain the speaker's identity. In situations where the ISP notifies the John Doe, the speaker often files a motion to quash the subpoena. Courts must then balance the plaintiff's right to prosecute the suit with the defendant's right to speak anonymously. A handful of courts of addressed this issue in recent years.

In *Columbia Ins. Co. v. Seescandy.com* and *In re Subpoena Duces Tecum to America Online*—both used to develop the *2TheMart.com* standard—the anonymous speakers were sued directly as John Does. In *Seescandy.com*, [1] the court articulated a very different four-part test. First, the plaintiff must be able to identify the missing person sufficiently for the court to determine that the party is a real person amenable to suit. Second, the plaintiff must describe his or her past attempts to unsuccessfully identify the defendant. Third, the plaintiff must show that the case would withstand a motion to dismiss (which both guarantees that the plaintiff has standing and prevents abuse of discovery to remove anonymity). Fourth, the plaintiff must file a discovery request to justify the need for the information. In that trademark case, the court held that because the plaintiff had met these requirements, and in particular because the court could compare the trademark used by the anonymous Web site operator and because the Web site operator had offered to sell the domain name to the trademark owner, discovery of the anonymous speaker was justified.

One year later, in *America Online, Inc.*, [2] an anonymous company sought discovery of five John Does who had made allegedly defamatory comments online concerning the company. AOL was unwilling to comply with the subpoena and filed a motion to quash. The Virginia Circuit Court recognized the protection for anonymous speech and required a party seeking to discovery the identity of an Internet speaker to show by pleadings or evidence that (1) the party seeking the information has a legitimate good faith basis to contend that it has been harmed by actionable conduct, and (2) the identity information is "centrally needed" to advance that claim.

In *Dendrite International, Inc. v. Doe No. 3*, [3] the appellate court affirmed the granddaddy of the Internet anonymous speech cases. Again, the allegations related to defamation. The New Jersey court established yet another four steps: (1) the plaintiff must undertake steps to notify the anonymous poster that he or she is the subject of a subpoena, such as posting a message of notification to the pertinent message board; (2) the plaintiff shall set forth the exact statements alleged to be actionable; (3) the plaintiff must set forth a prima facie case against the anonymous speaker; and (4) the court must balance the free speech rights against the strength of the prima facie case and the necessity for disclosure to allow the plaintiff to proceed.

In 2005, the Delaware Supreme Court issued a thorough and influential opinion that articulates a two-part test. [4] Doe v. Cahill involved an anonymous defendant who, writing under the moniker "Proud Citizen," criticized Cahill's work as a member of

the city council. The plaintiff obtained a court order requiring Proud Citizen's ISP to disclose his identity. Proud Citizen filed a motion to prevent disclosure, but the court denied it on the basis that the plaintiff had a good-faith basis to pursue the tort claim.

The Delaware Supreme Court, however, concluded that the good-faith standard was insufficient to protect an anonymous speaker's rights. The Delaware Supreme Court set forth a two-part balancing test, which requires a plaintiff seeking to learn to the identity of an anonymous speaker must (1) provide notice to the anonymous speaker that his or her identity is being sought and allow him or her a reasonable opportunity to respond; and (2) establish the prima facie elements of his or her claim sufficient to avoid summary judgment.[5]

The U.S. District Court for the District of Arizona has followed Cahill.[6] The U.S. District Court for the District of Massachusetts, however, has criticized the test.[7] The Arizona Court of Appeals has adopted the Cahill test but added a third prong; under the third prong, on balance, the parties' competing interests must favor disclosure.[8]

Cases involving allegations of trademark or copyright violations have been construed somewhat differently from those in which the content of the communication is essential to the cause of action. Indeed, a federal district court in Washington, D.C., originally construed the Digital Millennium Copyright Act to allow music copyright holders to subpoena the identity of music file-shares without filing a lawsuit. However, the D.C. Circuit Court of Appeals reversed that decision, and has held that such subpoenas are authorized only when the infringing material is stored on the ISP, thus forcing the music industry to file a complaint alleging copyright violations before it can obtain a subpoena to identify individual ISP users.[9]

Anonymous individuals posting commercial speech online may want to carefully consider their postings before uploading them to the Internet. The Ninth Circuit Court of Appeals in, *In re Anonymous Online Speakers*,[10] addressed the issue of First Amendment protections for online commercial speech. The case stemmed from longstanding commercial dispute between Quixtar, the successor company to "Amway"[11] and Signature Management Team ("Signature"), comprised of former independent business owners in Quixtar. Quixtar claimed that Signature engaged in an online smear campaign against their organization and attempted to lure away Quixtar members to Signature's competing business.

Quixtar asserted that several anonymous online postings and blogs directed at them were defamatory and disparaging. Inferring a link between Signature and the anonymous postings, Quixtar sought discovery of the identities of those individuals responsible for the blogs. Signature refused to identify the anonymous individuals. In resolving the discovery dispute, the district court applied the standard articulated in *Doe v. Cahill*[12] and ordered Signature to identify three of the five anonymous bloggers. Signature petitioned the Ninth Circuit for a writ of mandamus seeking a vacatur of the district court's order disclosing the names of the three anonymous individuals, and Quixtar counter-petitioned for a writ of mandamus to order Signature's disclosure of the remaining two anonymous bloggers.

In its analysis, the Ninth Circuit reiterated the fundamental differences between political, religious and literary speech as compared to commercial speech under First Amendment jurisprudence. Religious, political and literary speech are afforded the highest protections under the First Amendment, while commercial speech is not. In finding that Quixtar was entitled to disclosure of the remaining anonymous individuals, the court cited the Supreme Court's decision in Doe v. Reed,[13] in that "the nature of the speech should be a driving force in choosing a standard by which to balance the rights of anonymous speakers in discovery disputes." Accordingly, although Internet technology was constantly developing, there was no special First Amendment protection accorded commercial speech on the Internet.

As a result of the Ninth Circuit's decision, individuals engaged in anonymous online commercial speech should not automatically assume that their identity will remain protected. This would likely apply to anonymous individuals rating or commenting on a competitor's product or service.

A recent Virginia case addressed this issue. In *Hadeed Carpet Cleaning, Inc., v. Yelp,* [14] a rug cleaning company commenced a business defamation suit against seven anonymous reviewers from the website "Yelp." Hadeed subpoenaed Yelp to obtain the anonymous communicators' information, and Yelp opposed the subpoena. In affirming the lower court's decision upholding the validity of the subpoena, the Virginia Appeals Court noted that although the First Amendment protects anonymous speech it does not protect defamatory speech. Accordingly, if the Yelp reviews were unlawful, i.e., defamatory, then veil of anonymity may be pierced. Since the speech at issue was commercial in nature, the court found that the speech at issue was commercial speech, and the anonymous reviewers' "right to anonymity is subject to a substantial governmental interest in disclosure." [15] The Supreme Court of Virginia reversed, finding that the trial court lacked authority to enforce the subpoena against a non-party, nonresident website operator. The information sought was deemed to be beyond reach of trial court. [16]

Footnotes

* John B. Morris, Jr., is General Counsel at the Center for Democracy and Technology. Julie M. Carpenter is a partner in the Washington, D.C. office of Jenner & Block. The authors would like to thank Jodie Kelley, an original coauthor of this section, for her significant contribution to the discussions below. This section is dedicated to the memory of the authors' late partner, Bruce J. Ennis, who argued and won the Reno v. ACLU case in the Supreme Court and who set the standard for defending the First Amendment in the Internet context.

1 Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 51 U.S.P.Q.2d 1130 (N.D. Cal. 1999).

2 In re Subpoena Duces Tecum to America Online, Inc., 52 Va. Cir. 26, 2000 WL 1210372, *6 (2000), order rev'd on other grounds, 261 Va. 350, 542 S.E.2d 377, 29 Media L. Rep. (BNA) 1442 (2001).

3 Dendrite Intern., Inc. v. Doe No. 3, 342 N.J. Super. 134, 775 A.2d 756, 17 I.E.R. Cas. (BNA) 1336, 29 Media L. Rep. (BNA) 2265 (App. Div. 2001).

4 Doe v. Cahill, 884 A.2d 451, 460–61, 33 Media L. Rep. (BNA) 2441 (Del. 2005).

5 Best Western Intern., Inc. v. Doe, 2006 WL 2091695 (D. Ariz. 2006).

6 McMann v. Doe, 460 F. Supp. 2d 259, 35 Media L. Rep. (BNA) 1789 (D. Mass. 2006).

7 Mobilisa, Inc. v. Doe, 217 Ariz. 103, 170 P.3d 712, 36 Media L. Rep. (BNA) 2007 (Ct. App. Div. 1 2007).

8 Recording Industry Ass'n of America, Inc. v. Verizon Internet Services, Inc., 351 F.3d 1229, 69 U.S.P.Q.2d 1075 (D.C. Cir. 2003); see also, e.g., Guerrilla Girls, Inc. v. Kaz, 224 F.R.D. 571 (S.D. N.Y. 2004); Sony Music Entertainment Inc. v. Does 1-40, 326 F. Supp. 2d 556, 71 U.S.P.Q.2d 1661 (S.D. N.Y. 2004).

9 Doe v. Cahill, 884 A.2d 451, 33 Media L. Rep. (BNA) 2441 (Del. 2005).

10 In re Anonymous Online Speakers, 2011 WL 61635 (9th Cir. 2011)).

11 Amway was well-known for its "individual business owner" ("I.B.O.") model. Amway I.B.O.'s typically marketed the company's own branded products, including soaps, cosmetics and vitamins.

12 Doe v. Cahill, 884 A.2d 451, 33 Media L. Rep. (BNA) 2441 (Del. 2005). The Cahill standard sets a high bar as it requires the plaintiff to be able to survive a hypothetical summary judgment motion, in addition to giving, or attempting to give, the anonymous speaker notice before disclosing the speaker's identity. The high standard articulated by the court in Cahill was predicated on the fact that Cahill dealt specifically with political speech on the Internet. In the Quixtar matter, the Ninth Circuit disagreed with the district court's application of the Cahill standard to online commercial speech. Commercial speech on the Internet does not give rise to the same level of First Amendment protections afforded religious, political or literary speech. Accordingly, the court held that Quixtar's need for disclosure of the remaining anonymous individuals outweighed any First Amendment protections afforded Signature.

13 John Doe No. 1 v. Reed, 130 S. Ct. 2811, 2817–18, 177 L. Ed. 2d 493, 38 Media L. Rep. (BNA) 1833 (2010).

14 See., Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., 62 Va. App. 678, 752 S.E.2d 554, 42 Media L. Rep. (BNA) 1086 (2014), reversed and remanded, 770 S.E.2d 440 (Va. 2015).

15 Yelp, Inc. v. Hadeed Carpet Cleaning, Inc., 62 Va. App. 678, 692, 752 S.E.2d 554, 42 Media L. Rep. (BNA) 1086 (2014).

16 Yelp, Inc., 770 S.E.2d 440, 43 Media L. Rep. 1580 (Va. 2015).

End of Document