HARDIN LAW OFFICE

Matthew D. Hardin · 101 Rainbow Drive · PMB 11506 · Livingston, TX 77399
Phone: (202) 802-1948 · Email: HardinLawPLLC@icloud.com

EXHIBIT D

May 18, 2026

Lane Haygood, Esq.
Kamerman, Uncyk, Soniker & Klein P.C.
1700 Broadway, 16th Floor
New York, New York 10019

Re: Response to Notice of Deficiency dated May 1, 2026
Lolcow LLC v. Fong-Jones, Case No. 1:26-cv-02059-KPF (S.D.N.Y.)

Dear Mr. Haygood:

On behalf of Lolcow LLC, I thank you for your letter of May 1, 2026, which you captioned a "Notice of Deficiency." In that letter, you characterized all of your subpoenas in this matter as "identical" and requested that we supplement our earlier individual written objections pertaining to each subpoena not later than May 15, 2026. You later agreed, in our conferral on May 14, 2026, to extend the time for a further response through May 18, 2026. I appreciate your cooperation.

We do not agree that our earlier written objections were deficient, and we incorporate them by reference here. However, we are happy to provide this letter to further clarify and amplify our objections, especially in light of the information we have discussed in the intervening days and at our meeting on May 14, 2026.

Additionally, you will find enclosed with this letter redacted documents which we assert are responsive to your subpoenas. These documents are being provided in redacted form in order to facilitate our discussions, and are being provided in redacted form so that you can see what sort of information we have that is being withheld. Without waiving any other objections, our position is that searching for or producing other documents than those enclosed herewith would be unduly burdensome, and that producing the material which is redacted in the attached documents is impermissible for the reasons set forth herein and in our previous correspondence.

As another preliminary matter, I note that counsel for most of the subscribers whose identifying information you seek (Jay M. Wolman and Marc J. Randazza[1] of the Randazza Legal Group—have now entered their appearance in this matter). ECF No. 21. These counsel also participated in the May 14 meet and confer. Mssrs. Wolman and Randazza represent Doe 1 (a/k/a 3MMA), Doe 2 (a/k/a Sexy Senior Citizen), Doe 3 (a/k/a Diggus Bickus), Doe 4 (a/k/a Teriyakiburns), Doe 5 (a/k/a Dread First), Doe 6 (a/k/a The Mass Shooter Ron Soye), and Doe 7 (a/k/a GettrGrifter). Their engagement underscores the harm that your subpoenas threaten to cause

[1] As he indicated in our conferral last week, a motion for Mr. Randazza's appearance *pro hac vice* is forthcoming.

to First Amendment and Fair Use rights. Nothing in this letter should be taken to waive the rights of Kiwi Farms' users.

I. Defendant's Subpoenas Exceed the Statutory Purpose of § 512(h).

This is the central problem with your position, and it became unmistakably clear during the May 14 meet and confer. When pressed on why you are seeking identifying information for these users, you stated that you believe each user is a *witness* in the underlying litigation. You did not say (because you cannot say) that you intend to bring a separate DMCA infringement action against each user. That admission is fatal to the validity of these subpoenas.

A § 512(h) subpoena is not a general-purpose discovery device. It is a narrow statutory mechanism by which a copyright owner may obtain the identity of *an alleged infringer.* 17 U.S.C. § 512(h)(1). The statute requires a sworn declaration "to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title." 17 U.S.C. § 512(h)(2)(C).[2] At the conferral meeting, your paralegal, Ms. Tewson, focused on only the final clause of that statutory provision – "for the purpose of protecting rights under this title" – but made no accounting for whether Defendant alleges that the individuals whose identities are sought are the identities of "alleged infringer[s.]" If they are not alleged to have infringed and are mere witnesses, § 512 (h) does not authorize a subpoena.

You have told us plainly that you do not seek identifying information in order to bring copyright claims against the individual users. Instead, you seek identifying information of your client's anonymous critics because you want witnesses. That is a purpose for which § 512(h) subpoenas simply are not available. Every federal circuit to have addressed the scope of § 512(h) has emphasized its limited, targeted nature. The D.C. Circuit in *Recording Industry Ass'n of America v. Verizon Internet Services*, 351 F.3d 1229 (D.C. Cir. 2003), held that the subpoena power is structurally linked to identifying infringers, not to general information-gathering. The Eighth Circuit in *In re Charter Communications, Inc.*, 393 F.3d 771 (8th Cir. 2005), agreed. And just last year, the Ninth Circuit in *In re Subpoena of Internet Subscribers of Cox Communications,*

[2]On information and belief, we assert that the KUSK firm and/or its client have executed DMCA takedown notices and perhaps also sworn declarations in support of subpoena applications under penalty of perjury without conducting a meaningful review of the underlying material to determine whether the use in question actually constitutes infringement. Should this matter be litigated, we reserve the right to introduce evidence to that effect, which would undermine the credibility of the declarations filed in support of these subpoenas and may expose either the KUSK firm or its client to sanctions under Fed. R. Civ. P. 11, to liability under 17 U.S.C. § 512(f) for knowing material misrepresentation in a DMCA notification, or both.

LLC, No. 24-3978, 2025 WL 2371947 (9th Cir. Aug. 15, 2025), reaffirmed that § 512(h) is not a general discovery mechanism.[3]

Your use of these subpoenas to identify persons you yourself describe as "witnesses" is precisely the kind of overreach these courts have warned against. If you wish to identify witnesses, you may do so through the ordinary discovery mechanisms of the Federal Rules of Civil Procedure. Notably, this can only take place after a Rule 26(f) conference, after the parties have exchanged initial disclosures, and subject to all the procedural protections those Rules provide. Defendant cannot commandeer a streamlined, *ex parte* statutory mechanism intended solely for identifying alleged infringers and repurpose it as a shortcut to avoid those protections.

II. Defendant's Motives are Both Relevant and Probative.

Defendant devoted a section of the "Deficiency Notice" letter to the proposition that our client's characterization of Ms. Fong-Jones's motives is "both inaccurate and irrelevant." We disagree on both counts, but the relevance point is the more important one. We note that we remain unclear, even after our conferral, whether Defendant believes the DMCA subpoenas are a general purpose discovery device governed by Rule 45 or something governed by a special set of rules. But regardless of which theory Defendant ultimately proceeds under, motive matters here.

If the subpoenas are what Defendant sometimes claims they are — DMCA subpoenas issued under 17 U.S.C. § 512(h) — then the statute requires a sworn declaration that the information sought "will only be used for the purpose of protecting rights under this title." 17 U.S.C. § 512(h)(2)(C). A well-documented pattern of using copyright mechanisms to unmask and retaliate against anonymous critics (rather than to vindicate any actual copyright interest) goes directly to whether that statutory condition is satisfied. Evidence that the real purpose is to "doxx" users, to get them fired, or to impose costs on a disfavored platform is not mere background noise; it is evidence that the sworn declaration does not mean what it says. Courts evaluating DMCA subpoenas have expressly held that motive is relevant. In *In re DMCA § 512(h) Subpoena to Twitter, Inc.*, 608 F. Supp. 3d 868 (N.D. Cal. 2022), the court quashed a § 512(h) subpoena in part because unmasking the anonymous user risked exposing him to "economic or official retaliation" by the subpoena's proponent (even assuming a prima facie case of infringement had been made). And in *In re DMCA Subpoena to Reddit, Inc.*, 441 F. Supp. 3d 875 (N.D. Cal. 2020), the court similarly acted to protect anonymous critics when they were sued by a religious organization. These cases are impossible to square with your bare assertion that your own client's (improper) motives are irrelevant.

But if the subpoenas are instead what Defendant sometimes alternatively claims they are (general discovery subpoenas governed by the Federal Rules) then motive matters for a different

[3] *See Recording Indus. Ass'n of Am., Inc. v. Verizon Internet Servs.*, 351 F.3d 1229, 1233-35 (D.C. Cir. 2003); *Recording Indus. Ass'n v. Charter Communs., Inc.* (*In re Charter Communs., Inc.*), 393 F.3d 771, 776-77 (8th Cir. 2005); *In re Subpoena of Internet Subscribers of Cox Commc'ns, LLC,* No. 24-3978, 2025 WL 2371947 (9th Cir. Aug. 15, 2025).

but equally fatal reason. Discovery must not be "interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation." Fed. R. Civ. P. 26(g)(1)(B)(ii). A retaliatory or harassing purpose renders the discovery abusive and disproportionate to the needs of the case under Fed. R. Civ. P. 26(b)(1). At this early stage of the litigation, with no responsive pleading filed and no issues joined, sweeping subpoenas aimed at identifying every anonymous poster who modified and criticized a particular photograph are difficult to justify under any proportionality analysis. They become impossible to justify when the evidence shows that the true aim is not to advance a copyright claim but to punish critics. Defendant cannot escape scrutiny of unsavory motivations by declaring them irrelevant. Under either procedural framework Defendant invokes, they are central.

III. Defendant's Position on Applicable Procedure is Internally Contradictory, and Service is Defective Under Either Theory.

Your deficiency letter occupies an incoherent middle ground on the question of what procedural rules govern these subpoenas. When it suits Defendant's argument, you insist that the subpoenas are issued under § 512(h) and that the DMCA provides its own service mechanism (delivery to the designated agent, accompanying or subsequent to a DMCA takedown notification). But when you want to hold our objections to a particular standard, you pivot to Rule 34(b)(2)(B)–(C) of the Federal Rules of Civil Procedure and cite *Fischer v. Forrest* for the proposition that our objections must meet the specificity requirements governing responses to requests for production between parties.[4]

Regardless of what label the Defendant applies to these subpoenas, the subpoenas actually served are on Form AO 88B (the standard form commanding production under Fed. R. Civ. P. 45) and they attach Rule 45 provisions. The applicable framework for objections is therefore Rule 45(d)(2)(B), and for privilege, Rule 45(e)(2)(A). Rule 34, which governs requests for production served between parties to litigation, is inapplicable. To the extent Defendant demands Rule 34-compliant objections, any reliance on that rule is misplaced.

As to service: if the Federal Rules govern (as the subpoena forms themselves suggest), then service must satisfy Rule 45(b)(1), which requires "delivering a copy" to the person to whom it is directed. The majority of courts interpret this as requiring personal service.[5] I am neither Lolcow

[4]Defendant's "deficiency" letter applies the standard of Fed. R. Civ. P. 34(b)(2)(B)–(C) and cites *Fischer v. Forrest*, 2017 WL 773694, at *3 (S.D.N.Y. Feb. 28, 2017), which addresses specificity requirements for objections to requests for production under Rule 34. But Rule 34 governs requests for production served between parties. These subpoenas—whatever their statutory basis—are not requests for production. The applicable framework for objections is Rule 45(d)(2)(B), and for privilege, Rule 45(e)(2). To the extent Defendant invokes Rule 34, it is the wrong rule.

[5]Most courts interpret Rule 45(b)(1)'s "delivering a copy" as requiring personal service. *See Concepts NREC, LLC v. Xuwen Qiu*, No. 5:20-cv-133, 2021 U.S. Dist. LEXIS 252822 (D. Vt. Sep. 20, 2021).

LLC's registered agent for service of process nor have I consented to accept service of compulsory process in my capacity as DMCA agent. Delivery via ECF or email to a DMCA agent does not satisfy Rule 45(b)(1).

Nor does the text of § 512(h) support your service theory as cleanly as you suggest. Section 512(h)(4) provides that the clerk shall "return [the subpoena] to the requester for delivery to the service provider." Section 512(h)(5) states that the subpoena is "authorize[d]" to be delivered "either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A)." You read this to mean that delivery to the DMCA agent suffices. But we would note that the statute says delivery to the *service provider*, not to the *designated agent*. A DMCA agent is designated for the limited purpose of receiving takedown notifications—not all compulsory legal process. A subpoena is not a takedown notice. Further, you admitted in an April 21, 2026 email to me that you rely entirely upon the clerk's ECF entry in support of the theory that the April 3, 2026 subpoena was served. Clearly, *the requester* made no effort at all to deliver that subpoena to the service provider or to anyone else after it was returned by the clerk.

IV. To the Extent these Subpoenas Seek Discovery in the Pending Case, they are Premature.

Your own statements in the May 14 meet and confer confirm what we have argued from the outset: that these subpoenas are a vehicle for premature discovery. You acknowledged that you seek user-identifying information because you regard each user as a potential witness in the underlying litigation. You did not claim (and the facts do not support such any hypothetical claim) that you intend to pursue separate copyright infringement actions against each user.

If the subpoenaed information is sought for use in the pending case (as your own statements confirm) then the ordinary rules apply. Discovery in a civil case does not commence "before the parties have conferred as required by Rule 26(f)." Fed. R. Civ. P. 26(d)(1). No Rule 26(f) conference has occurred. No responsive pleadings have been filed. The issues in dispute are undefined. Using a DMCA subpoena to circumvent these basic procedural requirements is improper. If, on the other hand, Defendant is truly pursuing standalone § 512(h) identification of alleged infringers, then the court will focus on § 512(h)'s statutory prerequisites and the *Arista*/*Sony Music* balancing—under which, as set forth below, Defendant's position fares no better.

We note that we stipulated to extend the deadline for your client's responsive pleading through June 22, 2026. ECF No. 11.[6] No answer has been filed, no counterclaim has been stated, and no affirmative defenses have been raised. At this juncture, neither side even knows what will

[6] At our May 14 meeting, I further agreed to an additional week. While you have not yet filed such a request with the clerk, it has already been agreed as between us that June 29, 2026 is a responsive pleading deadline to which the Plaintiff consents.

be at issue in this case. The idea that identifying every anonymous poster who has used a particular photograph is proportionate to the present needs of this case is difficult to credit.

V. The *Arista* Factors Weigh Against Disclosure.

Your deficiency letter applies the five-factor test from *Arista Records, LLC v. Doe 3*, 604 F.3d 110, 116 (2d Cir. 2010) (adopting the *Sony Music* framework), and claims that all five factors favor disclosure. We disagree. A careful application of the factors, informed by the record that now exists, demonstrates that the balance tips decisively against unmasking these anonymous speakers. *See also Strike 3 Holdings, LLC v. Doe*, 740 F. Supp. 3d 121 (D. Conn. 2024) (applying the *Arista*/*Sony Music* framework).

Factor 1: Concreteness of the prima facie claim.

You assert that your client has registered a copyright and that the works were published without consent, and that this alone satisfies the first factor. We do not dispute that your client holds a registration. But the first factor does not ask merely whether a registration exists. It asks about the *concreteness* of the showing of *actionable harm*. *Sony Music Ent. Inc. v. Does 1–40*, 326 F. Supp. 2d 556, 565 (S.D.N.Y. 2004). Where the allegedly infringing use is plainly fair use, there is no actionable harm and no concrete prima facie claim. The court in *In re DMCA Section 512(h) Subpoena to YouTube (Google, Inc.)*, 581 F. Supp. 3d 509, 518 (S.D.N.Y. 2022), held exactly this: that where a fair use defense is apparent on the face of the record, the subpoena is not authorized under the DMCA.[7] The images at issue here are, virtually without exception, transformative commentary. They may in a general sense resemble a professional portrait, but the resemblance is not intended to replicate its commercial function. Instead, the intent is to criticize, mock, and comment upon the public conduct of the person depicted. That is the heartland of fair use under 17 U.S.C. § 107.

Factor 2: Specificity of the discovery request.

Your subpoenas are not narrowly tailored. They do not merely request the name and address of each user, or even information which could arguably be used to obtain the name and address of each user (such as an IP address or email address). Instead, Defendant's subpoenas define "Kiwi Farms" to encompass multiple separate legal entities (Mad at the Internet LLC and

[7] I*n re DMCA Section 512(h) Subpoena to YouTube (Google, Inc.)*, 581 F. Supp. 3d 509, 518 (S.D.N.Y. 2022).

the United States Internet Preservation Society[8])—and request "Subscriber Information" and "Transactor Information" spanning years of financial and account records. The breadth of these requests is inconsistent with the narrow identification purpose of § 512(h), which authorizes disclosure only of "information sufficient to identify the alleged infringer." 17 U.S.C. § 512(h)(3). The statute is not a license to rummage through a service provider's entire financial history.

Factor 3: Absence of alternative means.

You argue that because users are pseudonymous, there is no alternative means to obtain identifying information. But this factor is not a rubber stamp. Where the purpose of the subpoena is not to identify an infringer for a copyright claim, but rather to identify a witness for use in existing litigation, ordinary discovery mechanisms are the appropriate alternative means. Those mechanisms include interrogatories, depositions, and document requests directed at parties. All of these mechanisms will be available once discovery commences. That those mechanisms are not yet available is a product of the early stage of the litigation, not a justification for end-running the rules.

Factor 4: Need for the subpoenaed information to advance the claim.

This factor asks whether the information is needed to advance a copyright claim against the identified infringer. But you have conceded that you are not pursuing copyright claims against these users, and stated that you regard them as witnesses. The fourth factor therefore cuts squarely

---

[8] Defendant's attempt to sweep Mad at the Internet LLC and the United States Internet Preservation Society into the "Definitions" section of a subpoena directed to Lolcow LLC is procedurally improper and substantively baseless. A Rule 45 subpoena commands production from the person or entity to whom it is directed and from no one else. Fed. R. Civ. P. 45(a)(1)(A)(iii). One cannot bootstrap separate legal entities into the scope of a subpoena through the expedient of a definitions clause. Mad at the Internet LLC and the United States Internet Preservation Society are distinct limited liability companies, each with its own separate legal existence. *See Wm. Passalacqua Builders, Inc. v. Resnick Developers S., Inc.*, 933 F.2d 131, 139 (2d Cir. 1991) (respecting corporate separateness absent a showing of alter ego). If Defendant wishes to obtain documents from those entities, the path is straightforward: Defendant must serve separate subpoenas on each of them, in compliance with Rule 45(b)(1), and afford each entity the opportunity to raise its own objections under Rule 45(d)(2)(B). What Defendant may not do is serve Lolcow LLC and then, by definitional fiat, purport to impose obligations on entities that were never served, never consented to production, and have had no opportunity to be heard. The Second Circuit's framework for "possession, custody, or control" under Rule 45 requires, at a minimum, that the subpoena recipient have either a legal right to demand the documents from the affiliated entity or, under the broader formulation, a "practical ability" to obtain them. *See In re NTL, Inc. Sec. Litig.*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007). Defendant has made no such showing. The mere fact that these entities may have partially overlapping membership or management does not establish alter-ego status or impute "control" for discovery purposes. Lolcow LLC object to the inclusion of these entities in the subpoena definitions and will not produce documents on their behalf. Because Lolcow LLC does not have possession, custody, or control of the documents of these non-parties, or the "practical ability" to direct the actions of these non-parties, Lolcow LLC cannot provide any accounting for what documents may or may not exist in their possession.

against Defendant: information sought for witness identification, rather than to advance a copyright claim against the person being identified, does not satisfy this element of the *Arista* test.

Factor 5: Expectation of privacy.

This factor requires consideration of two related but distinct interests: Lolcow LLC's interest as a corporate entity, and the users' interest as anonymous speakers. Lolcow exists in large part because it protects the anonymity of its users and hosts a forum for anonymous online criticism and expression. Similarly, the users have their own interest in engaging in the anonymous speech that Lolcow LLC fosters.

As to the users: they are the persons whose anonymity is at stake, and their expectation of privacy in anonymous online speech is substantial and protected by the First Amendment. *McIntyre v. Ohio Elections Commission*, 514 U.S. 334, 342 (1995). The users' interest is no longer abstract: most are now represented by counsel who have entered an appearance for the express purpose of opposing these subpoenas. *See also In re DMCA § 512(h) Subpoena to Twitter, Inc.*, 608 F. Supp. 3d 868, 876 (N.D. Cal. 2022). The *Arista* framework is designed to protect precisely this interest—the anonymity of speakers whose speech may be protected.

As to Lolcow LLC: it has independent grounds to resist. These include its own First Amendment rights as well as any express or implied contractual and statutory duties to its users, the undue burden of the subpoenas, and the improper purpose for which the subpoenas were issued. We note that *Arista*'s anonymity-protection rationale applies to subpoenas "designed to breach anonymity," 604 F.3d at 118, regardless of whether the service provider itself asserts a personal privacy interest.

You cite the Kiwi Farms Terms of Service provision that content "may be reviewed by staff members" and "may be sent to third-party verification services" as evidence that users have abandoned their privacy expectations. This is a remarkable stretch. A platform's reservation of the right to moderate content or use spam-filtering services is not remotely equivalent to a blanket waiver of the right to anonymous speech. Every major platform reserves similar rights. If this were sufficient to extinguish anonymity, then no user of any internet service would ever enjoy First Amendment protection. To our knowledge, no court has ever endorsed such a novel proposition.

As to your demand that we demonstrate the citizenship of each user: Lolcow LLC cannot certify the citizenship or location of pseudonymous users whose identities it does not know, but it is a natural proposition that a West Virginia LLC with its servers in the United States will expect to primarily serve American citizens. We note that the burden of establishing that a subpoena is proper rests with the party seeking to compel disclosure, not with the party resisting it.[9] Neither *Arista* nor its progeny impose a threshold citizenship-showing requirement on the party asserting a First Amendment interest before the balancing test even applies. Even assuming, arguendo, that one or more users is not an American citizen, citizenship or lack thereof is only one consideration within the fifth factor and is not dispositive. Defendant's citation to *In re Gliner*, 133 F.4th 927

[9]*See Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc.*, 591 U.S. 430, 433 (2020).

(9th Cir. 2025) has almost no bearing in the DMCA context: that case involved 28 U.S.C. § 1782 discovery for foreign litigation. Naturally, the First Amendment applies differently in such a case than it does in one directly involving expressive activity on an American website.

VI. The Fair Use Defense is Apparent on the Record.

Defendant, in the May 12, 2026 letter to Mr. Wolman, undertakes an image-by-image analysis of the fair use question. We appreciate the detail you have provided. We disagree with virtually every conclusion.

The images at issue are critical commentary on a public figure's conduct and public statements. They resemble a professional portrait in a general sense but contain extensive alterations and are not intended to serve the commercial purpose for which it was created. Instead, they use that resemblance as raw material for satire, mockery, and commentary on the subject's public behavior. That is transformative use under 17 U.S.C. § 107. The first statutory factor—"the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes"—favors the users, because their use is noncommercial critical commentary, not commercial exploitation. The fourth factor—"the effect of the use upon the potential market for or value of the copyrighted work"—likewise favors the users, because critical commentary on a forum does not substitute for or impair the market for licensed uses of a professional portrait.

The *Andy Warhol Foundation for the Visual Arts v. Goldsmith* decision, 598 U.S. 508, 143 S. Ct. 1258 (2023), does not change this analysis in the way your client suggests. *Warhol* held that where a secondary use shares the same *purpose and character* as the original (there, a magazine illustration licensing a portrait for the same editorial function) the first factor weighs against fair use. But the uses here do not share the same purpose. The underlying portrait was created as a flattering professional depiction. These posts use it as the basis for ridicule and critical commentary. A hostile editorial purpose directed at the subject of a photograph is a materially different purpose than the flattering commercial depiction for which the photograph was created. *See also Hachette Book Grp., Inc. v. Internet Archive*, 115 F.4th 163 (2d Cir. 2024) (analyzing transformative use in the Second Circuit post-*Warhol*).

Moreover, a court in this very district has already held, in an analogous case, that where a fair use defense is apparent on the face of the record, a DMCA subpoena is not authorized. *In re DMCA Section 512(h) Subpoena to YouTube (Google, Inc.)*, 581 F. Supp. 3d at 518. We are confident that the same result would obtain here.

VII. The Pattern of Conduct Supports a Finding of Copyright Misuse.

The broader pattern here is one of using copyright law as a pretext to unmask anonymous critics rather than to vindicate any legitimate copyright interest. Your client has a well-documented history of efforts to deplatform Kiwi Farms, to "doxx" its users, and to impose costs on anyone associated with the platform. These facts were set out in our earlier correspondence and are

incorporated by reference here. When copyright is wielded not to protect creative works but to silence speech, the doctrine of copyright misuse provides an affirmative defense.[10]

That your client's real purpose is to identify and retaliate against critics rather than to enforce copyright is further confirmed by your own admission that the users are sought as witnesses, not as defendants. The copyright subpoena mechanism is being deployed for a non-copyright purpose. That is misuse.

We reserve all rights to seek relief for copyright misuse either by way of an appropriate motion or through an amendment to our complaint.

VIII. Response to Specific Claims in the Deficiency Letter.

A. Waiver.

You assert that our objections are deficient and threaten that they will be "deemed waived." As noted above, these subpoenas command production and are governed by Rule 45—not Rule 34. But even under Rule 45(d)(2)(B), our objections are more than sufficient. The cases you cite—principally *Fischer v. Forrest*, 2017 WL 773694, at *3 (S.D.N.Y. Feb. 28, 2017)—addressed boilerplate objections that failed to state *any* specific grounds. Our objections—spanning multiple detailed letters—state their grounds with particularity: fair use, First Amendment protection, improper service, premature discovery, undue burden, overbreadth, and the statutory limitations of § 512(h). These are not boilerplate. They are substantive. And they are not waived.

B. Possession, Custody, and Control.

You assert that all documents in the custody of Lolcow LLC, Mad at the Internet LLC, and USIPS are within the control of Joshua Moon and therefore producible by Lolcow. We have consistently maintained that Mad at the Internet LLC and the United States Internet Preservation Society are separate legal entities. Whether Mr. Moon has a relationship with those entities does not make their records "in the possession, custody, or control" of Lolcow LLC within the meaning of the Federal Rules. In any event, these subpoenas were directed at Lolcow LLC, and Lolcow LLC can only produce what Lolcow LLC possesses.

C. Burden and Privilege.

You demand that we articulate the burden with specificity and provide an affidavit. We have explained the burden: your subpoenas define terms so broadly as to sweep in records of multiple separate entities and demand "Transactor Information" that would require manually reviewing Lolcow LLC's entire financial history to associate payments with particular users. That is a burden we have described with reasonable particularity.

[10] *See Coleman v. ESPN, Inc.*, 764 F. Supp. 290, 295 (S.D.N.Y. 1991) (recognizing the doctrine of copyright misuse).

As to privilege: consistent with Rule 45(e)(2)(A), we have identified attorney-client privilege and work product as applicable to categories of documents your subpoena's definitions would reach (specifically, communications between counsel and client, and materials prepared in anticipation of litigation). To the extent specific documents are withheld on the basis of privilege, we will describe the nature of the withheld documents in sufficient detail to enable an assessment of the claim, as Rule 45(e)(2)(A) requires. We remain willing to prepare a privilege log for any reasonably disputed subset of documents if you narrow your requests to materials actually in the custody of Lolcow LLC.

Without in any way waiving the objections set forth above: even if your subpoena were otherwise permissible, *arguendo*, the statute only authorizes you to obtain "information sufficient to identify the alleged infringer." 17 U.S.C. § 512(h)(3). Lolcow LLC acknowledges that it possesses the IP address and email address for each subscriber whose information you have subpoenaed other than "Lollardy." Lolcow LLC possesses the email address, only, for "Lollardy." Lolcow LLC's custodian of records is familiar with the records management practices of his organization and is aware that Lolcow LLC does not maintain the name or address for any users, including but not limited to the users whose information you have requested, in any format (including but not limited to in its financial records). Any search for such information would therefore be futile. To the extent that Lolcow LLC possesses "information sufficient to identify" the users, such information is limited to the website logs which identify the email address and/or email address for each user.

You specifically requested in your "Deficiency Notice" that Lolcow LLC identify with greater specificity the documents it is withholding and the reason(s) for such withholdings. Without waiving our objections, we are enclosing with this letter, in redacted form, the information Lolcow LLC maintains in its custody which is sufficient to identify the users in question. The information we are withholding is identified and is placed behind the redactions. Any additional information we would possess, in any location, would be duplicative or would not identify the users in question. As indicated above, financial records are not maintained in a fashion that allows payments to be sourced to individual subscribers. Any contact that individual users have made with Lolcow LLC has been conducted pseudonymously, using the username and/or email address on file, rather than via any mechanism which would identify the user.

X. Conclusion.

Defendant's subpoenas are an attempt to use a narrow statutory mechanism for a purpose it was never intended to serve. Your own admissions in the May 14 meet and confer confirm that you seek this information to identify witnesses, not to bring copyright claims against the persons whose identities you seek. That is not what § 512(h) is for. Your position on what procedural rules apply is internally contradictory. The *Arista* factors, properly applied, weigh against disclosure. The underlying uses are fair use. And the broader pattern of conduct raises serious concerns about copyright misuse.

Lolcow LLC does not withdraw any of its objections. We stand ready to meet and confer further, and we understand that Messrs. Wolman and Randazza intend to move to quash on behalf of the individual users. We reserve all rights to join in that motion or to file our own, to seek a protective order, or to pursue any other relief to which we may be entitled.

Nothing in this letter should be construed as a waiver of the First Amendment rights of Lolcow LLC or any of its subscribers, or of any other objection, defense, or right not expressly addressed herein.

Very truly yours,

Matthew D. Hardin
Counsel for Lolcow LLC

cc: Jay M. Wolman, Esq., Randazza Legal Group, PLLC
Marc J. Randazza, Esq., Randazza Legal Group, PLLC

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LOLCOW LLC,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 1:26-cv-2059
	)	
ZHEN ELIZABETH FONG-JONES,	)	
	)	
Defendant.	)	

DECLARATION OF JOSHUA MOON

NOW COMES Joshua Moon, and declares as follows:

1. I am an adult resident, citizen, and domiciliary of the United States. I am competent to testify to the matters set forth herein based upon my personal knowledge and my knowledge as the custodian of records for Lolcow, LLC.

2. I make this declaration to explain the burdens that Lolcow, LLC would face in responding to subpoenas in this matter, including the technical steps, burdens, and time that searching for the requested records would require. For reasons more fully set forth below, I also believe that any burden of searching for records responsive to the subpoenas would likely be futile, because of the likely content of any records that do exist.

3. I also make this declaration to explain that Lolcow, LLC is not affiliated with and does not control two other entities: Mad at the Internet LLC and the United States Internet Preservation Society.

4. I am the sole member and the Custodian of Records for Lolcow, LLC, a West Virginia limited liability company which operates the Kiwi Farms website and forum.

5. I am the sole member of Mad at the Internet LLC, but that entity is not a subsidiary of Lolcow, LLC or in any way associated with Lolcow, LLC. The two entities are separately managed and maintain separate corporate records.

6. I am one of three board members for the United States Internet Preservation Society, which is a South Dakota nonprofit corporation recognized under Section 501(c)(4) of the Internal Revenue Code. That entity is not a subsidiary of Lolcow, LLC or in any way associated with Lolcow, LLC. The two entities are separately managed and maintain separate corporate records. Indeed, as a nonprofit entity, the United States Internet Preservation Society cannot be controlled by a for-profit entity or serve for-profit purposes.

7. Lolcow, LLC's website, known as Kiwi Farms, is a pseudonymous discussion forum. With very few exceptions, users do not participate under their legal names. The site's operational

design and community norms strongly favor compartmentalized identities and minimization of personally identifying information.

8. Kiwi Farms warns users during registration that the site is controversial and that some people try to identify or harass users. Users are advised to use an identity separate from their real identity and from accounts used elsewhere, to use a username they have never used before, to use an email address not tied to their real name or other accounts, not to reuse avatars or personal details, and to use VPN or Tor where network-level separation is needed.

9. Kiwi Farms is operated as a privacy-first website. As a matter of policy and security design, Kiwi Farms retains as little user-identifying information as practicable.

10. This minimization policy exists because Kiwi Farms and its users have been targeted by hackers, activists, and other adversarial actors seeking confidential identifying user information, including email addresses and IP addresses.

11. Kiwi Farms has previously been compromised. In or around 2019, a compromise resulted in exfiltration of user email addresses. That incident harmed user trust and caused substantial disruption to the community of users who patronize the site. Kiwi Farms was also compromised in or around 2022. Following these incidents, Kiwi Farms adopted stricter data-minimization and retention practices.

12. Kiwi Farms' security posture is based on the principle that, even in a worst-case compromise, there should be as little sensitive user-identifying information as possible available to steal.

13. Kiwi Farms provides and encourages privacy-protective access methods. The site is Tor- and VPN-friendly. The site provides onion access, including through Onion-Location headers and links on the site.

14. Kiwi Farms has at times required users from certain locations to use Tor rather than clearnet access when necessary for security or user protection.

15. Kiwi Farms does not treat an IP address as a reliable identifier of a real-world person. An IP address may reflect Tor, a VPN, a proxy, a shared network, mobile carrier infrastructure, public Wi-Fi, a workplace, a school, or other intermediary infrastructure.

16. Kiwi Farms retains IP logs for only a short period in ordinary operation, generally approximately two weeks or less depending on operational and security conditions.

17. Other server, firewall, reverse-proxy, or technical logs are not maintained as long-term account-identification records and may be retained for as little as approximately 24 hours.

18. Historical IP information, to the extent it exists at all beyond ordinary retention periods, would generally exist only incidentally inside encrypted database snapshots or backups. Those backups are not indexed or searchable for ordinary account-lookup purposes.

19. Restoring historical backups to search for isolated user records would require substantial technical work, including downloading, decrypting, and restoring large database snapshots. Kiwi Farms' database contains hundreds of millions of rows and occupies hundreds of gigabytes. Restoring the entire database to a duplicate location with all records necessary for the searches requested would require either building new custom software specifically for that purpose or expanding existing hardware infrastructure to accommodate a separate,

secure copy of the database. That has never been done before. Backups have only been restored in-place to replace a broken copy of the site where the site was already running.

20. Restoring and searching backups would also create new sensitive copies of user data, including unrelated user data, thereby increasing the very security risks Kiwi Farms' retention practices are designed to avoid.

21. Kiwi Farms' on-site direct-message conversations automatically delete after 30 days of inactivity. Once pruned from the live system, those conversations are not recoverable by administrators through ordinary administrative tools.

22. The direct-message auto-delete feature is automatic. Users can see countdown notices indicating when inactive conversations will be deleted.

23. Kiwi Farms receives donations and payments by several methods, including checks, money orders, cryptocurrency, account credits, and user-to-user sponsored payments.

24. Kiwi Farms users often pay for other users. It is common for one person to provide payment or credit for multiple usernames. Therefore, a payment associated with an account benefit does not establish that the recipient account holder made the payment.

25. Kiwi Farms' internal account-credit system generally does not identify whether a payment came from a check, money order, cryptocurrency, third-party sponsorship, or manual credit, except in limited circumstances such as cryptocurrency-related rewards.

26. Mail-in checks and money orders are commonly sent without reliable identifying information. Users may provide only the recipient account details, may omit sender information, may use names that do not correspond to the account holder, or may send funds on behalf of someone else.

27. Mail-in payments are not retained as account-linked copies by Lolcow, LLC. Checks and money orders are not scanned, photographed, or copied by Lolcow, LLC in the ordinary course after payment is applied.

28. Deposit information received from the bank generally reflects aggregate deposit totals, not account-linked copies of individual checks or money orders.

29. Cryptocurrency payments do not identify a real-world payor. Cryptocurrency transaction data, even where retained, does not establish the legal identity of the person associated with a Kiwi Farms account.

30. Searching historical financial records for the subpoenaed information would be burdensome, unreliable, and likely to expose unrelated donors and supporters. I do not hold all financial records that might theoretically be relevant to the requests, and I do not know whether my bank keeps photocopies or images of checks, money orders, or other payment instruments. In ordinary operation, the deposit records available to me are simple deposit slips that reflect aggregate deposit information and do not contain the payment information necessary to link a payor, payee, or payment instrument to a particular Kiwi Farms user account. I estimate that even attempting such a search would take tens or possibly hundreds of hours of my time, and I am the only individual who has access to the necessary internal systems. Ultimately, the information uncovered in such a search would not likely identify any user because of the lack of a reliable connection between any payment and any individual user.

31. Kiwi Farms receives a large volume of email across multiple providers and systems, including Gmail, Proton Mail, and self-hosted mail systems.

32. I receive at least approximately 100 emails per week related to Kiwi Farms and related matters. These emails are not consistently organized by user account, legal name, donor identity, or subpoena target.

33. Users virtually never identify themselves to me by legal name. Kiwi Farms users are encouraged not to disclose unnecessary identifying information, including to me.

34. Some communications are encrypted. Kiwi Farms provides PGP-enabled methods for secure communication.

35. Searching years of email across multiple accounts for possible identity clues would be extraordinarily burdensome, likely requiring tens or possibly hundreds of hours of my time, and unlikely to produce reliable identifying information. It would also risk exposing private communications from hundreds or thousands of unrelated persons.

36. Defendant has publicly targeted Kiwi Farms' infrastructure and security posture.

37. Attached as Exhibit A is a true and correct copy of the README.md from a public GitHub repository the public commit history of which attributes all commits to Defendant (who uses the name “Liz Fong-Jones” and the GitHub accounts identified below). The repository is currently located at https://github.com/endharassment/tor-fetcher, was previously located at https://github.com/lizthegrey/tor-fetcher, and the redirect from the previous location has been archived at https://archive.is/6VHkM. The repository targets multiple security systems used by Kiwi Farms, including “haproxy-protection,” “BasedFlare,” and Tartarus.

38. Tartarus is a security system that I developed. To my knowledge, Tartarus is not a generally deployed third-party security product and is generally associated with Kiwi Farms.

39. Defendant has engaged in a sustained, public course of conduct directed at Kiwi Farms and its infrastructure. Among other things, Defendant has organized and personally appeared at efforts to persuade Kiwi Farms' service providers to terminate service to the site, and has delivered a public presentation at Oxford addressing litigation against persons associated with the forum. Defendant is also the author of the tor-fetcher software attached as Exhibit A, the public commit history of which attributes all commits to Defendant, and which is designed to complete the proof-of-work and related security mechanisms used by Kiwi Farms in order to retrieve content from the site.

40. Based on the foregoing, including Tartarus's limited deployment, its association with Kiwi Farms, and the function of the tor-fetcher software, the targeting of Tartarus is consistent with an effort to retrieve data from Kiwi Farms by bypassing the site's security mechanisms.

41. The conduct described above reflects a pattern in which Defendant has repeatedly targeted Kiwi Farms, sought to strip it of security services, and then targeted the security systems Kiwi Farms was able to develop or assemble for itself.

42. Because of this history, production of broad user-identifying, donor-identifying, or security-sensitive information to Defendant or Defendant's counsel presents serious privacy, safety, and security concerns.

43. In my experience operating the site, users and supporters who are associated with their accounts or donations have been subjected to identification efforts, harassment, employment consequences, and other harm. Based on the site's history of compromise and the consequences described above, disclosure of identifying information creates a real risk of the same harm to the persons identified.

44. The subpoenas seek categories of information that are not maintained in a manner that reliably identifies the real-world persons behind pseudonymous accounts.

45. Email addresses may be aliases, forwarding addresses, disposable addresses, or otherwise unrelated to users' legal identities.

46. IP addresses may reflect Tor, VPNs, proxies, shared networks, or other infrastructure.

47. Payment information may reflect third-party sponsors, anonymous money orders, cryptocurrency transactions, or payments made on behalf of other users.

48. Postal or mailing information, where present on an envelope, check, or money order, may not belong to an account holder and may not be retained.

49. I am able to search live production systems for the exact account identifiers specified in the subpoenas. Such a search does not require the restoration, reconstruction, or archival-search steps described above. I have undertaken such a search, and have provided the records responsive to that search in redacted form, via my attorney.

50. Restoring encrypted historical backups, reconstructing old financial records, or searching years of unrelated email archives would impose the burdens described above and would necessarily create new copies of unrelated donor and user information. Even attempting to restore the relevant backups in a separate duplicate environment would likely require tens or possibly hundreds of hours of my time, new custom software or expanded hardware infrastructure, and the creation of a separate sensitive copy of a database containing hundreds of millions of rows and hundreds of gigabytes of data. This type of duplicate restoration and search environment has never previously been built or used by Lolcow, LLC; prior backup restorations have only been performed in-place to replace a broken copy of the site where it was already running.

51. Lolcow, LLC is willing to confer regarding a narrower process, including confirmation of whether current live account data exists, whether any live IP logs exist, and whether any non-identifying account metadata can be produced.

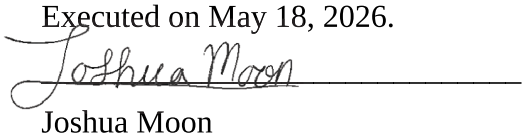
52. Based on the site's data-minimization design, its prior data breaches, and the consequences described above, the fact that the categories the subpoenas seek (including email addresses, IP addresses, and payment information) are precisely the categories that can be used to identify pseudonymous users, and the fact that Defendant is an adverse party in this litigation and a public advocate for the site's removal who authored the software attached as Exhibit A, I fear that compliance with a subpoena producing user-identifying information to Defendant would expose the site's users to identification and resulting harm. That concern applies to every user whose identifying information would be produced, because the records at issue are not maintained in a manner that reliably distinguishes any individual user from any other.

53. Any production of user-identifying information, if ordered, should be narrowly limited, redacted, and subject to strict safeguards, including sealing, attorneys'-eyes-only treatment, or in camera review.

54. Further I say nothing.

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

Executed on May 18, 2026.



Joshua Moon

Custodian of Records

Lolcow, LLC

EXHIBIT A

README.md from public GitHub repository currently located at https://github.com/endharassment/tor-fetcher; previously located at https://github.com/lizthegrey/tor-fetcher; redirect archived at https://archive.is/6VHkM.

tor-fetcher

Like curl, but for fetching .onion URLs that require "haproxy-protection"/"BasedFlare"/Tartarus PoW completion before access is granted.

Uses Golang's argon2 and sha256 libraries instead of running the Javascript/WebAssembly bundle.

Usage

```
tor-fetcher --target <url> [flags]
```

Flags

Flag	Default	Description
--target	(required)	The URL to retrieve
--proxy	socks5://127.0.0.1:9050	SOCKS5 proxy address for Tor
--ua	Firefox 140 on Windows	User-Agent string
--debug	False	Enable debug logging to stderr
-p	1	Argon2 parallelism
-l	32	Argon2 key length