No. B242700

COURT OF APPEAL OF THE STATE OF CALIFORNIA

SECOND APPELLATE DISTRICT, DIVISION ONE

IN MATTER OF SUBPOENA IN UMG RECORDINGS

Plaintiff and Appellant,

v.

DIGITAL MUSIC NEWS LLC,

Defendant and Appellant.

Appeal from An Order Enforcing a Subpoena Emanating from Another State
Of the Superior Court, County of Los Angeles, No. SS022099
Hon. Richard Stone, Judge

APPELLANT'S OPENING BRIEF

Paul Alan Levy, Pro Hac Vice
PUBLIC CITIZEN LITIGATION GROUP
1600 20th Street, N.W.
Washington, D.C. 20009
202.588.7725
plevy@citizen.org

*Charles A. Bird (SBN 056566)
McKENNA LONG & ALDRIDGE LLP
600 West Broadway, Suite 2600
San Diego, California 92101-3372
619.236.1414
cbird@mckennalong.com

Attorneys for Digital Music News LLC

TO BE FILED IN THE COURT OF APPEAL

APP-008

COURT OF APPEAL, Second APPELLATE DISTRICT, DIVISION 1	Court of Appeal Case Number: B243623
ATTORNEY OR PARTY WITHOUT ATTORNEY (Name, State Bar number, and address): Paul Alan Levy, Public Citizen Litigation Group, 1600 20th Street NW, Washington, D.C. 20009 TELEPHONE NO.: 202-588-7725 FAX NO. (Optional): E-MAIL ADDRESS (Optional): plevy@citizen.org ATTORNEY FOR (Name): Digital Music News LLC	Superior Court Case Number: SS022099 FOR COURT USE ONLY
APPELLANT/PETITIONER: UMG Recordings RESPONDENT/REAL PARTY IN INTEREST: Escape Media Group	

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

(Check one): ☑ INITIAL CERTIFICATE ☐ SUPPLEMENTAL CERTIFICATE

Notice: Please read rules 8.208 and 8.488 before completing this form. You may use this form for the initial certificate in an appeal when you file your brief or a prebriefing motion, application, or opposition to such a motion or application in the Court of Appeal, and when you file a petition for an extraordinary writ. You may also use this form as a supplemental certificate when you learn of changed or additional information that must be disclosed.

1. This form is being submitted on behalf of the following party (*name*): Digital Music News LLC

2. a. ☐ There are no interested entities or persons that must be listed in this certificate under rule 8.208.

   b. ☑ Interested entities or persons required to be listed under rule 8.208 are as follows:

Full name of interested entity or person	Nature of interest (Explain):
(1) Paul Resnikoff	100% owner
(2)	
(3)	
(4)	
(5)	

☐ Continued on attachment 2.

The undersigned certifies that the above-listed persons or entities (corporations, partnerships, firms, or any other association, but not including government entities or their agencies) have either (1) an ownership interest of 10 percent or more in the party if it is an entity; or (2) a financial or other interest in the outcome of the proceeding that the justices should consider in determining whether to disqualify themselves, as defined in rule 8.208(e)(2).

Date: September 11, 2012

/s/ Paul Alan Levy
(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY)

Form Approved for Optional Use
Judicial Council of California
APP-008 [Rev. January 1, 2009]

CERTIFICATE OF INTERESTED ENTITIES OR PERSONS

Cal. Rules of Court, rules 8.208, 8.488
www.courtinfo.ca.gov

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

CONSTITUTIONAL PROVISIONS

STATUTES

RULES

OTHER AUTHORITIES

INTRODUCTION

Digital Music News (Digital) is an online newsletter and blog about the digital music industry. (2 AA 277 ¶ 2.) As a journalistic enterprise, Digital has covered the public controversy about Grooveshark, a streaming music business of Escape Media Group (Escape). (See, e.g., 2 AA 278-279 ¶¶ 9-13.) UMG Recordings, Inc. (UMG) sued Escape in New York state court for Grooveshark's alleged infringement of state-law copyright protections. (1 AA 106-116.)

Escape served a discovery subpoena on Digital in connection with the New York state court action. Escape sought information that might reveal the identity of an Internet user who criticized Escape on Digital's blog. Any identifying data that existed, however, had been deleted in the ordinary course of Escape's business months before service of the subpoena, and the computer drives where the data was originally stored had been repeatedly overwritten in normal business operations.

This appeal arises from a pair of orders issued in favor of Escape, compelling journalist Digital to freeze its computer systems for six weeks. The purpose of the shut-down was to conduct a forensic examination for vestiges of the blog poster's identity. The superior court neither required Escape to show a basis to believe identifying data remained nor applied the test commonly used in other jurisdictions to decide whether to conduct such a forensic examination of a witness's electronics. Initially, the court compelled journalist Digital to freeze computer operations while Escape considered whether it wanted

to pay for the forensic examination. Ultimately, the court ordered a limited form of copying and forensic examination. Although the copying has occurred, the examination has been stayed by this court's writ of supersedeas.

Implicit in all the superior court's orders is a presumption that all Internet journalists and hosting companies must adopt business methods that preserve identity data of anonymous blog posters—or face shut-down for others' litigation discovery. This presumption lacks any legal support; the court's orders threaten the operation of every journalistic and hosting company in California.

Further, to the extent courts may ever order forensic examinations of electronics when the discovery target is only a witness, the superior court failed to articulate an acceptable standard for the intrusion. That information "might" exist is too low a standard.

Finally, the superior court failed to give sufficient weight to the First Amendment protection for anonymous speech. Nothing about the posts on Digital's blog justified court orders aimed at penetrating the poster's anonymity.

APPELLATE JURISDICTION

On June 18, 2012, the trial court ordered Digital to comply with a subpoena issued in aid of an out-of-state proceeding to which is it not a party. (2 AA 459.) Digital appealed that order on July 6, 2012. (2 AA 469.) The court issued a supplemental order compelling Digital to preserve its virtual servers and to allow them to be subjected to forensic examination on July 26, 2012.

(2 AA 462.) Digital appealed that order on August 27, 2012. (2 AA 470.) Although mandamus is the normal route for appellate review of discovery orders, review is by appeal when the subpoena is in aid of an out of state proceeding. (*H.B. Fuller Co. v. Doe* (2007) 151 Cal.App.4th 879, 885-886; *City of Woodlake v Tulare County Grand Jury* (2011) 197 Cal.App.4th 1293, 1298; *Dana Point Safe Harbor Collective v. Superior Court* (2010) 51 Cal.4th 1, 13, fn. 8.)

STATEMENT OF FACTS

A. Escape's Copyright Disputes with UMG

This subpoena proceeding arises from a lawsuit brought by UMG against Escape over Escape's operation of a music streaming service called Grooveshark. Escape, which has license agreements with several recording companies, has often faced litigation over allegations that it hosts music in excess of its license rights and that it has not lived up to its royalty agreements. (See, e.g., *Capitol Records v. Escape Media Group*, No. 151440/2012 (N.Y.); *EMI Entertainment World v. Escape Media Group*, No. 650013/2012 (N.Y.); *Yesh Music v. Escape Media Group*, 1:12-cv-00290-JBW-VVP (E.D.N.Y.).) Here, UMG alleges in a New York state court that Grooveshark is infringing its common law copyrights in many pre-1972 sound recordings. Because sound recordings that old are not subject to copyright under federal law, common law enforcement is not preempted by federal law. (1 AA 106-116.)

In a parallel case pending in the United States District Court for the Southern District of New York, UMG charges

Escape with infringing recordings that *are* subject to federal copyright protection. (1 AA 141-151.) In defending against both cases, Escape has claimed immunity under the Digital Millennium Copyright Act (DMCA), which immunizes online hosts from liability for infringement under federal law so long as they promptly remove copyrighted recordings posted on their servers upon receiving notice that the posting infringes copyright. (1 AA 125.)

B. Digital Is an Internet Journalist that Covers Businesses Like Escape and UMG and Hosts Blogger Comments

Digital is an online newsletter and blog about the digital music industry that is posted online at www.digitalmusicnews.com. (2 AA 277 ¶ 2.) The blog is aimed at an audience of executives in the music industry as well as technology companies; its readers include decision-makers from every segment of the business, spanning major labels to artists to garage start-ups. (*Ibid.*) Paul Resnikoff (Resnikoff) is Digital's owner and main writer; technical matters are handled by Steve Hindle (Hindle). (*Id.* at p. 278 ¶ 3.) The blog strives to provide an independent voice on issues arising in the industry that it covers. Digital has covered the public controversy about Grooveshark, as well the litigation brought against it. See, e.g., http://digitalmusicnews.com/stories/ 100711grooveshark; 2 AA 278-279 ¶¶ 9-13.)

In addition to carrying Resnikoff's articles, Digital allows readers to post comments. Readers need not register to post comments; anybody who wants to comment need only choose the

name under which the comment will be posted and complete a "CAPTCHA" box to ensure that a real person is posting the comment. (*Id.* at p. 278 ¶ 4.) Resnikoff reads comments posted on Digital, and often responds to the commenters, always posting under his own name. (*Id.*, ¶ 6.) Resnikoff scrutinizes the comments for story ideas and for information that he can further investigate to continue reporting on the matter covered by the story in question. (*Ibid.*) Although he recognizes that anonymous comments are not always reliable, he depends on readers feeling free to express themselves in the commentary because of the news value that he often gains from the comments. (*Ibid.*) Although the Internet Protocol address (IP address) associated with each comment is recorded in a log file along with the time of posting, Digital has only limited space on the servers that it uses to host its content, and it puts no priority on retaining such identifying information when it overwrites its servers. (*Id.*, ¶¶ 7-8; 2 AA 259-261.)

C. Digital Covers King Crimson's Copyright Story and Receives Two Anonymous Posts, Much to Escape's Annoyance

On October 13, 2011, Resnikoff wrote one of several articles about Grooveshark, providing copies of email correspondence between Grooveshark executive Paul Geller and Robert Fripp, a member of the rock band King Crimson, and others associated with the band, in which the latter complained about their inability to keep King Crimson's copyrighted recordings from being hosted on Grooveshark. (1 AA 39-40 [].) Geller responded bitterly to Resnikoff's publication of the correspondence, accusing

Fripp of deliberately omitting emails from the correspondence chain which, Geller assumed, had been leaked by Fripp, and objecting to "the headlines you've been creating out of my exchanges" with Fripp. (http://www.digitalmusicnews.com/stories/101711grooveshark.) Geller's email, which Resnikoff published in its entirety on his blog, concluded by saying, "your coverage has been disingenuous at best," and demanding that Resnikoff stop republishing Geller's emails. (*Ibid.*)

The King Crimson article provoked an extended discussion among commenters; on October 17, 2011, an anonymous Internet user, claiming to be an employee of Escape, and using the pseudonym "Visitor," posted the following comment on the story (hereafter First Anonymous Comment):

> I work for Grooveshark. Here is some information from the trenches:
>
> We are assigned a predetermined amount of weekly uploads to the system and get a small extra bonus if we manage to go above that (not easy).The assignments are assumed as direct orders from the top to the bottom, we don't just volunteer to "enhance" the Grooveshark database.
>
> All search results are monitored and when something is tagged as "not available", it get's queued up to our lists for upload. You have to visualize the database in two general sections: "known" stuff and "undiscovered/indie/underground". The "known" stuff is taken care internally by uploads. Only for the "undiscovered" stuff are the users involved as explained in some posts above. Practically speaking, there is not much need for users to upload a major

> label album since we already take care of this on a daily basis.
>
> Are the above legal, or ethical? Of course not. Don't reply to give me a lecture. I know. But if the labels and their lawyers can't figure out how to stop it, then I don't feel bad for having a job. It's tough times.
>
> Why am I disclosing all this? Well, I have been here a while and I don't like the attitude that the administration has acquired against the artists. They are the enemy. They are the threat. The things that are said internally about them would make you very very angry. Interns are promised getting a foot in the music industry, only to hear these people cursing and bad mouthing the whole industry all day long, to the point where you wonder what would happen if Grooveshark get's hacked by Anonymous one day and all the emails leak on some torrent or something.
>
> And, to confirm the fears of the members of King Crimson, there is no way in hell you can get your stuff down. They are already tagged since you sent in your first complaint. The administration knows that you can't afford to sue for infringement.

(1 AA 54.)

A day later, the following anonymous comment was posted to the story, purporting to be from the same poster and again using the pseudonym "Visitor" (hereafter Second Anonymous Comment, and together with the first, Anonymous Comments):

> Yeah, sorry but that is not going happen any time soon. I am not stupid. If someone from digitalmusicnews.com thinks I am trolling, they can go ahead and delete my post. All the King Crimson music will eventually be available again, anyway. Song by song, perhaps, so that pissed English old man won't notice too soon. Don't take my word for it, just be a little bit patient, wait and see for yourselves.

> Do a search after a couple days or whatever. Maybe make a "mistake" and search for "King Crimson" as "song", instead of "artist".
>
> Just because you can't see an album available right now, doesn't mean its not sitting quietly in the background. It is policy to put albums on "backup", when they have to be taken down due to a DMCA notice, to chill things out with the labels and what not. The albums are not deleted, if that's what you guys think.
>
> My impression is that the labels only take action when some artist literally prints a page and holds it in front of their noses. So, if you are an artist, either accept it and move on, maybe find some other business to invest your time and talent, or do what you have to do to defend your current business. Pretending that there is some sort of middle ground won't take you very far.
>
> (You should hear the Big Boss screams today. Ho ho ho. Furious. King Crimson - office chair / Big Boss - Steve Balmer)

(AA 55.)

UMG referred to the First Anonymous Comment in an amended complaint in its federal suit to support its contention that Escape was knowingly hosting copyrighted recordings without the consent of the owners of the copyright in those recordings. (1 AA 144.) Escape objected,[1] pointing out that the reliability of anonymous comments is suspect and that, in any event, an anonymous comment is unsworn hearsay and hence not

---

[1] See Memorandum Supporting Motion to Dismiss, *UMG Recordings v. Escape Media Co.*, No. 1:11-cv-08107-TPG, Document No. 23, at 11-14, available on the Southern District of New York PACER docket.

admissible as evidence. (Fed. Rules Evid., rule 802.) The online docket for the federal lawsuit reveals that the motion to dismiss the federal court action was denied. (2 AA 344.) The record does not reflect that any party has yet attempted to use the Anonymous Comments in the state court action.

On November 28, 2011, Digital received a demand from Escape for the preservation of identifying information about the authors of the First Anonymous Comment. (2 AA 235 ¶ 3.) Such identifying information, had it still existed, would have a consisted of a computer server log file containing the Internet Protocol address used by the commenter's computer in gaining access to the server at the moment of posting, along with a record of the time of posting. (*Ibid.*) Digital knew that its standard procedure was not to maintain such identifying information for more than a few days—given its limited server space, it was Digital's policy to conserve space by overwriting unnecessary information every few days. (2 AA 278 ¶ 7.) Digital's policies treat identifying IP log files as being unnecessary data; this treatment also furthers its policy of protecting the privacy of the blog's users. (*Ibid.*) However, just to be certain, its technical director, Hindle, conducted a search of the location on Digital's computer servers where such identifying information to determine whether any identifying information from the October postings had been retained. Hindle confirmed that the information had not been retained. (2 AA 235 ¶ 3.) Resnikoff posted an article on his blog describing the demand. (1 AA 202-203.)

STATEMENT OF THE CASE

A. The Subpoena and Digital's Further Investigation

On January 9, 2012, Escape subpoenaed Digital to produce documents identifying information about the posters of both Anonymous Comments, and pertaining to any communications between Digital and UMG about either Escape, Grooveshark, or the article about King Crimson to which the comments were posted. (2 AA 279 ¶ 14, 281-290.) Geller sent an email to fellow industry executives explaining that the subpoena "demands details of the relationship UMG had with Digital, which we believe to be nefarious." Resnikoff obtained the email and published it on his blog. (2 AA 279 ¶ 13; http://www.digitalmusicnews.com/permalink/2012/120122grooveshark.) In correspondence with Resnikoff, one of Escape's lawyers asserted that Geller was not speaking for the company in justifying the subpoena that way; but in the same letter, that lawyer accused Resnikoff of "aligning" himself with the assertions of the anonymous posters. (*Id.* at pp. 100, 280 ¶ 16.)

When Digital received the subpoena, its technical director, Hindle, conducted yet another search of Digital's computer servers to determine whether any identifying information had been retained. (2 AA 235 ¶ 4.) In addition to checking the location on Digital's servers where the information would have been saved in the first place, Hindle checked to see whether there were any extant backups of Digital's system from the period when the October 17 log file would still have been in existence. (*Ibid.*) He

determined that there were no extant backups from that time. (*Ibid.*)

Digital served written objections to the subpoena, arguing both that, as a journalist, it was privileged by the California's shield law not to reveal sources, and that the First Amendment protects the right of anonymous Internet speakers to remain anonymous unless Escape follows well-established procedures to notify the poster of the effort to identify her and presents evidence sufficient to show that the disclosure would serve a compelling government interest because the identifying information is essential to permit Escape to protect its litigating interests. (2 AA 279 ¶ 15, 291-304.) In addition, trying to avoid the need for litigation over these privileges, Digital pointed out that it makes no efforts to preserve identifying information, that the non-priority data on his servers is regularly overwritten more than once each week, and, indeed, that given his ordinary business practices, it is highly unlikely that any identifying information remains. (*Ibid.*; 2 AA 278 ¶ 8, 259-260.) Digital also told Escape's counsel that any identifying information about the posters of anonymous comments from mid-October would be long gone. (*Id.* at pp. 292-293.)

In a letter dated January 30, one of Escape's attorneys denied the legal validity of Digital's objections. (*Id.* at p. 99.) In addition, he took issue with the assertion that the identifying information had not been retained, claiming that even when computer files are overwritten, it is possible for fragments of the data to be scattered elsewhere in a server. (*Id.* at pp. 100-101.)

However, the attorney provided no reason for believing that files overwritten within days after their creation, and then overwritten again and again, would still survive in any retrievable form. (*Ibid.*) Nor did he explain why Digital, a third party, should be put to the trouble of searching for data on the theoretical and remote, highly theoretical possibility that fragments could be retrieved. (*Ibid.*)

B. The Motion To Enforce

On March 20, 2012, Escape moved to compel compliance with the subpoena. (1 AA 1-16.) It argued both that the Anonymous Comments were defamatory, and hence unprotected by the First Amendment, (1 AA 12-14), and that identification of the anonymous speakers was needed so that Escape, by showing the falsity of the comments, could bolster its invocation of the DMCA immunity defense in New York state court (1 AA 15). Digital technical staff Hindle conducted yet another search of Digital's servers, digging through databases to ascertain whether any identifying information might be locatable outside the log files that had been overwritten. (2 AA 235 ¶ 5.) Hindle concluded that no data about anonymous commenters was retained. (*Ibid.*)

On April 2, Resnikoff filed a pro se opposition to the motion to enforce. (1 AA 152-163.) The pro se opposition argued First Amendment protection and protection for reporters' sources; it also pointed out that any identifying information had already been deleted. (1 AA 154, 161.)

Expressing doubt about the veracity of Resnikoff's assertion that the data was no longer extant, Escape asked for the opportunity to propound a number of technical questions, in

writing, indicating that it had in mind to take depositions in furtherance of those questions. (2 AA 249-253.) Digital answered Escape's questions in writing, confirming that it has no responsive documents. (2 AA 254, 259-261.)

Digital then retained pro bono counsel who filed a supplemental brief elaborating the arguments against enforcement of the subpoena. (1 AA 166-189.) Digital argued that there was no need to reach Digital's constitutional arguments because its routine deletion of identifying information made the subpoena for identifying material moot. (1 AA 177-178.) On the merits, Digital showed that, to the extent that Escape was seeking to identify the unknown authors of the Anonymous Comments so that it could sue them for defamation, the subpoena was barred because California does not allow pre-litigation discovery to identify parties before a complaint has been filed. (1 AA 178-184.) Moreover, even if a complaint had been filed against Visitor, the test for identifying anonymous defendants so that they can be served with process required Escape to present not just allegations of defamation but evidence that the statements are false and damaging. (1 AA 178-184.)

To the extent that Escape sought to identify the authors in the hope of supporting its DMCA defenses in the New York litigation—that is, by rebutting UMG's potential reliance on the Anonymous Comments to show that copyrighted recordings were being uploaded with Escape's connivance—Digital argued this theory was inadequate for two reasons. First, the Anonymous Comments are not admissible evidence, and hence Escape had no

need to show that the comments were false. (1 AA 184-186.) Second, Escape had not shown that it had exhausted alternative means of discovering the information supposedly needed to support its defenses. (*Ibid.*)

Finally, Digital argued that, because Resnikoff regularly reviews comments posted to his stories to glean information that he can use in future stories, the authors of such comments should be treated as sources and hence protected against disclosure based on California's constitutional shield provision. (1 AA 186-188.)

Escape's reply brief argued that the identity of Visitor was needed not just to further its defense against the state copyright infringement claims but also to pursue counterclaims in the state court action. (1 AA 192, 196.) At the hearing on the motion, Escape clarified this argument, contending that it hoped to show that the Anonymous Comments were posted by a surrogate for UMG, arguably supporting Escape's existing counterclaim that UMG was employing anti-competitive tactics to harm Escape. (2 AA 352, 354.) Escape also included an affidavit from one of Escape's principals, explaining in some detail how statements about Escape in the Anonymous Comments were false. (1 AA 198.) Escape also provided an affidavit from one of its attorneys showing that, in the New York state court litigation, UMG's responses to written discovery had denied any knowledge of the identities of the authors of the Anonymous Comments. (1 AA 200, 208-210, 215-216.) Escape argued, without proffering evidence, that Digital's evidence about the deletion of identifying

information did not entirely negate the possibility that overwritten data might be locatable somewhere on its servers. (1 AA 219-220.)

At oral argument on the motion to compel, Escape's counsel asserted that, as a former prosecutor, he was aware that deleted data could "sometimes" be "retrieve[d]" even though the computer owner believes that the information is unavailable. (2 AA 337.) The same lawyer acknowledged that he was "really . . . not technologically conversant." (2 AA 364.)

The superior court enforced the subpoena. It never issued a written ruling, but its reasoning is reflected in the transcript of the May 15 hearing. (2 AA 313-370.) First, it indicated that, because it had found insufficient affirmative evidence that identifying information could no longer be recovered, it was unwilling to treat the motion to compel as moot. (2 AA 321, 323.) Next, it ruled that although an anonymous comment might fall within California's Shield Law, the law did not apply in this case. (2 AA 361.)[2] Turning to Digital's First Amendment arguments, the court indicated that Escape had established a prima facie case that some statements were false, and thereby met the standard for identifying anonymous defamation defendants established by *Krinsky v. Doe 6* (2008) 159 Cal.App.4th 1154 (*Krinsky*). (*Ibid.*) However, the court did not address the propriety of enforcing a subpoena to identify a possible defendant

---

[2] Digital does not seek review of the issue whether anonymous commenters can ever be sources protected under California's Shield Law.

in a case yet to be filed; instead, it ruled that the subpoena should be enforced because the identity of Visitor was relevant to a core defense in the state court action (*ibid.*) because the court believed the Anonymous Comments might be admissible in the state court litigation under the catchall exception to hearsay, on the theory that the declarant was unavailable and the comment might or might not be deemed sufficiently trustworthy (2 AA 361-363). At the same time, the court suggested that it did not consider the proposed use of identifying information to support a possible counterclaim to be sufficiently related to a core claim or defense to support disclosure under the applicable standard. (2 AA 354-355.) The court did not address whether Escape had shown that it had exhausted alternative means of establishing the falsity of the anonymous comments.

C. Dispute over Preservation and Inspection of Digital's Servers

After the court explained its discovery ruling, Escape's counsel claimed that, in their experience, deleted data can remain in the unallocated blocks of a hard drive, and that data, or fragments of that data, can often be recovered through forensic inspection of the hard drives on which the data had been originally stored. (2 AA 366.) Based simply on that theoretical possibility, Escape asked the court to allow an inspection of Digital's computer equipment, using a computer expert, to see whether the information could be recovered, (2 AA 338.) Escape also asked the court to order Digital to preserve its servers to prevent any further destruction of data that might be responsive to the subpoena. (1 AA 224.) Digital's counsel expressed concern

that it might not be possible to copy or inspect the hard drives without taking the entire system offline, thus taking Digital's web site down. (2 AA 366.) Escape's counsel stated, "I do know the answer, and it definitely can be done." (*Ibid.*) Escape offered no evidence on this point apart from its counsel's ipse dixit; indeed, during the entire time that the parties were conferring and litigating over preservation and inspection, Escape never offered any *evidence* on this question, while Digital's evidence established the opposite of what Escape's counsel represented. Nevertheless, the court accepted Escape's argument and directed Digital to take immediate steps to prevent further overwriting of deleted data, and further directed the parties to meet and confer about an order regarding the preservation. (2 AA 366-369.)

In fact, given the length of time since the log files for comments posted in October 2011 were first overwritten, it was likely that the unallocated blocks in which those log files were originally located would have been overwritten multiple times by January 2012, when Escape's subpoena was first received, not to speak of May 15, when the motion to compel disclosure was granted. (2 AA 237 ¶¶ 12-13, 276 ¶ 4.) Nor did Escape present any evidence that the deleted temporary log files could still be recovered through a forensic examination of the servers on which Digital maintains its web site.

Nevertheless, Digital promptly took steps to comply with the preservation order. (2 AA 236-237 ¶¶ 8-11.) Specifically, Digital operates its web site by creating virtual servers that run on a cluster of several physical servers. (2 AA 234-235.) Digital

immediately copied these virtual servers. (2 AA 236 ¶ 9.) This copy could only be made when Digital's web site was offline, because a server cannot be copied when it is operating. (*Ibid.*; 2 AA 309 ¶ 2.) Because copying the virtual servers was a relatively simple operation that required the web site to be taken offline only for a relatively brief period, Digital technical staff Hindle made copies of both Digital's servers and its content management system during the late night hours on the day of the hearing, the time of day when the Digital web site generally experiences the least traffic. (2 AA 236 ¶ 9.) The copied virtual servers were then stored on one of the physical servers. (2 AA 236 ¶ 11.)

Escape, however, did not accept the preservation of the virtual servers for possible future inspection as sufficient—it insisted that the entire physical server cluster be mirrored forensically, so that it could conduct a forensic examination of the mirrored copy. (1 AA 224-227; 2 AA 393-396.) Given the trial court's preservation order, and because each morsel of data saved onto the physical hard drives could overwrite previously deleted data, Digital suspended the regular security procedures of backing up its web site pending final agreement on the terms of a preservation order. (2 AA 236 ¶ 10.) This suspension was risky—had the web site failed during this period, Digital would have been unable to restore any data added to the site since the last backup had been made. (*Ibid.*)

Complying with Escape's demand would have been expensive, and was well beyond Digital's budget. Paying for the

time of a forensic expert to create a mirror of the entire cluster of physical servers on which Digital maintains its virtual servers would have cost in excess of $20,000. (2 AA 238 ¶ 16.) The process would also be fraught with risk for Digital, because the computer equipment in question is not just a system for storing information while Digital goes about its business; it is the very means by which Digital does its business, by displaying Digital's web site and the advertising that produces all of Digital's revenue. (Id. at p. ¶¶ 15-16.) To avoid closing Digital's web site entirely during the many hours that the servers were being copied, it would have been necessary to take one server at a time offline, during the site's typically slow time in the early hours of several consecutive weekend mornings. (*Ibid.*) It is not uncommon for Digital to clock traffic levels surpassing half-a-million page views or more per month, with huge and unexpected traffic surges over tightly-contained periods of time (hours, a day, several days). (2 AA 235 ¶ 2, 240.) Each server would have to be taken offline for a few hours while it was copied, and after the copying it would have to be re-synchronized with the other servers, a process that also takes several hours; then another server would have to be taken offline and copied. (2 AA 237-238 ¶ 15, 276 ¶ 5.) Even were this process confined to the times when traffic to Digital's site was the lowest, there would be a significant danger that the performance of the web site would be degraded. (*Ibid.*)

Moreover, Digital was convinced that the entire exercise would be wasteful. Despite the theoretical possibility that overwritten identifying information might at one time have been

scattered into the unallocated blocks, the amount of traffic Digital receives would cause the data on the physical storage drives to be overwritten frequently. (2 AA 237 ¶ 12.) That was especially so because the information in question would have been deleted seven months before the preservation order was entered. Moreover, a series of searches beginning six months before the order was entered confirmed that the deletion had occurred. (2 AA 235 ¶¶ 3, 4, 5.) Hence the deleted data was likely to have been overwritten multiple times. (2 AA 237 ¶ 12.) Two experts unaffiliated with Digital concurred in this assessment. (*Ibid.*; 2 AA 276 ¶ 4.)

Digital argued that no further preservation requirements should be imposed, because the burden of establishing the need for a forensic examination of computer equipment rests on the party seeking to impose that process on a discovery target, and that burden is an especially heavy one when it is a non-party witness on whom a party seeks to impose. (Mem. in Support of Digital's Proposed Preservation Order, pp. 7-8.) Moreover, because Digital was not a party to the New York litigation, Digital argued that all the expenses of both preservation and inspection had to be borne by Escape. (*Id.* at pp. 9-10.)

The superior court agreed with Digital's expense argument but was unwilling to address the argument that Escape had not borne the burden of proving the propriety of a forensic examination. (2 AA 385-387.) The court ordered the parties' respective in-house technical experts to meet and confer to determine whether any useful data might be recoverable. (2 AA

387, 389. 401.) That conference occurred on June 5, 2012. (2 AA 266 ¶ 2.) After obtaining this information, Escape still did not submit any evidence or even argument contesting Digital's evidence on the impact and expense of the preservation orders or on the unlikelihood of recovering any useful fragments of identifying information. Nevertheless, the trial court insisted that, so long as Escape was willing to foot the cost of both the preservation and the eventual forensic examination, Digital must preserve the physical servers from the further overwriting of any unallocated blocks. (2 AA 404-407.) Thus, Digital not only continued to run the risk of losing data because of its inability to run backups, but it had to suspend other regular business operations, including software upgrades, new projects, and rental of service space to outside companies, for as long as it took to secure agreement on a procedure for making a mirror image of Digital's hard drives, and to get the necessary equipment into place. (2 AA 236 ¶ 11, 243-245.)

That delay stretched out for seven weeks because, once the superior court had forced Digital to preserve its physical hard drives against further deletion of any fragments of data that might theoretically remain in the unallocated blocks (2 AA 365-367, 406-407), Escape had no incentive to make further decisions about paying for the needed equipment and the needed technical services of a forensic expert (2 AA 405-406, 267-268 ¶¶ 4-6). On June 1, the trial court instructed Escape that, if it wanted to obtain a forensic examination Digital's physical servers, it would need to buy a backup server for Digital so that Digital could

resume the necessary backup process pending the mirroring of the four servers. (2 AA 405-406.) Escape explained that it needed to evaluate the likelihood whether identifying information "will ever be retrievable in terms of the expenditure." (2 AA 405-406.) Then Escape took more than a week to agree to order the backup server (2 AA 266-267) and another two weeks to get the backup server delivered and housed so it could be installed on June 22, 2012 (2 AA 242-243 ¶¶2-4, 267-268 ¶¶ 4-6). Even then, Escape delayed making a final decision about whether to foot the costs of making a mirror image of the physical servers so that Digital could resume full business use of its equipment. (2 AA 270-271 ¶¶ 6-7.)

Given Escape's continuing delays, Digital asked the court to take a different approach, under which Escape would have to finance replacement servers, so that Digital could move its entire operation to a new set of servers, leaving the old servers to be inspected once Digital's planned appeals from the subpoena compliance and inspection orders were completed. (2 AA 272-273 ¶¶ 15-18, 429-430.) Only then, on July 3, 2012, did Escape decide that a forensic inspection of the virtual servers was sufficient for its needs, thus releasing Digital from any further obligation to preserve its physical servers. (2 AA 310-311 ¶ 4, 432-433.)

Having regained full use of its equipment after a seven-week freeze, Digital discontinued the retention of any log files for comments posted to its articles. (2 AA 311 ¶ 5.) Log files serve important business purposes, including identification of the sources of hacking and similar attacks, but Digital decided that it

simply could not afford to face another lengthy suspension of its ordinary business operations in the event that another third party sought to identify a commenter after the files had been deleted, and then demanded preservation of Digital's servers for a forensic inspection. (*Ibid.*)

Escape asked the trial court to obstruct Digital's intended appeal by ordering that the inspection of Digital's virtual server take place immediately, although without disclosing to Escape any identifying information obtained. Escape explained that legal representation on appeal would be expensive, and it did not want to have to defend the inspection it had obtained on appeal unless a forensic expert were able to ascertain that the virtual server contained sufficient fragments of the deleted log files to make the compliance and inspection orders that it had obtained worth defending. (2 AA 432-433.) Escape's counsel made clear that, if no such information could be found, Escape would withdraw any further claim to have the subpoena enforced, thus potentially mooting Digital's appeal. (*Ibid.*) By taking this position, Escape admitted that it lacked confidence that the virtual servers would have any useful data. The trial court agreed to this procedure, reasoning that although the legal issues presented by Digital's appeals were interesting, Escape should not have to defend its victories on appeal if, in fact, the virtual servers contained no useful identifying information. (2 AA 433.) In response to Digital's petition, this court granted a stay of the inspection pending appeal, thus preserving a live controversy.

ARGUMENT

I. Summary and Standard of Review

The superior court's orders should be reversed for two independent reasons. First, the motion to enforce the subpoena was moot when filed because Digital responded to the subpoena, in part, by explaining that it had no responsive documents; the requested documents had been discarded in the ordinary course of business. To avoid mootness, Escape raised the theoretical possibility that overwritten data could be retrieved from the unallocated blocks of Digital's servers through a forensic examination, but it presented no evidence in support of its argument, and in any event none of the circumstances that can, in rare cases, justify such an intrusion were present here. The subpoena was directed to a non-party; there was no evidence of discovery misconduct; and there was no evidence specific to this case showing it was likely that useful information could be gleaned from the unallocated blocks. The trial court should have denied enforcement of the subpoena under discovery law, making the First Amendment argument unnecessary and therefore avoidable.

If the First Amendment argument is reached, enforcement of the subpoena would infringe Visitor's right to speak anonymously. Courts apply a multi-part test when, as in this case, a party seeks to identify anonymous speakers because they are believed to have information that would be useful evidence in support of litigation against another party—here, to bolster Escape's DMCA immunity argument and support Escape's claims

that UMG has been tortiously interfering with Escape's business. Escape has not shown that the evidence is needed to support a core claim or defense, and it has not shown that it has exhausted alternative means to obtaining the information that it needs to advance such a core claim or defense.

An order granting or denying a motion to quash a subpoena normally would be reviewed under the abuse of discretion standard. (*Krinsky*, *supra*, 159 Cal.App.4th at p. 1162.) The same standard presumably applies to orders enforcing subpoenas. (*Johnson v. Superior Court* (1968) 258 Cal.App.2d 829, 837 [holding the superior court abused its discretion by enforcing].) But independent review applies in at least three circumstances. First, the Court of Appeal reviews apparent discretion independently when the facts are undisputed. (*Krinsky*, 159 Cal.App.4th at p. 1161.) Second, the Court of Appeal reviews independently whether the superior court exercised discretion within applicable principles of law. (*Ibid.*) Third, the Court of Appeal reviews independently whether a communication is protected by the First Amendment, deferring only in reviewing findings of contested fact under the substantial evidence standard. (*Id.* at pp. 1161-1162.)

All three exceptions to the deferential standard apply here. Although Escape *argued* contrary to evidence, there are no disputed relevant facts. To the extent one can discern principles of law on which the superior court relied, the court applied the wrong principles in treating operating servers as if they were boxes of old papers in a warehouse; no court operating under

correct principles of electronic discovery could have made the decisions made below. And the ultimate issue here is First Amendment protection. It must be reviewed de novo "both to be sure that the speech in question actually falls within the unprotected category and to confine the perimeters of any unprotected category within acceptably narrow limits in an effort to ensure that protected expression will not be inhibited." (*Bose Corporation v. Consumers Union of U.S., Inc.* (1984) 466 U.S. 485, 505.)

II. The Court Should Have Denied Enforcement to Escape Because the Documents Had Been Discarded in the Ordinary Course of Business and Escape Did Not Justify Forensic Examination

Digital was not required to produce documents that were subpoenaed for use in out-of-state litigation to which it was not a party because those documents had been discarded in the ordinary course of business within a few days of creation. It does not matter that, in theory, a forensic examination of computer equipment can sometimes allow an expert to recover fragments of data from a computer's unallocated blocks. Escape neither showed this is a case in which a court should allow potentially productive forensic examination nor demonstrated any reasonable prospect of discovery of useful information.

A. Digital Had No Duty To Preserve or Submit to Forensic Search of Its Electronic Trash

The well-respected second edition of the Sedona Principles Addressing Electronic Document Production instructs against ordering production in an illustration that perfectly matches this case:

> A party seeking relevant emails demands a search of backup tapes and hard drives for deleted materials. No showing of special need or justification is made for the search. The request should be denied. Parties are not typically required to sequester and search the trash bin outside an office building after commencement of litigation; neither should they be required to preserve and produce deleted electronic information in the normal case. Production should primarily be from sources of active information which is arranged in a manner conducive to retrieval and storage.

(Sedona Principles Addressing Electronic Document Production (2d ed. 2007) (Sedona Principles), Principle 8, com. 8.a, illus. 1, p. 45.)

1. A Nonparty Witness's Data That Is Not Reasonably Accessible Cannot Be Subjected To Forensic Discovery

As the Sedona illustration reflects, California and other jurisdictions draw a line between access to electronic data that is "reasonably accessible" and data that is not "reasonably accessible." For example, the California's e-discovery act permits discovery targets to object to subpoenas or seek protective orders when the requested electronic information "is not reasonably accessible because of undue burden and expense." (Code Civ. Proc. § 1985.8, subd. (d).) This conforms to the Sedona Principles, Principle 8, page 45, and Comments 2.c, page 18, 8.a, page 45, and 8.b, page 46.

Electronic files that have been routinely discarded in the ordinary course of business are "not reasonably accessible because of undue burden and expense." (Code Civ. Proc. § 1985.8, subd. (e).) California's e-discovery statute does not define the key

terms, but a leading case focuses the inquiry on the format of the data: "whether production of documents is unduly burdensome or expensive turns primarily on whether it is kept in an accessible or inaccessible format." (*Zubulake v. UBS Warburg LLC* (S.D.N.Y. 2003) 217 F.R.D. 309, 318.) *Zubulake* has been widely followed by courts in California (*Toshiba America Electronic Components, Inc. v. Superior Court* (2004)124 Cal.App.4th 762, 771; *Conn. Gen. Life Ins. Co. v. Earl Scheib, Inc.* (S.D. Cal. Feb. 6, 2013, No. 11-cv-0788-GPC (WVG)) 2013 WL 485846 at *2; *OpenTV v. Liberate Technologies* (N.D. Cal. 2003) 219 F.R.D. 474, 476), and elsewhere (*Juster Acquisition Co., v. North Hudson Sewerage Authority* (D.N.J. Feb. 11, 2103, No. 12-3127) 2013 WL 541972; *Boeynaems v. LA Fitness Internat. LLC* (E.D. Pa. 2012) 285 F.R.D. 331, 335-338).

The data, production of which was ordered below, is in an inaccessible format. (See *Zubulake v. UBS Warburg LLC*, *supra*, 217 F.R.D. at pp. 318-319 [classifying "[e]rased, fragmented, or damaged data" as the "least accessible" of five categories of data].) If data still exists at all—which is doubtful—it can be located and restored only through a comprehensive forensic examination, a process involving tremendous "burden and expense." The estimate that Digital received from a California-based forensic expert put the cost of the expert's services alone well into the five figures. (2 AA 238 ¶ 16.) In the court below, Escape never disputed these cost projections, but in any event, courts faced with conflicting accounts generally credit the testimony of a computer system's owners and operators, given

their firsthand knowledge of the systems involved. (See, e.g., *Jimena v. UBS AG Bank, Inc.* (E.D. Cal. Aug. 27, 2010, No. 1:07-cv-00367-OWW-SKO) 2010 WL 3397431 at *4 ["Because Yahoo states that further searches for responsive electronic data would be extremely expensive and unlikely to yield different results, the Court cannot compel Yahoo to conduct additional costly and burdensome searches"]; *Alexander v. Federal Bureau of Investigation* (D.D.C. 1998)188 F.R.D. 111, 116-117 [refusing to order costly and time-consuming restoration of deleted files, and stating that "the court finds [respondent's] declarations are more persuasive given the declarants' familiarity with the systems at issue"].)

One reason that courts draw a line between reasonably accessible and not reasonably accessible data is that the recovery of inaccessible data generally requires taking the relevant computer equipment offline so that it can be copied, with possible disruption of the business of the party that is the target of discovery. (See, e.g., *Simon Property Group L.P. v. mySimon, Inc.* (S.D. Ind. 2000) 194 F.R.D. 639, 642 ["The court does not intend that the inspection apply to defendant's computers and servers that actually provide defendant's comparative shopping services over the Internet"].) The evidence in this case amply supports that proposition—to comply with the preservation order while awaiting Escape's decision about whether to mirror the physical servers, Digital had to forego ordinary security backups of its web site for well over a month, and it had to forego normal business uses of its servers for seven weeks. The copying of the virtual

servers was effected more quickly, but still required that the web site be taken off line for a period of time. (2 AA 309 ¶ 2, 237 ¶ 15.)

Given the burden and expense of mirroring servers so that forensic inspection may occur, courts have generally resorted to this extraordinary remedy only upon a showing that the opposing party has been delinquent in its disclosure obligations. Several federal appellate courts have indicated that forensic inspection can be ordered only when a party from whom discovery is sought has failed to comply with the discovery rules in significant ways. (*John B. v. Goetz* (6th Cir 2008) 531 F.3d 448, 460; *McCurdy Group v. Am. Biomedical Group, Inc.* (10th Cir.2001) 9 Fed.Appen. 822, 831; *In re Ford Motor Co.* (11th Cir. 2003) 345 F.3d 1315, 1317.) The burdens of forensic examination are imposed as a remedy for misconduct in discovery. (*Bennett v. Martin* (Ohio App. 2009) 186 OhioApp.3d 412, 928 N.E.2d 763, 774.) It takes a "background of noncompliance" before the wronged party "can seek an order to tromp through the opposing parties' electronically stored garden." (*Scott Process Systems, Inc. Mitchell* (Ohio App. Dec. 17, 2012, 2012-CA 00021) 2012 WL 6617363 at *5 .)

Several federal courts in California and elsewhere have applied similar standards. (See, e.g., *Dawe v. Corrections USA* (E.D. Cal. 2009) 263 F.R.D. 613, 619 [suspecting, based on "the level of contention and distrust that permeates this litigation," that there had been intentional "transfer or deletion of information, or other efforts to minimize, hinder or prevent access to information"]; *Playboy Enterprises, Inc. v. Welles* (S.D.

Cal. 1999) 60 F.Supp.2d 1050, 1054 [ordering mirroring because defendant continued to actively delete emails "apparently without regard for this litigation"]; *Simon Property Group L.P. v. mySimon, Inc.*, *supra*, 194 F.R.D. at p. 641 [ordering imaging after observing "troubling discrepancies with respect to [the subpoenaed party's] document production"]; *Diepenhorst v. City of Battle Creek* (W.D. Mich. June 30, 2006, No. 1:05-cv-734) 2006 WL 1851243, at *3 ["In the absence of a strong showing that the responding party has somehow defaulted in [its discovery] obligation, the court should not resort to extreme, expensive, or extraordinary [electronic discovery] means to guarantee compliance]."") Similarly, the Sedona Principles provide that "[i]ntrusive access to desktop, server, laptop or other hard drives or media storage devices . . . should not be required unless exceptional circumstances warrant the extraordinary cost and burden." (Sedona Principles, *supra*, com. 8.c, p. 47.)

The California e-discovery statute provides additional support for this distinction. Code of Civil Procedure, section 1985.8, subdivision (m)(1) provides that "[a]bsent exceptional circumstances, the court shall not impose sanctions on a subpoenaed person or any attorney of a subpoenaed person for failure to provide electronically stored information that has been lost, damaged, altered, or overwritten as the result of the routine, good faith operation of an electronic information system."[3] Imposing the burden of forensic inspection on Digital would, in

[3] This statute is cited as subdivision (*l*) in trial court papers. It was rearranged without substantive change in 2012.

effect, severely penalize it for simply carrying on the commonplace practice of overwriting IP address data daily.

Tellingly, to the extent the cases cited *ante* allowed forensic intrusion into data not reasonably available, they ordered production by parties to litigation. No party to this case has identified authority subjecting a third-party witness to the kind of discovery ordered here. Digital is not a party to the suits between Escape and UMG, and, despite occasional hints from Escape's counsel that his client believes Digital colluded with UMG in some unspecified way, no evidence has been provided, nor has any specific allegation of wrongdoing been leveled against Digital.

It is well-established in both California and federal law that nonparties enjoy special protection from burdensome discovery requests. (See, e.g., *Calcor Space Facility v. Superior Court* (1997) 53 Cal.App.4th 216, 225 ["The concerns for avoiding undue burdens on the 'adversary' in the litigation . . . apply with even more weight to a nonparty"]; *Exxon Shipping Co. v. U.S. Dept. of Interior* (9th Cir. 1994) 34 F.3d 774, 779 ["The Federal Rules . . . afford nonparties special protection against the time and expense of complying with subpoenas"].) This is especially true in the e-discovery context, with its elevated concerns of expense and privacy. California's e-discovery statute includes a provision granting protections to third parties over and above those generally applicable. (See Code Civ. Proc., § 1985.8, subd. (*l*) ["An order of the court requiring compliance with a subpoena issued under this section shall protect a person who is neither a

party nor a party's officer from undue burden or expense resulting from compliance"].) A federal court recently emphasized the importance of nonparty status in refusing to order invasive electronic discovery similar to the type sought here. (See *Tucker v. Am. Int'l Group* (D. Conn. Mar. 15, 2012, No. 3:09-cv-1499) 2012 WL 902930, at *9 ["[Subpoenaed entity] is not a party in this case and would be subjected to significant burden and expense in the event of the requested inspection"].)

2. *Digital's Data Is Not Reasonably Accessible*

Escape argued that, although Digital had denied having any discoverable information, its affidavits had simply said Digital *assumed* it had not retained identifying information. (2 AA 320-323.) Escape thus argued that Digital's evidence did not show Visitor's identifying information had been destroyed. (*Ibid.*) The superior court may have adopted this argument. (2 AA 323.)

First, Escape's argument misplaces the burden. Once a discovery target denies having the relevant documents, the party seeking discovery should have the burden to show that the relevant data exists, before imposing the significant trouble and expense of taking heroic measures to preserve data for possible forensic examination. Escape provided no evidence supporting a prospect of recovering useful information. It persisted in this failure even after its technical experts conferred with Digital's. Coldly put, in the whole Southern California market of e-discovery consultants, Escape could not pay a single witness to say there was any reasonable chance of finding anything.

Perhaps nothing speaks louder than Escape's actions—whenever it was faced with a material expense to proceed with the discovery, it declined to proceed. It even tried to mot this appeal, expressing no confidence in recovery of any useful data.

Second, continued existence of useful information is *not* an inference that a reasonable mind can draw from Digital's evidence. Digital showed below that it had searched for the data on three separate occasions, each search more thorough than the previous one—after receiving a preservation demand six weeks after the deletion would have occurred (2 AA 235 ¶ 3), after receiving Escape's subpoena (*id.* ¶ 4), and before Resnikoff submitted his pro se opposition to the motion to compel (*id.* ¶ 5). Even assuming that it was Digital's burden to *prove* that it had searched for the information, but found the information did not exist, Digital carried that burden, and there is nothing in the record upon which a trier of fact could discredit Digital's proof. Nevertheless, the trial court first enforced the subpoena (2 AA 459-460) and then required preservation and forensic examination (2 AA 462-468). Because there was no evidence of discovery non-compliance—indeed, the undisputed evidence is that Digital conducted a diligent search for the requested documents—there was no basis for ordering preservation of servers or forensic inspection or such preserved servers.

The burdens imposed by the superior court are manifestly unfair, as well as contrary to widely shared statutory and decisional law. Research has not turned up a single case in which

a non-party witness was ordered to submit its computers for forensic examination.

B. Escape Made No Showing of a Reasonable Likelihood of Discovering Useful Information

Digital's failure to prove a reasonable likelihood of discovering useful information provides an independent ground to reverse the discovery orders. Both Digital's technical staff and two different independent experts agree that, because of the way Digital maintains its web site, using virtual servers that sit on the actual physical servers, and because of the number of times that the physical servers would have been written over in the seven months since the log files were first deleted, the chance is negligible that fragments of those log files can be found in the nooks and crannies of the servers. (2 AA 237 ¶ 12, 275-276 ¶¶ 3-4.) And there is a serious danger that fragments that appear to be related could actually be unrelated, thus creating false positives that would not be admissible in the New York litigation. (2 AA 237 ¶ 13.) Escape submitted *no* evidence in support of its counsel's arrant speculation on this point, even after its expert was given the opportunity to interrogate Digital's in-house technical expert about the operation of its hardware and software.

Some standard of probability of success comes into play even in considering an order for forensic examination of a party's computers. A federal court in California, for example, ordered mirroring only on the condition that the requesting party "can provide the Court with sufficient evidence that recovering some deleted e-mail is just as likely as not receiving any deleted

email." (*Playboy Enterprises, Inc. v. Welles*, *supra*, 60 F.Supp.2d at pp. 1054-1055.) Similarly, the Sedona Principles declare that the duty to preserve information in formats that are not reasonably accessible arises "only when there is a substantial likelihood that the information exists." (Sedona Principles, *supra*, com. 5.e, p. 33.) By contrast, Escape's request for copying of the physical servers, in the hope that some fragments might be recoverable from the servers, is nothing more than a shot in the dark.

The history of this case shows the dangers that the trial court's approach poses to other California companies that host online data on computer servers that are available for third party use. The burden of storing server logs indefinitely can be substantial, because as more IP addresses accumulate over time on a high-traffic web site, they can take over server space that is needed for other data. (2 AA 311 ¶ 5.) Every company that hosts computer servers on which identifying information is collected and retained for a discrete period of time necessarily has a policy about deleting that information after the business reasons for collecting that information have dissipated. (2 AA 307 ¶ 5.) The Best Practices for Online Service Providers, published by the Electronic Frontier Foundation, (https://www.eff.org/wp/osp (June 20, 2008)) recommends for privacy reasons that servers "logs [be] retained for the shortest possible time."

Hosting online commentary is a major industry in California, where many of the nation's largest hosting companies are located, including Google, Yahoo!, Twitter, Automattic

(WordPress), and SAY Media (Typepad). Media companies, too, commonly allow individual subscribers to comment on stories. All together, these companies receive thousands of subpoenas every year, and if the mere fact that their ordinary business practices include the eventual deletion of log files for anonymous comments means that those companies are subject to the sort of data preservation and forensic examination orders that to which Digital was subjected below, the impact on their business could be serious. Further, the proceedings below provide a virtual textbook for attacks on journalists and hosting businesses by disgruntled subjects of Internet journalism and blogging. Harassment can and will suppress legally protected free expression. To illustrate, based on its experience in this case and the continuing hostility of Escape (2 AA 279 ¶¶ 12-13, 307-308 ¶ 6) Digital decided that turning off server logging altogether, despite the security risks, is better than risking a repeat experience with the superior court. (2 AA 311 ¶ 4.)

Finally, a decision to make mere witnesses' electronic trash available to any litigant willing to pay the out-of-pocket costs of forensic examination implies a philosophy of judicial intervention not approved by the California Supreme Court or the Legislature. Escape argued that a business should be exposed to tort damages and criminal prosecution for failure to preserve electronic trash after having notice that some litigant may want to search the trash. (2 AA 365-366, 404.) The California Supreme Court rejected the much less intrusive theory of spoliation of tangible evidence. (*Temple Community Hospital v. Superior Court* (1999)

20 Cal.4th 464, 466.) While the superior court stated that continued operation of servers—overwriting possible trash on unallocated blocks—did not violate the oral preservation order (2 AA 404), the court's oral interpretation of its oral order gives hosts of online commentary no comfort that some other court or public official will not charge a host with obstruction of justice simply for continuing to operate its servers. Whether to elevate litigants' interest in electronic trash over the Internet expression enabled by hosts is a public policy choice that, if worthy of consideration at all, should be debated in Sacramento. It certainly should not be decided by mission creep in superior courts, contrary to the fundamental policy choices the California Supreme Court made in *Temple*.

III. Enforcement Would Violate Third-Party First Amendment Rights

A. The First Amendment Constrains Judicial Power To Uncover the Identity of Anonymous Internet Speakers

The subpoena violates the First Amendment's protections for the right of anonymous speech.[4] The First Amendment protects the right to speak anonymously. (*Watchtower Bible &*

---

[4] Web site hosts have standing to litigate the rights of their users not to be identified. (*Matrixx Initiatives, Inc. v. Doe* (2006) 138 Cal.App.4th 872; see, e.g., *McVicker v. King* (W.D.Pa. 2010) 266 F.R.D. 92, 95-96; *Enterline v. Pocono Medical Center* (M.D. Pa. 2008) 751 F.Supp.2d 782, 785-786.) Moreover, given the way in which Resnikoff uses the comments as part of his newsgathering effort, and the potential impact of compelled disclosure on his continuing ability to report the news, Resnikoff's own free speech rights are implicated by the discovery orders.

Tract Society of N. Y., Inc. v. Village of Stratton (2002) 536 U.S. 150, 166-167; *Buckley v. American Constitutional Law Foundation, Inc.* (1999) 525 U.S. 182, 199-200; *McIntyre v. Ohio Elections Com.* (1995) 514 U.S. 334, 342; *Talley v. California* (1960) 362 U.S. 60, 64.) The Supreme Court has celebrated the important role played by anonymous or pseudonymous writings over the course of history, from the literary efforts of Shakespeare and Mark Twain to the authors of the Federalist Papers. As the Supreme Court said in *McIntyre*:

> [A]n author generally is free to decide whether or not to disclose his or her true identity. 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, . . . 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.
>
> [¶]
>
> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent.

(*McIntyre*, 514 U.S. at pp. 341-342, 357.)

California courts have squarely agreed that the First Amendment protects the right to speak anonymously (*Krinsky*, *supra*, 159 Cal.App.4th at pp. 1163-1164), and also held that the

California Constitution provides its own independent support for this right (*Rancho Publications v. Superior Court* (1999) 68 Cal.App.4th 1538, 1144).

The right of anonymous expression applies to speech on the Internet. The Supreme Court has treated the Internet as a forum of preeminent importance because it places in the hands of any individual who wants to express his views the opportunity to reach other members of the public who are hundreds or even thousands of miles away, at virtually no cost. (*Reno v. American Civil Liberties Union* (1997) 521 U.S. 844, 850-853.) Accordingly, First Amendment rights fully apply to communications over the Internet. (*Id.* at pp. 868-869.)

Internet speakers speak anonymously for various reasons. They might wish to avoid having their views stereotyped according to their race, ethnicity, gender, or class characteristics. They might be associated with a group but want to express opinions of their own, without running the risk that, however much they disclaim attribution of opinions to the group, readers will assume that the individual speaks for the group. They might discuss embarrassing subjects and might want to say or imply things about themselves that they are unwilling to disclose otherwise. And they might wish to say things that might make other people angry and stir a desire for retaliation. As the Sixth District Court of Appeal recognized in *Krinsky*, *supra*, 159 Cal.App.4th at p. 1162:

> The use of a pseudonymous screen name offers a safe outlet for the user to experiment with novel ideas, express unorthodox political views, or criticize

> corporate or individual behavior without fear of intimidation or reprisal. In addition, by concealing speakers' identities, the online forum allows individuals of any economic, political, or social status to be heard without suppression or other intervention by the media or more powerful figures in the field.

Whatever the reason for wanting to speak anonymously, a rule that makes it too easy to remove the cloak of anonymity will deprive the marketplace of ideas of valuable contributions.

While the Internet gives individuals the opportunity to speak anonymously, it creates an unparalleled capacity to monitor speakers and discover their identities. Speakers who send e-mail or visit a website leave behind electronic footprints that can, if saved by the recipient, provide the beginning of a path that can be followed back to the original senders. Thus, anybody with enough time, resources and interest, if coupled with the power to compel the disclosure of the information, can learn who is saying what to whom, if the information has been retained.

A court order, even if granted for a private party, is state action and hence subject to constitutional limitations. (*N. Y. Times Co. v. Sullivan* (1964) 376 U.S. 254, 265; *Shelley v. Kraemer* (1948) 334 U.S. 1, 14.) A court order to compel production of individuals' identities in a situation that threatens the exercise of fundamental rights "is subject to the closest scrutiny." (*National Assn. for the Advancement of Colored People v. Alabama* (1958) 357 U.S. 449, 461 (*NAACP*); *Bates v. City of Little Rock* (1960) 361 U.S. 516, 524.) Abridgement of the rights to speech and press, "even though unintended, may inevitably

follow from varied forms of governmental action," such as compelling the production of names. (*NAACP*, 357 U.S. at p. 461.) Rights may also be curtailed by means of private retribution following court-ordered disclosures. (*Id.* at p. 462-463; *Bates*, 361 U.S. at p. 524.)

As one court stated in refusing to enforce a subpoena to identify anonymous Internet speakers whose identities were allegedly relevant to defend against a shareholder derivative action, "If Internet users could be stripped of that anonymity by a civil subpoena enforced under the liberal rules of civil discovery, this would have a significant chilling effect on Internet communications and thus on basic First Amendment rights." (*Doe v. 2theMart.com, Inc.* (W.D. Wash. 2001) 140 F.Supp.2d 1088, 1093.) Similarly, in *Columbia Insurance Co. v. Seescandy.com* (N.D. Cal. 1999) 185 F.R.D. 573, 578, the court expressed concern about the possible chilling effect of such discovery:

> People are permitted to interact pseudonymously and anonymously with each other so long as those acts are not in violation of the law. This ability to speak one's mind without the burden of the other party knowing all the facts about one's identity can foster open communication and robust debate . . . . 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.

B. Escape Failed To Meet Any Standard To Discover Identity for Future Litigation

The superior court correctly discarded as too speculative Escape's theory that discovery Visitor's identity would enable Escape to pursue a tort claim against UMG. (2 AA 355.)

That leaves Escape's potential suit against Visitor. Before reaching the constitutional issue, the defamation theory should be discarded because California does not permit pre-litigation discovery to identify defendants. Escape has not sued Visitor, and doubts whether it wants to. (2 AA 324.) The statute of limitations has almost certainly expired. (Code Civ. Proc., § 340, subd. (c).) California does not allow pre-litigation discovery to obtain the identity of proposed defendants (Code Civ. Proc., § 2035.010) and similarly does not allow foreign discovery in support of such an objective (Code Civ. Proc., § 2029.600 [California law applies to discovery in California based on out-of-state action]). In *Christ v. Superior Court* (1931) 211 Cal. 593, the California Supreme Court said that the only reason a trial court had jurisdiction to issue subpoena for pre-litigation discovery, on commission from a Guatemala court, was that the Guatemala proceeding was the same as what Code of Civil Procedure authorized within California. (211 Cal. at pp. 597-598.) Therefore, even crediting Escape with a genuine motive to pursue a defamation case, that purpose for the subpoena does not support enforcement of the subpoena.

If identifying defendants, when no action is pending, for the purpose of suing them, is permissible in California, California should adopt the multi-part constitutional balancing test,

articulated in *Dendrite Internat., Inc. v. Doe, No. 3* (App. Div. 2001) 342 N.J. Super. 134, 775 A.2d 756, 767-768 and since followed in many other states, including the Sixth Appellate District in *Krinsky*, *supra*, 159 Cal.App.4th 1154.[5] Under that test, the plaintiff (i) must give reasonable notice the potential defendants and an opportunity for them to defend their anonymity before issuance of any subpoena, (ii) must allege with specificity the speech or conduct claimed to have violated its rights, (iii) must state a cause of action against each defendant, and (iv) must produce evidence supporting each element of its claims.[6] (See, e.g., *Doe v. Cahill* (Del. 2005) 884 A.2d 451, 460; *Solers, Inc. v. Doe* (D.C. App. 2009) 977 A.2d 941, 954; *In re Does 1-10* (Tex. Civ. App. 2007) 242 S.W.3d 805, 814, fn. 3, collecting cases.)

---

[5] In *Krinsky*, the plaintiff sued the defendants as Does and then sought their identities in the pending action against them.

[6] A majority of states also apply a fifth criterion, first articulated in *Dendrite*, but not adopted in *Krinsky*, under which the court must weigh the potential harm (if any) to the plaintiff from being unable to proceed against the harm to the defendant from losing the First Amendment right to anonymity. (*In re Ind. Newspapers, Inc.* (Ind. App. 2012) 963 N.E.2d 534, 549-553; *Pilchesky v. Gatelli* (Pa. Super. 2011) 12 A.3d 430; *Mortgage Specialists, Inc. v. Implode-Explode Heavy Industries, Inc.* (N.H. 2010) 160 N.H. 227, 999 A.2d 184, 192; *Independent Newspapers, Inc. v. Brodie* (Md. 2009) 407 Md. 415, 966 A.2d 432, 456-457; *Mobilisa, Inc. v. Doe* (Ariz. Ct. App. 2007) 170 P.3d 712; see Levy, *Litigating Civil Subpoenas to Identify Anonymous Internet Speakers*, 37 Litigation No. 3 (Spring 2011).)

Escape did not meet the *Krinsky* standard. It produced no evidence of element (i) and no evidence of causation or damages under element (iv).

C. Escape Failed To Meet the Standard for Discovery To Assist Pending Litigation

The leading case of *Doe v. 2theMart.com, Inc.*, *supra*, 140 F.Supp.2d 1088, establishes the test to be applied when a party seeks to identify an anonymous speaker to obtain evidence for use against a party in pending litigation. The test is similar to the First Amendment test for a subpoena for a reporter's sources. (*2theMart.com, Inc.*, 140 F.Supp.2d at p. 1095.) Under that test, once notice has been given to the anonymous commenters,

> 1. The subpoena must have been issued in good faith.
>
> 2. The information sought must relate to a core claim or defense.
>
> 3. The identifying information must be directly and materially relevant to that claim or defense.
>
> 4. Information sufficient to establish or to disprove that claim or defense must be unavailable from any other source.

(*Id.* at pp. 1095-1097.) In addition, "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." (*Id.* at p. 1095.)

Several courts have followed this test. (*In re Rule 45 Subpoena Issued to Cablevision Systems Corp. Regarding IP Address 69.120.35.31* (E.D.N.Y. Feb 5, 2010, No. MISC 08-MC-347 (ARR) (MDG)) 2010 WL 2219343 at *8-11, *adopted in*

relevant part, (E.D.N.Y. Apr. 26, 2010, No. MISC 08-MC-347 (ARR) (MDG)) 2010 WL 1686811 at *2-3; *McVicker v. King*, *supra*, 266 F.R.D. at pp. 94-97; *Sedersten v. Taylor* (W.D. Mo. Dec. 9, 2009, No. 09-3031-CV-S-GAF) 2009 WL 4802567, at *2; *Enterline v. Pocono Medical Center*, *supra*, 751 F.Supp.2d at pp. 787-788; see also *Anderson v. Hale* (N.D. Ill. May 10, 2001, No. 00-C-2021) 2001 WL 503045, at *7-9.)

Escape failed the test. First, by the time of the second order, it should have been clear to the superior court that if Escape ever acted in good faith, it no longer met that criterion. Escape's behavior puts the lie to its words: Although it demanded that Digital stop overwriting data on Digital's physical servers, thus freezing Digital's business development, Escape was never willing to incur material expense to pursue data on those physical servers.

Second, the identity of Visitor does not go to a core claim or defense. The Anonymous Comments are inadmissible hearsay from an unknown declarant or unknown declarants. Escape provided no New York state law that could have allowed UMG to offer them.[7] UMG takes its own risks by mentioning the First Anonymous Comment in a federal pleading, but its attempt to slip in olfactory evidence should be of no concern to California

---

[7] The superior court speculated about the possibility that a trial judge might be willing to treat an anonymous Internet comment as having sufficient indicia of trustworthiness to warrant admission under the federal "catch-all" exception to the hearsay rule, but cited not a single supportive case in the entire country. (2 AA 361-363.) It is hard to imagine such ruling.

courts or to Digital. Escape produced no evidence that UMG has proffered either of the comments as evidence for any purpose. Indeed, review of an oral argument transcript in the federal case revealed that the only party that was making reference to the First Anonymous Comment was Escape. (2 AA 344.) Because UMG cannot rely on the Anonymous Comments, information about the Visitor's identity does not go to the core of anything about either the state court case from which the discovery demand issued or the related federal case.

To be sure, the truth or falsity of the contents of the anonymous comments could be relevant to the underlying litigation—that is, do Escape's employees engage in the uploading of copyrighted content without permission from the copyright holders? Do they do this with the knowledge of their supervisors? Does Escape have a compensation or evaluation system under which staff believe that they have an incentive to infringe violate copyright? But neither a logical theory of relevance or "discovery relevance"—the possibility of leading to admissible evidence—is enough in the First Amendment context. Under the analogous situation of subpoenas to identify confidential sources, courts have held that the party seeking such discovery has to provide at least a prima facie basis for believing that the discovery will produce information supporting the discovering party's case. (*In re Petroleum Products Antitrust Litigation* (2d Cir. 1982) 680 F.2d 5, 6-8; *Richards of Rockford, Inc. v. Pacific Gas & Electric Co.* (N.D. Cal. 1976) 71 F.R.D. 388, 390-391.) At most, it is UMG that might be interested in

identifying Visitor in the hope he, she, or they could give admissible testimony. There is no reason to believe UMG has done so. And if it does, Escape can notice the deposition of the person whose name has been provided by UMG. It will not need discovery from Digital.[8]

Escape also flunked the unavailability test. The truth about the matters to at issue between Escape and UMG will be found by discovery from Escape's present employees, its former employees, and its own documents, both electronic and hard copy. Until that discovery is completed, neither UMG nor Escape will have exhausted the other sources from whom discovery must be sought before the First Amendment rights of the anonymous commenters and of Resnikoff himself can be infringed. "[A]n alternative requiring the taking of as many as 60 depositions might be a reasonable prerequisite to compelled disclosure." (*Zerilli v. Smith* (D.C. Cir. 1981) 656 F.2d 705, 714.)

Escape's theory of exhaustion of other sources does not pass muster. For example, Escape stated it had served written

---

[8] In the court below, Escape argued that the very fact that UMG was not trying to identify the anonymous speaker supported its speculation that UMG might have been the source of the comment. (2 AA 336.) As UMG argued in response to Escape's federal court motion to dismiss, it considers that it has abundant direct evidence that Escape employees deliberately uploaded copyrighted sound recordings to its site. (See Mem. in Opposition to Motion to Dismiss, *UMG Recordings v. Escape Media Co.*, No. 1:11-cv-08107-TPG, Document No. 29, at 11-14, available on the Southern District of New York PACER docket.) A reasonable lawyer for UMG, having no ill will toward Digital, would not waste resources on an anonymous Internet post.

discovery on UMG asking about the identity of the authors of the anonymous comments, and UMG had denied having any such knowledge or contacts. (1 AA 200 ¶ 8, 205-217.) At most, that discovery addressed Escape's speculation that Visitor was a proxy for UMG. It did not address whether other sources exist to support or refute the substance of the Anonymous Comments.

Escape made no showing that it conducted any internal investigation into either the identity of Visitor or the veracity of the posted comments. After all, the premise for the Anonymous Comments was that the poster is an Escape employee with inside knowledge. Escape has not disclosed how large is the set of such people, nor has it explained why it could not establish the falsity of the information in the posts by interviewing those employees.

But even informal investigation would not be enough. In *O'Grady v. Superior Court* (2006) 139 Cal.App.4th 1423, the Court of Appeal considered the application of the qualified First Amendment privilege for journalists to withhold the identity of their sources, in a situation very similar to this case—the plaintiff was seeking to identify a source that might or might not have been one of its own employees. In applying the part of the test that considers whether the discovering party had exhausted alternative means of obtaining the relevant information the court approvingly cited *Zerilli v. Smith*, *supra*, 656 F.2d 705, and *In re Petroleum Prod. Antitrust Litigation*, *supra*, 680 F.2d 5, including their language about taking sixty depositions as cited *ante*. (*O'Grady*, 139 Cal.App.at pp. 1471-1472.) The Court of Appeal noted that there were only twenty-nine Apple employees who

would have had access to the trade secrets disclosure of which was the subject of the litigation. Apple had interviewed each of them about whether they were responsible for the disclosure, but even that was not enough, because admitting to leaking trade secrets would likely be grounds for discharge, and "[p]eople who are willing to take risks of one type may yet be very reluctant to lie under oath. . . . Questioning under oath exposes the person questioned to criminal prosecution for any willful falsehoods. That is no guarantee of truthful answers, but it certainly provides a stronger incentive to tell the truth than the mere risk of discharge." (*Id.* at p. 1472.) The court granted mandamus requiring the trial court there to set aside the order compelling compliance with a third-party subpoena. (*Id.* at pp. 1431, 1479.) Similarly, here, Escape's failure to show that it has pursued discovery from its own staff is sufficient reason to hold that it has not exhausted alternative means of proving the facts that it claims are the reasons for the subpoena in this case.

The superior court should have applied *O'Grady v. Superior Court*, *supra*, 139 Cal.App.4th 1423 with special emphasis here. That is because Digital is not a party whose liability is sought to be enforced through discovery. As the Court of Appeal said in *O'Grady*, "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." (*O'Grady*, 139 Cal.App.4th at p. 1468.) The fact that the subpoenaed journalists were *not* defendants weighed

against disclosure. (*Id.* at p. 1470.) Digital is not a party to the litigation. Escape failed to show unavailability.

In sum, if the superior court's order could be affirmed as a matter of discovery law, it violates the First Amendment rights of Visitor and must be reversed.

CONCLUSION

The orders enforcing the subpoena, and commanding Digital to preserve its servers and make them available for forensic inspection, should be reversed with directions to enter a new and different order denying enforcement.

Respectfully submitted,

PAUL ALAN LEVY
PUBLIC CITIZEN LITIGATION GROUP

MCKENNA LONG & ALDRIDGE LLP
BY CHARLES A. BIRD

Attorneys for Digital Music News LLC

CERTIFICATE OF COMPLIANCE

I, Charles A. Bird, appellate counsel to Digital Music News LLC, certify that the foregoing brief is prepared in proportionally spaced Century Schoolbook 13 point type and, based on the word count of the word processing system used to prepare the brief, the brief is 13,004 words long.

Charles A. Bird

PROOF OF SERVICE

IN THE MATTER OF SUBPOENA IN UMG RECORDINGS et al. v. DIGITAL MUSIC NEWS, LLC.
Court of Appeal, Second Appellate District, Division One, Case No. B242700
c/w B243623
Los Angeles Superior Court, Case No. SS022099; Judge Richard A. Stone, Jr.

I, Leisa Bitting, declare as follows: I am employed with the law firm of McKenna Long & Aldridge LLP, whose address is 600 West Broadway, Suite 2600, San Diego, California 92101-3372. I am over the age of eighteen years, and am not a party to this action. On **April 18, 2013**, I served the foregoing document described as:

APPELLANT'S OPENING BRIEF

[X] **U. S. MAIL:** I placed a copy in a separate envelope, with postage fully prepaid, for each addressee named below for collection and mailing on the below indicated day following the ordinary business practices at McKenna Long & Aldridge LLP. I certify I am familiar with the ordinary business practices of my place of employment with regard to collection for mailing with the United States Postal Service. I am aware that on motion of the party served, service is presumed invalid if postal cancellation date or postage meter date is more than one day after date of deposit or mailing affidavit.

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

Executed at San Diego, California on **April 18, 2013**.

Leisa Bitting

Leisa Bitting

SERVICE LIST

John Rosenberg Rosenberg & Giger 488 Madison Avenue, 10th Floor New York, NY 10022	Attorneys for Plaintiff and Respondent Escape Media Group, Inc. **(1 copy of brief)**
Pierre B. Pine McPhereson & Associates 1801 Century Park East, 24th Floor Los Angeles, CA 90067	Attorneys for Plaintiff and Respondent Escape Media Group, Inc. **(1 copy of brief)**
Los Angeles County Superior Court Beverly Hills Courthouse 9355 Burton Way Beverly Hills, CA 90210-3669 Attn: The Hon. Richard A. Stone, Jr.	**(1 copy of brief)**
Supreme Court of California 350 McAllister Street San Francisco, CA 94102-4797	**(Electronically Submitted via electronic submission to the Second District Court of Appeal)**

US_WEST 803731536.1