TOWNSHIP OF MANALAPAN, **Plaintiff,** **vs.** **STUART MOSKOVITZ, ESQ., JANE DOE and/or JOHN DOE, ESQ. I-V (these names being fictitious as their true identities are presently unknown) and XYZ Corporation, I-V (these names being fictitious as their true corporate identities are currently unknown)** **Defendants.**	SUPERIOR COURT OF NEW JERSEY LAW DIVISION MONMOUTH COUNTY DOCKET NO. MON-L-2893-07 **CIVIL ACTION** **(LEGAL MALPRACTICE)** **BRIEF OF ANONYMOUS SPEAKER "DATRUTHSQUAD" IN SUPPORT OF MOTION TO QUASH AND FOR A PROTECTIVE ORDER**

Frank L. Corrado, Esquire
BARRY, CORRADO, GRASSI & GIBSON, P.C.
2700 Pacific Avenue
Wildwood, NJ 08260
(609)729-1333 Fax:(609)522-4927

Matthew J. Zimmerman, Esquire (pro hac application pending)
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415-436-9333 x127
415-436-9993 Fax

Attorneys for Movant Datruthsquad.com a/k/a John Doe

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Court Rules

Other Authorities

I. INTRODUCTION

Pursuant to New Jersey Rule of Court 1:9-2A, an anonymous "blogger"[1] ("datruthsquad" or "Doe") who criticized Manalapan Township regarding its decision to file this underlying lawsuit hereby moves to quash the township's discovery subpoena of September 26, 2007, to Google, Inc., ("Google") which seeks the blogger's identity, communications, and "all other information associated with the account." Doe also moves for a protective order preventing the township from issuing any future discovery subpoenas to Google or any other individual or entity that might possess identity-related information, communications, or other records regarding the blogger.

Based on the township's previous filings and court statements, it is clear that the township has subpoenaed Doe's information not for any authorized discovery purpose but instead as part of an unrelated and unauthorized campaign to embarrass or otherwise outmaneuver the Defendant, Stuart Moskovitz. Moskovitz has repeatedly stated – under penalty of perjury – that he is not the blogger targeted by the Google subpoena. And despite repeated attempts to explain to the township's attorneys that the subpoena is obviously invalid and unenforceable, the township's attorneys have refused to withdraw the subpoena and have instead informed Doe's counsel that he could "address the issues via motion practice." Left with no other alternative, Doe is forced to come before this Court to protect his constitutionally and statutorily-protected right to anonymity.

II. PROCEDURAL HISTORY AND STATEMENT OF FACTS

On June 13, 2007, Manalapan Township filed a malpractice suit against its former attorney Stuart Moskovitz, alleging misconduct regarding the township's purchase of polluted land in 2005. See Complaint, Exhibit A to Zimmerman Certification. The allegations in the

[1] "A blog ... is a website where entries are written in chronological order and commonly displayed in reverse chronological order. … Many blogs provide commentary or news on a particular subject; others function as more personal online diaries. A typical blog combines text, images, and links to other blogs, web pages, and other media related to its topic. The ability for readers to leave comments in an interactive format is an important part of many blogs." "Blog." Wikipedia. November 27, 2007. <http://en.wikipedia.org/wiki/Blog>.

Complaint deal solely with conduct that took place during or before 2005 and center on whether Moskovitz breached his duty to the township concerning this property acquisition.

Before and after the filing of this lawsuit, the township's elected officials have been repeatedly criticized – about both the wisdom and the cost of the suit – in a variety of forums, including in the print media and on Internet blogs.[2]

One of the bloggers critical of township officials writes under the pseudonym "datruthsquad." In prior court filings and during oral argument before Judge Richard W. English, the township repeatedly alleged, without support, that datruthsquad[3] is actually Moskovitz. See Brief in Support of Plaintiff's Application to Vacate the Order to Show Cause (August 3, 2007), Exhibit B to Zimmerman Certification, at pp. 6, 7-9, 15-16, 41, 46-48; Certification of Daniel J. McCarthy (August 3, 2007), Exhibit C to Zimmerman Certification, at p.3. Moskovitz has repeatedly denied the allegation, both in court filings as well as during oral argument before Judge English. See Moskovitz Brief in Opposition to Plaintiff's Application (August 12, 2007), Exhibit E to Zimmerman Certification, at p.1; generally, Certification of Stuart Moskovitz (August 12, 2007), Exhibit F to Zimmerman Certification. See also Affidavit of Stuart Moskovitz (November 20, 2007), filed in support of this Motion.

Despite Moskovitz's repeated assertions that he is not the blogger in question – and more importantly, despite the irrelevance of the blogger's identity to this litigation – on September 26, 2007, the township issued a sweeping subpoena to Google asking for not only the identity of datruthsquad but for "any and all information" associated with the account for the entire existence of the blog, explicitly including but not limited to drafts, e-mails, and contact

---

[2] See, e.g., Mark Rosman, "Legal Case is Costing Town, But How Much?" News Transcript, September 26, 2007, <http://newstranscript.gmnews.com/news/2007/0926/editorials/042.html> (visited November 20, 2007), Exhibit I to Zimmerman Certification; screenshots of blog entries from http://datruthssquad.blogspot.com, originally submitted as Exhibits to the Certification of Daniel J. McCarthy (August 3, 2007), Exhibit D to Zimmerman Certification.

[3] For simplicity's sake, Doe will be referred to for the remainder of the brief using the masculine pronoun "him." This should not be taken as an admission as to his gender.

information. See Subpoena to Google (September 26, 2007), Exhibit G to Zimmerman Certification.

III. LEGAL STANDARD

Under New Jersey Rule of Court 1:9-2A, a court may, on motion, quash or modify a subpoena if compliance would be "unreasonable or oppressive." Similarly, R. 4:10-3 permits a target of discovery to seek a protective order shielding him from discovery that would result in "annoyance, embarrassment, oppression, or undue burden or expense." See also Kerr v. Able Sanitary & Env. Services, Inc., 295 N.J. Super. 147, 155 fn4 (App. Div. 1996) (motion to quash discovery subpoena is considered equivalent of motion for protective order).

IV. ARGUMENT

Four separate grounds exist to quash the township's September 26th subpoena to Google. First, the subpoena was not properly served on Google as required by New Jersey Rule of Court 1:9-4 and is therefore unenforceable. Second, the subpoena is not reasonably calculated to lead to any admissible evidence about any of the township's causes of action and therefore violates Rule 4:10-2. Third, the township fails to meet the heightened First Amendment requirements demanded of litigants seeking the identity of anonymous discovery targets. And fourth, the federal Stored Communications Act bars the township – a government entity – from obtaining the contents of electronic communications or customer records through the use of a discovery subpoena.

A. The Subpoena – Issued From New Jersey and Served on Google in California – Is Unenforceable.

The township's subpoena is unenforceable on several grounds, the most obvious being that the township failed to comply with the applicable standard for service: R. 1:9-4 requires litigants to issue civil subpoenas within the state's borders. In violation of that requirement, the township delivered the subpoena to Google at its corporate headquarters in Mountain View, California. See Subpoena and Postal Service certified mail receipt, Exhibits G and H to

Zimmerman Certification, respectively. The subpoena has no extra-territorial power and cannot be enforced.

An inability to directly serve non-parties in other states does not preclude the township from proceeding with legitimate discovery requests: jurisdictionally valid procedures exist which allow litigants to seek discovery in other states. For example, R. 4:11-5 permits a litigant to seek a commission authorizing a deposition to be taken outside the state. Correspondingly, the California Code of Civil Procedure permits out-of-state litigants who have obtained such a commission to depose witnesses in California. See California Code of Civil Procedure § 2029.010. See also, e.g., Fuller v. Doe, 151 Cal.App.4th 879, 884 (Cal. App. 2007) ("[P]laintiff commenced this proceeding under Code of Civil Procedure section 2029.010 by filing a declaration of counsel placing the Minnesota commission before the superior court and stating an intention to issue a subpoena duces tecum directing Yahoo to produce … information identifying, or aiding in discovering the identity of" an anonymous Internet user.).

Doe's counsel has repeatedly discussed this and other procedural and substantive failings with the township's counsel,[4] and the township's counsel has all but conceded that it failed to comply with the court rules.[5] However, the township has refused to withdraw its subpoena. Because it cannot be enforced, the township must not be allowed to continue to hold the threat of this invalid subpoena over Doe's head. Accordingly, the non-compliant subpoena[6] must be quashed.

---

[4] See Zimmerman Certification at ¶¶ 11-14.
[5] See Plaintiff letter of November 8, 2007, Exhibit K to Zimmerman Certification.
[6] Plaintiff also apparently failed to serve the Defendant with a copy of the subpoena, as required by R. 4:14-7(c). See Moskovitz Affidavit, filed with and in support of this Motion at ¶ 3. This failure is not merely a "procedural technicality":

> [The] evident intent [of R. 4:14-7(c)] is to prohibit the apparently proliferating documentary practice of some attorneys, wholly unauthorized, to obtain discovery from non-parties, unilaterally and without notice to other parties, by the simple expedient of issuing a subpoena. The design of this rule makes it clear that a 'discovery' subpoena may be issued only in connection with a scheduled deposition of the subpoenaed person, that all parties

B. The Information and Materials Sought by the Subpoena Are Not Likely to Lead to Admissible Evidence About Any of Plaintiff's Causes of Action.

A second reason that the subpoena must be quashed is that it is not likely to lead to the discovery of admissible evidence. Litigants may only obtain discovery "which is relevant to the subject matter involved in the pending action." R. 4:10-2. While discovery requests need not seek only admissible information, they must seek "information … reasonably calculated to lead to the discovery of admissible evidence" relevant to a "claim or defense of the party seeking discovery." Id. In spite of its broad scope, discovery "is not unbridled and not unlimited." Berrie v. Berrie, 188 N.J.Super. 274, 282 (App. Div. 1983). In no case should a party be permitted to launch a "fishing expedition" to establish otherwise factually unsupported allegations. See, e.g., Axelrod v. CBS Pubs., 185 N.J. Super. 359, 372 (App. Div. 1982).

The township's subpoena unequivocally fails this requirement.

1. Doe's Identity and the Other Subpoenaed Material Are Not Remotely Related to Plaintiff's Causes of Action.

Plaintiff alleges multiple causes of action that purportedly stem from violations of N.J.S.A. 2A:13-4: "If an attorney shall neglect or mismanage any cause in which he is employed, he shall be liable for all damages sustained by his client." To establish a claim under this statute, the township must show that:

(1) an attorney-client relationship existed between Plaintiff and Defendant,

(2) Defendant was obligated to fulfill a duty in furtherance of that relationship,

(3) Defendant failed to exercise reasonable care and prudence in connection to fulfilling that duty, and

---

> must be noticed of the issuance of such a subpoena and that all responses to the subpoena must be disclosed to all parties. It should, moreover, be interpreted and applied consistently with its intention of foreclosing unilateral discovery and giving adverse parties the opportunity to move to quash the subpoena or otherwise object to its compliance on the basis of privilege or other appropriate ground.

Pressler, Current N.J. Court Rules, Comment to R. 4:14-7(c) (Gann 2007) (emphasis added).

(4) Plaintiff sustained damages as a result.

See, e.g., St. Pius X House of Retreats, Salvatorian Fathers v. Diocese of Camden, 88 N.J. 571, 588 (1982) (attorney is obligated to exercise that degree of reasonable knowledge and skill that lawyers of ordinary ability and skill possess and exercise); Brach, Eichler, Rosenberg, Silver, Bernstein, Hammer & Gladstone, P.C. v. Ezekwo, 345 N.J. Super. 1, 12 (App. Div. 2001) ("To prevail on a claim of legal malpractice, a plaintiff must prove the existence of an attorney-client relationship that gives rise to a duty of care, the breach of such duty, and proximate causation.").

In its Complaint, the township claims Moskovitz negligently breached the following duties:

- "Duty to negotiate a contract that contained a clause that the Township's obligation to purchase the Dreyer property was contingent on obtaining a favorable PASI report or an equivalent environmental inspection which stated that the property was free of contamination and therefore fit for public use." Complaint, Exhibit A to Zimmerman Certification, at p.8.
- "Duty to protect the Township from purchasing property that is contaminated and therefore unfit for public use." Complaint, Exhibit A to Zimmerman Certification, at p.10.

Plaintiff also brings a "Third Count," again under N.J.S.A. 2A:13-4, alleging that unnamed John Does I-V and XYZ Corporations I-V "deviated from the accepted standards of practice by, among other things, failing to properly abandon the oil tanker [on] the Dreyer property in 1995."[7]

Doe takes no position on the merit of Plaintiff's claims. However, the information the township seeks in its subpoena is utterly irrelevant to those claims. Despite repeated prompting,

[7] The township's "Count Three" is deficient on its face and is thus difficult to discuss in any meaningful way. N.J.S.A. 2A:13-4 obligates attorneys to perform duties for their clients and imposes damages when that duty is breached. The specific allegations of Count Three center on the purported failures of anonymous (non-attorney) individuals and corporations to meet unarticulated (non-attorney) duties regarding proper waste disposal, yet Count Three is purportedly brought under the attorney malpractice statute, N.J.S.A. 2A:13-4.

the township has not made even the most cursory attempt to explain how piercing the anonymity of a blogger who wrote material critical of the township in 2007 could be "reasonably calculated to lead to the discovery of admissible evidence" relevant to claims that deal exclusively with events in 2005 and before. Rather, the township seeks to improperly interfere with the First Amendment rights of a pseudonymous critic for reasons separate from any legitimate need for discovery it possesses in this case.[8] See, e.g, Axelrod, 185 N.J.Super. at 372 (affirming Monmouth County Superior Court ruling) (identities of authors of self-help books not relevant to claims of fraud and breach of contract against publisher and discovery request amounted to "little more than a fishing expedition lacking a basis in fact.").[9]

2. Plaintiff Apparently Seeks the Subpoenaed Material In Order To Unmask or Intimidate a Vocal Critic.

Included for the Court's convenience is a chart that highlights every written statement counsel for the township has made about datruthsquad in this litigation.[10] The statements range from the baseless to apparent fabrications and indicate that Plaintiff seeks the subpoenaed information not to advance its claims but instead to improperly expose the identity of a vocal critic.

---

[8] The township has, in prior filings and during oral argument, expressed the unsupported hypothesis that Moskovitz is "datruthsquad" and that Moskovitz therefore violated the Court's prior Order preventing the Plaintiff and its agents from speaking publicly about this litigation (see Plaintiff's Brief in Support of Plaintiff's Application to Vacate the Order to Show Cause, Exhibit B to Zimmerman Certification, at p.9), as well as New Jersey Rule of Professional Conduct 4.2 (Id. at pp.41-49). Even if both were true, that would not permit the township to subpoena Google for information and material about Doe: R. 4:10-2 only permits discovery relevant to the township's claims or defenses. The Court and the New Jersey bar are perfectly capable of investigating any alleged violations of their orders or rules, and the township may not deputize itself through the discovery process to investigate such allegations on its own.

[9] See also, e.g., K.S. v. ABC Professional Corp., 330 N.J.Super. 288, 291-92 (App. Div. 2000) (deposition questions regarding defendants' prior consensual sexual relationships "not relevant to plaintiffs' hostile work place … since it cannot 'in reason ... prove or disprove any fact of consequence to the determination of the action' as it has been pleaded and prosecuted by plaintiffs."); Prashker v. New Jersey Title Guarantee & Trust Co., 135 N.J. Eq. 329, 332 (Ch. 1944) (requested discovery to inspect records denied as it "would not assist the complainants in determining" any issue before the court).

[10] See "Chart of Plaintiff's Written Court Statements Alleging That Defendant Moskovitz is Blogger 'Datruthsquad,'" attached Exhibit L to Zimmerman Certification.

The township's theory as to why it needs access to the subpoenaed information rests on a single unsupported assertion by its counsel, Daniel J. McCarthy:

> There are internet blog entries discussing Defendant's involvement in the Township's purchase of the Dreyer property and the ensuing issues with environmental problems and the Green Acres and the Monmouth County grants. The blog is entitled "daTruthSquad" and appears to have been written by Defendant.

McCarthy Certification, Exhibit C to Zimmerman Certification at ¶ 6 (emphasis added).

That "there are internet blog entries discussing Defendant's involvement in the township's purchase of the Dreyer property" is not in dispute. However, McCarthy has not explained the basis for his conclusion about the author of those entries, much less offered any evidence to support that conclusion. Instead, the township has pointed only to a pile of screenshots from the datruthsquad's blog which the township obliquely references and mischaracterizes in its papers. The township and its attorneys simply do not like what datruthsquad has to say and apparently want him to stop speaking.

For example, the township has asserted – without qualification – that "Defendant further uses the blog to accuse various Township officials of improper motives and repeatedly threaten the Township with a retaliatory lawsuit." Brief in Support of Plaintiff's Application to Vacate the Order to Show Cause, Exhibit B to Zimmerman Certification, at p.8. But the township fails to point to any evidence that Moskovitz is the blogger in question. "Datruthsquad" discusses Moskovitz – as well as every other subject of his posts (aside from self-references) – in the third person, and never asserts that he is Moskovitz. Moreover, the assertion that datruthsquad "repeatedly threaten[s] the Township with a retaliatory lawsuit" – once again besides being irrelevant to this litigation – appears to be a fabrication as it is unsupported by the screenshots the township has submitted to the Court.

The township makes the further remarkable statement: "… Defendant's recent communications coupled with his attacks on Township officials posted on his blog, 'daTruthSquad,' betray a mental instability and dangerous fixation on elected and appointed Township officials." Plaintiff's Application to Vacate the Order to Show Cause, Exhibit B to

Zimmerman Certification, at p.41. This statement shows a callous disregard for the protections of the First Amendment and makes clear that a desire to unmask anonymous critics lies at the core of the Township's legal strategy. The Court should not allow this abuse of the discovery process.

3. The Subpoena is Also Overbroad, and Compliance Would Unnecessarily Invade Doe's Privacy.

Even if Doe's identity were relevant to the Plaintiff's claims, the information sought by the subpoena is absurdly overbroad. Indeed, it appears designed to improperly pry into Doe's personal life as well as the lives of those who comment on his blog. In addition to Doe's name and contact information, the subpoena seeks the following information from Google:

- Doe's IP address
- Browser type and language
- "Any and all" information related to the datruthsquad blog
- Account settings and profile information
- Copies of the weblog posts and comments, including drafts
- Any and all e-mails received by Google from the account holder
- Any and all e-mails sent on Google's server by the account holder
- "The source of the information being posted on the blog"
- "Any other information associated with the account"

Given the broad scope of the subpoena, compliance might expose extensive personal information about Doe and the people who anonymously post comments on his blog. For example, Doe's IP address – the numerical identifier associated with an Internet connection – might allow the township to track Doe's online browsing habits, either directly (by searching publicly available Internet traffic logs) or by subpoenaing Doe's Internet service provider (ISP) for similarly invasive records. In addition, gaining access to the IP addresses of anonymous posters of comments (if Google retains such records) would allow the Township to continue it

campaign of chilling speech by subpoenaing other ISPs to identity subscribers who expressed views on datruthsquad's blog that are unpopular with the township.

The chilling effect that would result from the enforcement of such a subpoena cannot be overstated. Subpoenas seeking draft copies of "weblog posts" would give a litigant access to material that was, for whatever reason, never publicly released. And obtaining "all e-mails sent on Google's server by the account holder" and "any … information associated with the account" could be orders of magnitude more invasive than the other categories previously discussed. Furthermore, because Google's multiple services are linked and allow Google users to utilize them through a single account,[11] such a broad subpoena could give a litigant access to, among other things, messages from Google's Gmail e-mail service (www.gmail.com), financial records from Google Finance (finance.google.com), non-blog-related documents from Google Calendar (calendar.google.com) and Google Docs (docs.google.com), and records of videos viewed or posted at Google Video (video.google.com) and YouTube (www.youtube.com),[12] not to mention associational information from the collaborative features of these and other Google services. Moreover, access to Google "Web History" (www.google.com/psearch) information associated with a user's Google account would (if that feature has been activated by a user) give a litigant the opportunity to discover what web sites a user visits and what search terms he or she has entered into the Google search engine – an egregious invasion of privacy[13] that would certainly demand justification.

---

[11] From Google's online documentation: "What's a Google Account? It's a unified login system that gives you access to: Free Google services, including iGoogle, Gmail, Google Groups, Picassa, Web History, and more. … If you've used any of these services before you already have a Google Account. Your account username is simply the email address you used during the creation process." See "Google Accounts Help: What's a Google Account," <http://www.google.com/support/accounts/bin/answer.py?answer=27439&topic=10458>, Exhibit M to Zimmerman Certification.

[12] Records regarding video rentals and sales are subject to protections even stronger than those offered by the Stored Communications Act, discussed below. See, generally, the Video Privacy Protection Act, 18 USC 2710.

[13] For a recent discussion of the negative privacy implication of access to search data, see, e.g., Dawn Kawamoto and Elinor Mills, "AOL Apologizes for Release of User Search Data," CNet

None of this information is relevant to the township's claims. It is highly likely, therefore, that the real purpose of this vast subpoena is to harass and intimidate Doe, his readers, and those who post comments on his blog. The Court should not permit this improperly motivated "fishing expedition" to continue. See, e.g., Axelrod 185 N.J. Super. at 372; Korostynski v. Div. of Gaming Enforcement, 266 N.J.Super. 549, 559 (App. Div. 1993); Brock v. Public Service Elec. & Gas Co., 325 N.J.Super. 582, 587 (App. Div. 1999).

C. Plaintiff Cannot Meet the First Amendment Requirements Regarding Attempts to Unveil Anonymous Online Speakers.

Under the broad protections of the First Amendment and Article I, paragraph 6 of the New Jersey Constitution, speakers have not only a right to criticize public policies and governmental officials – speech that "may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials"[14] – but also the right to do so anonymously. As New Jersey courts have recognized for many years, in order to protect these rights, the First Amendment and the New Jersey Constitution require that those who seek to unmask vocal critics demonstrate a compelling need for such identity-related information before proceeding with discovery. See, e.g., Dendrite Int'l v. Doe No. 3, 342 N.J.Super. 134, 142 (App. Div. 2001) (discussed in detail below).

The Supreme Court has consistently defended the right to anonymous speech in a variety of contexts, noting that "[a]nonymity is a shield from the tyranny of the majority ... [that] exemplifies the purpose [of the First Amendment] to protect unpopular individuals from retaliation … at the hand of an intolerant society." McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (See also id. at 342: "[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment."). See also Gibson v. Florida Legislative Investigative Comm'n, 372 U.S. 539, 544 (1963) ("[I]t is ... clear that [free speech

---

News.com, August 7, 2007, at <http://www.news.com/2100-1030_3-6102793.html> (visited November 19, 2007).

[14] New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)

guarantees] ... encompass[] protection of privacy association …"); Talley v. California, 362 U.S. 60, 64 (1960) (finding a municipal ordinance requiring identification on hand-bills unconstitutional, and noting that "[a]nonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind.").

These fundamental rights enjoy the same protections whether their context is an anonymous political leaflet or an Internet blog. See Reno v. ACLU, 521 U.S. 844, 870 (1997) (there is "no basis for qualifying the level of First Amendment protection that should be applied to" the Internet). See also, e.g., Doe v. 2theMart.com, 140 F. Supp. 2d 1088, 1093 (W.D. Wash. 2001) ("The right to speak anonymously extends to speech via the Internet. Internet anonymity facilitates the rich, diverse, and far ranging exchange of ideas.").

1. Anonymous Speech Enjoys a Qualified Privilege Under the First Amendment Which Requires the Evaluation of Multiple Factors Prior to Subpoena Enforcement.

Because the First Amendment protects anonymous speech and association, efforts to use the power of the courts to pierce anonymity are subject to a qualified privilege. Courts must "be vigilant . . . [and] guard against undue hindrances to … the exchange of ideas." Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 192 (1999). This vigilant review "must be undertaken and analyzed on a case-by-case basis," where the court's "guiding principle is a result based on a meaningful analysis and a proper balancing of the equities and rights at issue." Dendrite Int'l v. Doe No. 3, 342 N.J.Super. 134, 142 (App. Div. 2001).

Just as in other cases in which litigants seek information that may be privileged, courts must consider the privilege before authorizing discovery. See, e.g., Sony Music Entm't Inc. v. Does 1-40, 326 F. Supp. 2d 556, 565 (S.D.N.Y. 2004), ("Against the backdrop of First Amendment protection for anonymous speech, courts have held that civil subpoenas seeking information regarding anonymous individuals raise First Amendment concerns."); Grandbouche v. Clancy, 825 F.2d 1463, 1466 (10th Cir. 1987), citing Silkwood v. Kerr-McGee Corp., 563 F.2d 433, 438 (10th Cir. 1977) ("[W]hen the subject of a discovery order claims a First Amendment privilege not to disclose certain information, the trial court must conduct a

balancing test before ordering disclosure."). "People who have committed no wrong should be able to participate online without fear that someone who wishes to harass or embarrass them can file a frivolous lawsuit and thereby gain the power of the court's order to discover their identity." Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999). See also 2theMart.com, 140 F. Supp. 2d at 1093 ("[D]iscovery requests seeking to identify anonymous Internet users must be subject to careful scrutiny by the courts.").

The constitutional privilege to remain anonymous is not absolute. Plaintiffs may properly seek information necessary to pursue reasonable and meritorious litigation. Seescandy.com, 185 F.R.D. at 578 (First Amendment does not protect anonymous Internet users from liability for tortious acts such as defamation); Doe v. Cahill, 884 A.2d 451, 456 (Del. 2005) ("Certain classes of speech, including defamatory and libelous speech, are entitled to no constitutional protection.").

However, litigants may not abuse the subpoena power to discover the identities of people who have simply made statements the litigants dislike. Accordingly, courts evaluating attempts to unmask anonymous speakers in cases similar to the one at hand have adopted standards that balance one person's right to speak anonymously with a litigant's legitimate need to pursue a claim. These courts have recognized that "setting the standard too low w[ould] chill potential posters from exercising their First Amendment right to speak anonymously," and have required plaintiffs to demonstrate their claims are valid and they have suffered a legally cognizable harm before the court will allow disclosure of the speaker's identity. Cahill, 884 A.2d at 457. See also Dendrite, 342 N.J. Super. at 141-42; Highfields Capital Mgmt. L.P. v. Doe, 385 F. Supp. 2d 969 (N.D. Cal. 2004).

In 2001, the appellate division in Dendrite Int'l v. Doe No. 3, 342 N.J. Super. 134 (App. Div. 2001) adopted a test for protecting anonymous speakers that has been followed not only in New Jersey but around the country.[15] Recognizing the Supreme Court's long support of the First

[15] See, e.g., Mobilisa, Inc. v. John Doe 1, No. 1 CA-CV 06-0521 at *14-17 (Ariz. Ct. App. November 27, 2007) (attached as Exhibit O to Zimmerman Certification); Greenbaum v. Google, Inc., --- N.Y.S.2d ----, 2007 WL 3197518 at *2 (N.Y.Sup. 2007) (attached as Exhibit N to

Amendment right to speak anonymously, the court underscored the ongoing need for vigorous protection of that right:

> The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. Whatever the motivation may be, at least in the field of literary endeavor, the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.

Id. at 148. Moreover, the Court also based its holding on the New Jersey Constitution's cognate free speech guarantees:

> Our Supreme Court has held that the rights attendant to this provision [N.J. Const., art. I, par. 6] are "the most substantial in our constitutional scheme." ... In fact, "the reach of our constitutional provision [is] affirmative. Precedent, text, structure, and history all compel the conclusion that the New Jersey Constitution's right of free speech is broader than the right against governmental abridgement of speech found in the First Amendment."

Id. at 149 (internal citations omitted).

Taking these protections into account, the court in Dendrite described "the appropriate procedures to be followed and the standards to be applied by courts in evaluating applications for discovery of the identity of anonymous users of Internet Service Provider (ISP) message boards" (Id. at 140) as follows:

(1) make reasonable efforts to notify the accused Internet user of the pendency of the identification proceeding and explain how to present a defense;

(2) quote verbatim the allegedly actionable online speech;

(3) allege all elements of the cause of action;

(4) present evidence supporting the claim of violation; and,

Zimmerman Certification; Doe v. Cahill, 884 A.2d at 459-60) (applying a modified Dendrite test); Highfields Capital Mgmt. L.P. v. Doe, 385 F. Supp. 2d 969, 974-76 (N.D. Cal. 2005).

(5) "[f]inally, assuming the court concludes that the plaintiff has presented a prima facie cause of action, the court must balance the defendant's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous defendant's identity to allow the plaintiff to properly proceed."

Id. at 141-42 .

The Dendrite test concerns party discovery and, as such, recognizes a minimum First Amendment standard. If anything, First Amendment protections for non-parties during discovery must be higher than those for parties to ensure that non-litigants are not embroiled in costly litigation to which they may only be tangentially related. See, e.g., 2theMart.com, 140 F. Supp. 2d at 1095 ("The standard for disclosing the identity of a non-party witness must be higher than that articulated in [party discovery cases]. When the anonymous Internet user is not a party to the case, the litigation can go forward without the disclosure of their identity. Therefore, non-party disclosure is only appropriate in the exceptional case where the compelling need for the discovery sought outweighs the First Amendment rights of the anonymous speaker."); Theofel v. Farey-Jones, 359 F.3d 1066, 1074-75 (9th Cir. 2004) ("Fighting a subpoena in court is not cheap, and many may be cowed into compliance with even overbroad subpoenas, especially if they are not represented by counsel or have no personal interest at stake.").

The Western District of Washington's opinion in Doe v. 2theMart.com, supra, 140 F. Supp. 2d at 1095 – decided within two months of Dendrite – remains the clearest guide to ensuring that non-party anonymous online speakers receive the protection the First Amendment demands. The 2theMart court's non-party test consisted of four additional First Amendment factors:

(1) whether the subpoena seeking the information was issued in good faith and not for any improper purpose,

(2) whether the information sought relates to a core claim or defense,

(3) whether the identifying information is directly and materially relevant to that claim or defense, and

(4) whether information sufficient to establish or to disprove that claim or defense is unavailable from any other source.

As the 2theMart court noted, its test "provides a flexible framework for balancing the First Amendment rights of anonymous speakers with the right of civil litigants to protect their interests through the litigation discovery process." While the Court was mindful of the "high burden" it imposed on litigants, "[t]he First Amendment requires us to be vigilant in making [these] judgments, to guard against undue hindrances to political conversations and the exchange of ideas." Id (citing Buckley v. American Constitutional Law Found., 525 U.S. 182, 192 (1999)).

The 2theMart holding is consistent with and complimentary to the Dendrite test for unmasking anonymous online speakers. The Dendrite court, for example, explicitly approved of the approaches of other courts in similar circumstances that required litigants to demonstrate that the subpoena was issued in good faith and that the subpoenaed identity information is "centrally needed to advance" the claim. See Dendrite, 342 N.J. Super. at 157-58. As applying both the Dendrite and 2theMart tests to discovery requests seeking the identity of non-parties would more appropriately protect the First Amendment interests of non-parties yet still permit legitimate requests to be fulfilled, the Court should apply both tests here.

2. Plaintiff's Discovery Subpoena Cannot Survive the Scrutiny Required By the First Amendment.

The Court need not consider steps (1) and (2) of the Dendrite test; the first has been met and the second (necessary for evaluating defamation claims) is not applicable in this non-defamation context. Similarly, Doe does not contest (as required by steps (3) and (4)) that Plaintiff has properly alleged all elements of Counts One and Two in its Complaint, or that it has submitted evidence establishing a prima facie case.[16]

[16] Count Three (as discussed above at pg. 6), however, is deficient and cannot serve as an independent basis for authorizing discovery.

However, the township cannot prevail in an evaluation of the fifth Dendrite factor: balancing the speaker's First Amendment right of anonymous free speech against the strength of the prima facie case presented and the necessity for the disclosure of the anonymous speaker's identity to allow the plaintiff to properly proceed. 342 N.J. Super at 142. First, the case can proceed without discovery from Doe. There is no reason to believe that Doe's identity or personal records and e-mails will affect the strength of the township's prima facie case. Second, Doe's First Amendment right to anonymous speech will be lost if the subpoena is enforced. The township has offered no basis to override these constitutionally-protected rights.

Moreover, as the township cannot satisfy the Dendrite factors, it similarly cannot satisfy those set forth in 2theMart. Given its lack of relevance and overbreadth, as well as the township's fixation on Doe's status as a critic and the fact that Moskovitz has repeatedly stated to the Court (as he has done again in support of this Motion) that he is not "datruthsquad," the subpoena was not issued in good faith. The requested discovery does not relate to any of Plaintiff's claims. And critically, Plaintiff has already alleged and presented evidence to support the core issues relevant to its claims, so it is capable of pursuing its claims without invading the personal lives of non-parties who disagree with its policy choices.

The First Amendment requires a litigant to show that it has a non-frivolous need to pursue discovery when free speech rights would be harmed as a result. Plaintiff cannot meet this standard. The Court should quash the subpoena and issue a protective order preventing Plaintiff from issuing the same or similar subpoenas.

D. Plaintiff Is Barred By the Stored Communications Act From Obtaining the Information It Seeks Through the Use of a Discovery Subpoena.

Apart from the other procedural and Constitutional flaws in its subpoena, the federal Stored Communications Act ("SCA")[17] prevents the township from using discovery subpoenas to obtain the information it seeks. The SCA, passed as part of the Electronic Communications Privacy Act of 1986, prohibits unauthorized access of electronic communications stored with

[17] 18 USC §§ 2701-11.

online services. It also limits the ability of providers of communications and computing services to disclose communications and records regarding users of such services. "The Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents, … the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic communications facility." Theofel, 359 F.3d at 1072-73. While the township may be able to use other procedural devices to obtain access to information relevant to its case, the SCA flatly bans it from using a discovery subpoena to gain access to the kinds of information and materials it seeks from Google.

1. The SCA Prohibits the Disclosure of the Contents of Communications or Customer Records and Related Information.

The SCA prohibits, subject to specific statutory exceptions, the disclosure of certain types of electronic information by two categories of service providers: providers of "electronic communication services"[18] ("ECS providers") and providers of "remote computing services"[19]

[18] "'[E]lectronic communication service' means any service which provides to users thereof the ability to send or receive wire or electronic communications …" 18 USC § 2510(15). The legislative history and case law indicate that the key issue in determining whether a company provides ECS is that company's role in providing the ability to send or receive the precise communication at issue, regardless of the company's primary business. See H.R. Rep. No. 99-647, at 65 (1986). "[T]elephone companies and electronic mail companies," for example, generally act as providers of electronic communication services (see S. Rep. No. 99-541 (1986)), but so can cities (see Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city that provided pager service to its police officers can be an ECS provider)) airlines (see United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system accessed through separate computer terminals can be an ECS provider)), and electronic bulletin board systems (see United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003), cert. denied, 538 U.S. 1051 (2003)), depending on the technological capabilities that they offer.

[19] "[T]he term 'remote computing service' means the provision to the public of computer storage or processing services by means of an electronic communications system …" 18 USC § 2711(2). Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. See S. Rep. No. 99-541, at 10-11 (1986), reprinted in 1986 U.S.C.C.A.N 3555, 3568. For example, a service provider that processes data in a time-sharing arrangement provides an RCS. See H.R. Rep. No. 99-647, at 23 (1986). So can

("RCS providers"). See 18 USC § 2702(a)(1) and 2702(a)(2), respectively. While prohibitions and exceptions vary somewhat depending on ECS or RCS provider characterization, the protections applied to each type of provider are indistinguishable for purposes of this discussion. Google qualifies as an ECS[20] and/or an RCS[21] provider for each category of information sought by Plaintiff's subpoena, and no statutory exception exists that would permit the lawful disclosure of that information by Google to the Plaintiff,[22] even through the use of an otherwise valid discovery subpoena.

Subsection 2702(a)(1) prohibits the disclosure of the "contents" of communications by ECS providers:

> [A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service …

Similarly, subsection 2702(a)(2) prohibits the disclosure of the "contents" of customers' electronics communications by RCS providers:

> [A] person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service …[23]

---

operators of electronic bulletin board systems. See Steve Jackson Games, Inc. v. United States Secret Service, 816 F. Supp. 432, 443 (W.D. Tex. 1993).

[20] Google, to the extent (through its Gmail e-mail service and otherwise) that it "provides to users thereof the ability to send or receive … electronic communications" that are responsive to Plaintiff's open-ended subpoena, qualifies as an ECS provider.

[21] Google qualifies as an RCS provider for much of the information sought by Plaintiff as the subpoena seeks information and materials in connection to Doe's use of Blogspot, a service with which users can create blogs and allow comments by third parties. See, infra, Steve Jackson Games, Inc.

[22] See "Chart Applying Restrictions of the Stored Communications Act to the Township's Subpoena to Google of September 26, 2007," attached as Exhibit P to the Zimmerman Certification.

[23] 18 USC § 2702 (a)(2 (A) and (B) further clarify the restrictions articulated in subsection 2702 (a)(2): the type of RCS customer communications whose disclosure is prohibited under subsection 2702(a)(2) are those (as in this case) that are made "(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service; (B) solely for the purpose of providing storage or computer processing services to

Beyond the blanket restrictions on the disclosure of communications content as identified in subsections 2702(a)(1) and (2), subsection (a)(3) explicitly prevents, unless an appropriate exception applies, the disclosure to the government by an ECS or RCS provider of a customer "record" or "other information pertaining to" a subscriber or customer:

> [A] provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

The township's subpoena seeks precisely this kind of information and is therefore not permitted under 18 USC § 2702. While sections 2702 and 2703 offer several exceptions to the general rules preventing disclosure of the material covered by the SCA, none apply here.[24]

---

such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing …"

[24] Subsection 2702(b) and (c), for example, specify when providers are permitted to voluntarily disclose information in their possession and to whom. Subsection 2702(b) identifies eight exceptions to the general rule preventing the disclosure of the content of communications. Similarly, subsection 2702(c) offers six exceptions to the general rule preventing the disclosure of customer "records" and related information – i.e. account information that does not amount to the contents of communications – such as the customer's name, address, contact information, and IP address. None are applicable here. Section 2703 offers other exceptions to the general rule preventing disclosure, this time identifying when covered providers are required to disclose customer communications or records. Once again, this section provides no legal avenue for Plaintiff to force Google to disclose the subpoenaed information in question through the use of a pre-trial civil subpoena. Subsection 2703(b), for example, only permits a governmental entity to require the disclosure of the contents of communications in their possession through the use of a criminal warrant (subsection 2703(b)(1)(A)); administrative subpoena, grand jury subpoena, or trial subpoena (subsection 2703(b)(1)(B)(i)); or court order issued in connection with a criminal investigation (subsection 2703(d)). Discovery subpoenas (as discussed in more detail below) may not be used. Similarly, subsection 2703(c) only permits a governmental entity to require the disclosure of customer (non-content) records and information related to a customer if it obtains a criminal warrant (subsection 2703(c)(1)(A)); administrative subpoena, grand jury subpoena, or trial subpoena (subsection 2703(c)(2)); court order issued in connection with a criminal investigation (subsection 2703(d)); or the consent of the customer (subsection 2703(c)(1)(C)).

2. The SCA Does Not Permit the Use of Discovery Subpoenas to Obtain Contents of Communications or Customer Records and Related Information.

While subsections 2703(b) and (c) affirmatively permit governmental entities to obtain certain types of information through the use of "administrative subpoenas," "grand jury subpoenas," or "trial subpoenas," this exception does not permit the use of discovery subpoenas. Subsection 2702(a) enacts a blanket prohibition on disclosure – providers "shall not knowingly divulge to any person" the contents of communications or records or other information pertaining to a subscriber or customer – unless they meet the strict and specifically articulated exceptions. The language of the statute is clear and must be given effect. See, e.g., Lamie v. U.S. Trustee, 540 U.S. 526, 534 (2004) ("when the statute's language is plain, the sole function of the courts – at least where the disposition required by the text is not absurd – is to enforce it according to its terms [citations omitted].").

The few courts to examine this aspect of the SCA have come to this conclusion. In FTC v. Netscape Communications Corp., 196 F.R.D. 559 (N.D. Cal. 2000), the Northern District of California ruled on a motion to compel by the Federal Trade Commission – a government entity – which was seeking to enforce a discovery subpoena seeking identity-related information about users of Netscape's e-mail service. The court held that the SCA's authorization for the disclosure of certain information to governmental entities under a trial subpoena did not permit disclosure under a civil discovery subpoena. Noting the well-recognized distinctions between trial and discovery subpoenas, the court found "no reason ... to believe that Congress could not have specifically included discovery subpoenas in the statute had it meant to." Id. at 561.

Similarly, in O'Grady v. Superior Court, 139 Cal.App.4th 1423 (Cal. App. 2006), a case in which a (non-government) litigant issued civil subpoenas to an ECS operator seeking the identity and e-mail communications of an online journalist who allegedly was in communication with a Doe defendant, the California Court of Appeals found that discovery subpoenas could not be used to obtain the material sought: "Few cases have provided a more appropriate occasion to apply the maxim expressio unius exclusio alterius est, under which the enumeration of things to

which a statute applies is presumed to exclude things not mentioned." Id. at 1443. "Since the Act makes no exception for civil discovery and no repugnancy has been shown between a denial of such discovery and congressional intent or purpose, the Act must be applied, in accordance with its plain terms, to render unenforceable the [discovery] subpoenas seeking to compel [providers] to disclose the contents of emails stored on their facilities." Id. at 1447 (holding that a protective order must issue to protect against such subpoenas).

Accordingly, even if the township's discovery subpoena had any merit, the SCA renders it – and any future discovery subpoenas similarly seeking materials covered by the Act – unenforceable.

3. Litigants – and Their Attorneys – Who Use Obviously Invalid Subpoenas to Access Communications In Electronic Storage Can Incur Civil and Criminal Liability.

In addition to the restrictions on Google imposed by sections 2702 and 2703, which alone are sufficient to support Doe's Motion, the SCA contains additional provisions that underscore the impropriety of these subpoenas and reinforce the need to quash the subpoenas and grant a protective order.

Subsection 2701(a) makes it a criminal offense to "intentionally access[] without authorization a facility through which an electronic communication service is provided; or intentionally exceeds an authorization to access that facility; and thereby obtains … access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section."[25] In addition, 18 USC § 2707 allows "any person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind" to bring a suit to recover damages as well as potential punitive damages and attorneys fees. 18 USC § 2707(a)-(c).

[25] Subsection 2701(b) provides that the punishment for such an offense is "(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and (B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section."

Compliance with the township's overbroad and irrelevant subpoena may constitute "intentional access without authorization" under subsection 2701(a).[26] The Ninth Circuit, addressing a strikingly similar set of facts, recently came to this same conclusion. In Theofel, supra, the court considered whether the defendants had violated subsection 2701(a) when they used a "patently unlawful" subpoena to gain access to e-mail stored by plaintiffs' ISP. The court found that they had.

In Theofel, the defendants during the course of discovery regarding pending commercial litigation issued a subpoena to plaintiffs' ISP seeking "[a]ll copies of e-mails sent or received by anyone" at the defendants' business, with no limitation as to time or scope." 359 F.3d at 1071. As the court pointed out, given the applicable duty under the discovery rules to "take reasonable steps to avoid imposing undue burden or expense" (see F.R.C.P. 45(c)(1)), "[o]ne might have thought, then, that the subpoena would request only e-mail related to the subject matter of the litigation, or maybe messages sent during some relevant time period, or in the very least those sent to or from employees in some way connected to the litigation." 359 F.3d at 1071. Because defendants did not take such rudimentary steps, the magistrate judge "roasted [defendants] for their conduct, finding that the 'subpoena, on its face, was massively overbroad' and 'patently unlawful,' that it 'transparently and egregiously' violated the Federal Rules, and that the defendants 'acted in bad faith' and showed 'at least gross negligence in the crafting of the subpoena.'" Id. at 1071-72. The magistrate granted the motion to quash and the accompanying motion for sanctions, which plaintiffs did not appeal.

The Theofel court found that such conduct "vitiate[d]" the "consent" of the ISP that turned over material in response to the subpoena, rendering defendants' access to materials held

[26] Once again, Plaintiff's subpoena sought generally "all information related to the internet blog, "daTruthSquad" as well as specifically "any and all e-mails sent on Google's server by the account holder …," both of which encompass "electronic communications while in electronic storage" under subsection 2701(a). See, e.g, Theofel, 359 F.3d at 1075 (e-mail messages saved on a server after delivery are "electronic communications in electronic storage" under subsection 2701(a)); H.R. Rep. No. 99-647, at 64-65 (1986) (noting that opened e-mail stored on a server are protected under provisions relating to remote computing services).

by the ISP "unauthorized" under subsection 2701(a). Id. at 1073. Analogizing to principles of common law trespass and noting the purpose of the SCA – to "protect[] individuals' privacy and proprietary interests" – the court noted that permission to obtain access to private areas or materials obtained deceptively renders that "permission" null and void. Id. at 1072-73. While a defendant is ordinarily not liable for trespass if a party authorizes his entry, "an overt manifestation of assent or willingness would not be effective … if the defendant knew, or probably if he ought to have known in the exercise of reasonable care, that the plaintiff was mistaken as to the nature of the invasion." Id. at 1073 (quoting Prosser and Keeton § 18 at 119).

An obviously invalid subpoena vitiates valid consent and voids any "authorization" obtained as a result of its issuance. See Theofel, 359 F.3d at 1073-74 ("Defendants had at least constructive knowledge of the subpoena's invalidity. It was not merely technically deficient, nor a borderline case over which legal minds might disagree. It 'transparently and egregiously' violated the Federal Rules, and defendants acted in bad faith and with gross negligence in drafting and deploying it.").[27]

Congress has not only prohibited ECS and RCS from voluntarily disclosing the requested information pursuant to a civil discovery subpoena (section 2702) and enacted strict standards for disclosure to the government (section 2703). It has also set forth severe penalties for unauthorized access (section 2701). Accordingly, not only must this subpoena be quashed, but since no other subpoena could properly issue, this Court should also enter a protective order.

V. CONCLUSION

Instead of narrowly tailoring discovery requests to pursue specific, identifiable, viable claims, Plaintiff has asked this Court to endorse a fishing expedition aimed instead at exposing

[27] Other courts have interpreted similar federal wiretapping and computer crime statutes and also held that "authorization," obtained fraudulently or by mistake, is not valid. See, e.g., EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) (holding access might be "unauthorized" under the Computer Fraud and Abuse Act if it is "not in line with the reasonable expectations" of the party granting permission); United States v. Morris, 928 F.2d 504, 510 (2nd Cir. 1991) (holding access unauthorized where it is not "in any way related to [the system's] intended function").

its anonymous critics. The Court should decline to do so. For the foregoing reasons, Doe respectfully asks the Court to quash the September 26th subpoena and grant the motion for a protective order to prevent future invalid discovery attempts.

11/28/07

Respectfully submitted,

By _____

Frank L. Corrado, Esquire
Barry Corrado Grassi & Gibson, P.C.
2700 Pacific Avenue
Wildwood, NJ 08260
609-729-1333

Matthew J. Zimmerman (pro hac application pending)
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
415-436-9333 x127
415-436-9993 Fax

Attorneys for Movant