

UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF MICHIGAN

MALIBU MEDIA, LLC,

Plaintiff,

v

JESSE RALEIGH,

Defendant.

Case No. **1:13-cv-00360-RJJ**

Hon. Robert J. Jonker

Mag. Judge: Hugh W. Brenneman

---

**Nicoletti & Associates, PLLC**

By: Paul J. Nicoletti (P44419)

Attorney for Plaintiff

36880 Woodward Ave., Suite 100

Bloomfield Hills, Michigan 48304

(248) 203-7800

[pauljnicolleti@gmail.com](mailto:pauljnicolleti@gmail.com)

**Blanco Wilczynski, PLLC**

By: Derek W. Wilczynski (P57079)

Attorneys for Defendant

2095 E. Big Beaver Rd., Suite 400

Troy, Michigan 48083

(248) 519-9000

[dsw@blancopc.com](mailto:dsw@blancopc.com)

**Lincoln G. Herweyer, PC**

By: Lincoln G. Herweyer (P55742)

Co-Counsel for Defendant

35054 Twenty-Three Mile Rd., Suite 115

New Baltimore, Michigan 48047

[lgherweyer@netscape.net](mailto:lgherweyer@netscape.net)

---

**DEFENDANT'S RESPONSE TO PLAINTIFF'S MOTION TO COMPEL  
AND INCORPORATED MEMORANDUM OF LAW**

**NOW COMES** Defendant Jesse Raleigh, by and through undersigned counsel, and Responds to Plaintiff's Motion to Compel, asking, *inter alia*, that this Court condition the discovery of Defendant's computer hard drives on a Protective Order, either as proposed to Plaintiff on February 27, 2014, or as settled on in a similar case pending in the Eastern District of Michigan (*Malibu Media v Shekoski*, ED MI 13-12217), where the same attorneys are litigating a similar case. Fed.

R. Civ. P. 37(a)(5) expressly provides that a party opposing a motion to compel may obtain a Protective Order pursuant to Fed. R. Civ. P. 26(c).<sup>1</sup>

More specifically, and as detailed in the accompanying brief in support, because of the personal and confidential nature of the information Defendant's hard drive, and because most or all of that information is irrelevant to the issues in this case, and because of the nature of Plaintiff and its industry-scale litigation and coercive settlement practices, Defendant wants the moral equivalent of an in camera inspection of his computer's hard drive, by using a licensed but neutral expert in computer forensics (paid for by Plaintiff) who can provide the information to both parties that is relevant to Plaintiff's claims, but who will not otherwise divulge the contents of Defendant's computer to Plaintiff or anyone else.

As early as February 27, 2014, Defendant's counsel proposed a procedure consistent with the relief requested in this motion. Plaintiff's counsel counter-proposed a protective order that simply protected the information from further disclosure, but which did nothing to address a number of concerns set forth in the accompanying brief.

Alternatively, Defendant Raleigh would request that at the very least the examination of this hard drives be subject to a Protective Order like the one mandated by Judge Roberts in the Shekoski case. Under the terms of such an order, Plaintiff would be responsible for the cost of making images (or "clones") of Defendant's hard drives, and the confidentiality of Defendant's hard drives would otherwise be protected.

**WHEREFORE**, Defendant respectfully requests that this Court **DENY** Plaintiff's Motion

---

<sup>1</sup> In the twin cases being (nearly) simultaneously litigated by these same attorneys on the same issues, the defense moved for a Protective Order in the *Shekoski* case on July 2, 2014. Malibu Media responded with a Motion to Compel in the *Raleigh* case on July 11, 2014. The only material difference between these cases is that the Defendant filed first in one, and the Plaintiff beat the Defendant to the punch in the other.

to Compel, and instead enter a Protective Order, limiting discovery, particularly with regard to Defendant's computer hard drive, to the procedures described in the accompanying supporting brief.

Respectfully submitted,

**Blanco Wilczynski, PLLC**

s/ Derek W. Wilczynski  
By: Derek W. Wilczynski (P57079)  
Attorneys for Defendant  
2095 E. Big Beaver Rd., Suite 400  
Troy, Michigan 48083  
(248) 519-9000  
[dsw@blancopc.com](mailto:dsw@blancopc.com)

**Lincoln G. Herweyer, PC**

s/ Lincoln G. Herweyer  
By: Lincoln G. Herweyer (P55742)  
Co-Counsel for Defendant  
35054 Twenty-Three Mile Rd., Suite 115  
New Baltimore, Michigan 48047  
[lgherweyer@netscape.net](mailto:lgherweyer@netscape.net)

**UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF MICHIGAN**

**MALIBU MEDIA, LLC,**

Plaintiff,

v

**GERALD SHEKOSKI,**

Defendant.

Case No. **2:13-cv-12217-VAR-RSW**  
Hon. Victoria A. Roberts

---

**Nicoletti & Associates, PLLC**  
By: Paul J. Nicoletti (P44419)  
Attorney for Plaintiff  
36880 Woodward Ave., Suite 100  
Bloomfield Hills, Michigan 48304  
(248) 203-7800  
[pauljnicolleti@gmail.com](mailto:pauljnicolleti@gmail.com)

**Blanco Wilczynski, PLLC**  
By: Derek W. Wilczynski (P57079)  
Attorneys for Defendant  
2095 E. Big Beaver Rd., Suite 400  
Troy, Michigan 48083  
(248) 519-9000  
[dsw@blancopc.com](mailto:dsw@blancopc.com)

**Lincoln G. Herweyer, PC**  
By: Lincoln G. Herweyer (P55742)  
Co-Counsel for Defendant  
35054 Twenty-Three Mile Rd., Suite 115  
New Baltimore, Michigan 48047  
[lgherweyer@netscape.net](mailto:lgherweyer@netscape.net)

---

**BRIEF IN SUPPORT OF  
DEFENDANT'S MOTION FOR PROTECTIVE ORDER REGARDING  
DEFENDANT'S COMPUTER HARD DRIVE**

**STATEMENT OF FACTS**

Pending before this Court is an action for direct copyright infringement, under 17 U.S.C. § 501, by Plaintiff Malibu Media LLC (“Malibu”) against Defendant Jesse Raleigh (“Defendant”).

Malibu is in the business of producing and distributing pornographic movies and, in cooperation with a German IT firm known (at least in this lawsuit) as IPP Limited<sup>2</sup> (“IPP”), is also a prolific, for-profit copyright infringement litigator that has, since 2012, filed over 1800 copyright infringement suits involving peer-to-peer filing sharing. Meanwhile, Defendant is a Software Engineer and former soldier who was previously tasked with maintaining and integrating military intelligence systems. While living in a multi-unit house in Petoskey, Michigan on weekends, and commuting to Grand Rapids during the week, Defendant maintained an “open” wireless internet service account for the specific benefit of his wife, but which was easily accessible by anyone else living in his multi-unit apartment house, or even by those in neighboring houses.

There are (and it practically goes with out saying) substantial non-infringing uses for internet service, so there is nothing even remotely unlawful in not password protecting a wireless router. In addition, Defendant was not even present in Petoskey when much of the alleged infringement was occurring, and is sophisticated enough that, had he wanted to engage in the downloading or uploading of copyrighted material, he could have done so without leaving footprints leading straight to his IP address. Malibu Media has sued the wrong person in this case, but acknowledging such mistakes is not within Malibu’s business plan.

Presently at issue before this Court is a controversy about the examination of the hard drive on Defendant’s computer(s). Understandably, given the nature of its case, Plaintiff wants to examine

---

<sup>2</sup> In some cases it files, Malibu refers to IPP as IPP International, UG.

Defendant's hard drive<sup>3</sup> in an effort to obtain evidence supporting its accusation that Defendant has used peer-to-peer file sharing to directly infringe the copyrights of its pornography. Presumably, Plaintiff would principally look for: the BitTorrent program, BitTorrent files, any usage indicating peer-to-peer file sharing, and any presence of allegedly infringed works. In order to facilitate its desire to poke around in Defendant's computer, Plaintiff proposes to have its paid expert spend up to an entire business day making an exact duplicate (image) of the hard drive on Defendant's computer, and thereafter have its expert spend "weeks if not months" conducting an examination of the contents of the image. Plaintiff proposes to protect Defendant by agreeing to a protective order that would prohibit Plaintiff from unnecessarily re-disclosing designated documents and information to third persons—provided that Defendant adheres to an onerous process of individually designating the confidentiality level of every document and item to be protected.<sup>4</sup>

From Defendant's perspective, however, the procedure contemplated by Plaintiff is needlessly invasive and lacks adequate safeguards, among other problems. In truth, Defendant welcomes the opportunity to demonstrate that he did not engage in peer-to-peer file sharing of Plaintiff's works, and fully expects that a forensic examination of his computer's hard drive will bear witness to that fact. Nonetheless, Defendant's computer hard drive is the repository of myriad documents and records that are of a private and confidential nature. These include (or may include): records regarding Defendant's and his family's banking transactions; their tax records and filings

---

<sup>3</sup> For the balance of this Brief, any reference to Defendant's computer hard drive (in the singular) should be understood to mean any and all computer hard drives that were in Defendant's home on a regular basis during the period of record infringement (as defined in the Complaint) and which are within Defendant's custody and control.

<sup>4</sup> As set forth in the body of the motion itself, and in compliance with both Fed. R. Civ. P. 26(c)(1) and E.D. Mich. LR 7.1(a), the parties attempted to resolve this disagreement through a proposal by Defendant and a counter-proposal by Plaintiff.

with the IRS and State of Michigan, their social security numbers and drivers license data; their mortgage payments and other bills; their purchasing habits and credit histories; their income and financial worth; school records; medical records; passwords of every kind, and private communications that were never intended to be revealed to third persons.

Moreover, Defendant understandably distrusts the particular persons who want to subject his confidential information to such exacting scrutiny. Defendant does not have the resources to monitor Malibu or IPP (the German IT firm on whose work Plaintiff's case is based) and hold them accountable should they violate the protective order contemplated by Plaintiff. Instead, Defendant would have to essentially *trust* them. Yet, pornographers with a industry-sized litigation practice of coercing settlements from blameless individuals do not instill the confidence necessary to such trust. Nor does a foreign IT company that may be a shell for a previously discredited firm instill such trust.<sup>5</sup> While Plaintiff may be heard to shout its own bona fides, one must remember that Defendant *knows* that he did not infringe Plaintiff's copyrights and, therefore, he *knows* that Plaintiff is the kind to sue innocent people and attempt (from his perspective) to extort money from them.

Further, Defendant fears what might be "planted" on his computer by an unlicensed imaging "expert" or what exculpatory evidence might be withheld by Plaintiff's forensic examiner in an effort to squeeze him for money. Since the imaging and examination would not have to be done twice if Defendant could both trust the results and have the same access to the results as Plaintiff, the procedure that Defendant proposes is far superior to that proposed by Plaintiff.

Finally, some accommodation must be made for the fact that what Plaintiff is proposing will itself constitute (or may constitute) one or more violations of law. That is, resident on Defendant's

---

<sup>5</sup> There is growing evidentiary support being presented in other Malibu cases that IPP is a new shell company for the pre-existing (but discredited) German company Guardaley Limited.

computer are many copyrighted works (e.g., computer programs that Defendant uses by license). It would be ironic indeed if Defendant were forced to actually abet copyright infringement in order to demonstrate that he had not previously done so. Moreover, in Michigan those who engage in computer forensic investigations for a fee must be licensed, and doing so without a license is a felony punishable by up to four years in prison. See MCL 338.822(b); MCL 338.822(e); MCL 338.823. Therefore, the individual paid to examine Defendant's computer hard drive should be licensed under MCL 338.821 *et seq.*

### ARGUMENT

**I. THIS COURT SHOULD ENTER A PROTECTIVE ORDER THAT LIMITS THE DISCOVERY OF THE CONTENTS OF DEFENDANT'S COMPUTER HARD DRIVE TO AN EXAMINATION BY A LICENSED AND INDEPENDENT EXAMINER, WHO CAN THEN DISCLOSE THE NECESSARY RELEVANT INFORMATION TO BOTH PARTIES IN ACCORDANCE WITH THE PROCEDURE PREVIOUSLY PROPOSED BY DEFENDANT.**

As only partially revealed in Plaintiff's Motion to Compel, the parties have not been able to agree on the terms of a protective order and, because of that, Plaintiff does not yet have an image of Defendant's hard drive. That is, Plaintiff served a request for Defendant to produce an image or "clone" of his hard drive. Defendant proposed a procedure for accomplishing the same. Under Defendant's proposal, the examination would be done by an "independent" expert, who reported to both sides, and who was licensed in Michigan to engage in computer forensics, and the cost of the examination would be borne by Plaintiff. Plaintiff has asked for Fed. R. Civ. P. 26(c)(1), in relevant part, provides that "[t]he court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Such an order may include "(A) forbidding the disclosure or discovery; (B) specifying the terms . . . for the disclosure or discovery; (C) prescribing a discovery method other than the one selected by the party seeking



discovery . . . .” *Id.* The decision to issue a protective order is left to “the broad discretion of the district court in managing the case.” *Lewelling v. Farmers Ins. of Columbus, Inc.*, 879 F.2d 212, 218 (6th Cir. 1989).

**Weighing the respective burdens.** As discussed earlier, Plaintiff wants to make a complete copy of everything on Defendant’s hard drive, and then have its paid examiners spend weeks or months poring over what they find there. Defendant is of the position that nothing found on his computer’s hard drive will have any relevance to this case—except that very conclusion, i.e., that there is nothing relevant to this case there. Because Defendant has no desire to let the details of all of his personal and confidential information be scrutinized by pornographers who (in his view) are engaging in a for-profit campaign of mass extortion, Defendant made a reasonable proposal as to how Plaintiff could obtain the information in which it has a legitimate interest. That is, on February 28, 2014, Defendant submitted the following objection to Plaintiff’s discovery request.

[Request No.1 by Plaintiff.] A forensically sound copy (a clone) of the hard drive for each of the Computer Devices in your house, apartment or dwelling.

**RESPONSE NO. 1:**

**Defendant objects to this request on the basis that, by its terms, it proposed to impose on Defendant annoyance, embarrassment, oppression or undue burden or expense. More specifically, Defendant does not personally have the skills or knowledge to produce such a copy, and should not be expected to bear the financial burden of hiring an expert to produce such a copy. Moreover, Defendant has neither permission, access to, or even knowledge of every computer device ever used in his house during the alleged "period of record infringement." Moreover, and more importantly, the hard drive of the only computer that Defendant has ever used in his house from well before, during, and after the alleged “period of record infringement,” contains private and confidential information completely unrelated to any legitimate purpose of Plaintiff in the instant lawsuit, and Defendant should not be compelled to entrust such private and confidential matters to the custody and control of a pornographer/plaintiff. Notwithstanding said objection, Defendant proposes to allow Plaintiff access to the information it seeks,**

as follows:

**Plaintiff and Defendant shall mutually agree upon the selection of an independent expert in "computer forensics" (as that term is defined by MCL 338.822(b)), who is licensed in Michigan under MCL 338.821 *et seq.* If Plaintiff and Defendant cannot agree on the selection of such an expert, then one shall be selected by the Court. Plaintiff will bring his computer, and any other video games or equipment within his custody and control and identified in these requests as being sought by Plaintiff for inspection, to the offices of Blanco Wilczynski at a mutually agreed upon time, where it/they can be examined by the independent expert in computer forensics. Said expert may make copies of the information stored on any such device, subject to the following conditions. First, the Plaintiff must agree to the entry of an appropriate protective order, being one that forbids the computer forensic expert from revealing to Plaintiff (or any other person) any of the information obtained from Defendant's computer or devices that is not relevant to this action under FRE 401. Second, the protective order must forbid the computer forensic expert from retaining such information after the close of this case, or permitting anyone else from retaining it. In addition, Plaintiff will be required to pay computer forensic expert's fees, but the computer forensic expert must agree to maintain his or her independence, rather than maintaining a client relationship with Plaintiff.**

(Defendant's February 28, 2014 Responses to Plaintiff's Requests for the Production of Documents [not filed].)

In response, Plaintiff's counsel has not agreed to pay for to make a copy of Defendant's hard drive, but offered to enter into a blanket protective order designed to protect Plaintiff's interests (e.g., customer lists, processes, operations, type of work, or apparatus, or to the production, type and volume of sales, shipments, purchases, transfers, identification of customers, inventories, amount or source of any income, profits, losses, or expenditures). Moreover, the protective order proposed by Plaintiff would require an onerous process of individually designating each document subject to non-disclosure as falling into one of three confidential categories. This would leave Defendant in the unenviable position of examining, or having his attorneys examine, every item on his hard drive, designate it with some identifier, and then classify it (or fail to classify it) with one of the three

categories of confidentiality proposed by Plaintiff. Moreover, the parties would thereafter be free to follow another procedure to challenge confidentiality level assigned by the other party to a document. Seriously?! The cost of going through that process, by itself, would engender defense costs far in excess of one of Plaintiff's notorious settlement demands.

In support of its proposal, and in opposition to Defendant's, Plaintiff's counsel has taken the position that Defendant is trying to determine who Plaintiff can have as its expert. Defendant would respond that he is only trying to prevent his personal and confidential information that is wholly irrelevant to this action from falling into the hands of Plaintiff or its experts—while at the same time providing Plaintiff with everything it needs in a manner by which Plaintiff can rest assured that nothing was withheld.

Obviously, Defendant's desire to not be subjected to annoyance, embarrassment, oppression, or undue burden or expense conflicts with Plaintiff's desire to open and broad discovery (assuming the best intentions on the part of Plaintiff, rather than inferring a desire to impose a hardship on Defendant). But resolving such tensions between the parties rights is exactly what Fed. R. Civ. P. 26(c) is for.

**Irrelevant Information.** Defendant is not claiming that any information on his hard drive that would support Plaintiff's case is confidential. Rather, he is claiming that nothing on his hard drive will be relevant to Plaintiff's claims, and that such irrelevant information includes all of the private and confidential information that he wants kept private and confidential. Should an independent expert determine that there is nothing on Defendant's hard drive in the nature of what Plaintiff seeks, Plaintiff can hardly object to being precluded from discovering irrelevant information. Indeed, the United States Supreme Court has expressly held that, pursuant to Fed. R. Civ. P. 26(b) relevancy is a *sine qua non* for information to fall within the scope of discoverability

in the first place. See *Schlagenhauf v Holder*, 379 U.S. 104, 85 S. Ct. 234, 13 L. Ed. 2d 152 (1964).<sup>6</sup>

**Financial Burden vs Plaintiff's Valuation of its Case.** . Plaintiff chose to bring this suit, and many more like it, based solely on its claim that it can allegedly trace infringing activity to someone using (or appearing to use) Defendant's IP address. Presumably, it must be aware that the correlation between IP address and user is somewhat loose, and that on many occasions it will have sued the wrong party. Apparently, it has determined that the financial gain it stands to realize through a broad application of that strategy outweighs the costs that it will incur (and impose) on those occasions where (as here) it has sued the wrong party. And, of course, the cost of having Defendant's hard drive examined for evidence of file sharing is obviously one of those contemplated costs.

Defendant, by contrast, did not sign up for this. He has been involuntarily dragged into this mess. Since an independent forensic examiner could provide the necessary information to both sides, it makes no sense for Defendant to have to retain his own expert. Why pay for two when one will do? Let Plaintiff front the cost of a licensed, independent forensic examiner, but allow both Defendant and Plaintiff to have equal access to the independent expert's report.

Incredibly, Plaintiff argues that Defendant should be required to bear the estimated \$2,400 to \$4,000 in costs produce the "clones" that Plaintiff desires. This, despite the fact that Fed. R. Civ. P. 26(b)(2) places a limitation on the discoverability of electronically stored information based on undue burden or cost. Moreover, Plaintiff's argument about accessibility is inapt. The cost is not

---

<sup>6</sup> In *Schlagenhauf* the Court's discussion of the "good cause" requirement of Fed. R. Civ. P. 35(a) gave substantial insight into the relevancy requirement of discoverability under Fed. R. Civ. P. 26(b)(1). That is, the Court noted that because the general scope of discovery is limited to any matter, not privileged, that is relevant to the subject matter of the litigation, then the "good cause" requirement of Rule 35(a) "would be meaningless if [it] could be established by merely showing that the desired materials are relevant, for the relevancy standard has already been imposed by Rule 26(b)." *Schlagenhauf, supra*, 379 U.S. at 117-118.

in *accessing* the information. The cost comes from the fact that Plaintiff wants something created that does not now exist. Presumably, Plaintiff would concede that it would be unduly burdensome for Defendant to be without his computer for six weeks while a computer forensic expert pores over his computer's hard drive. Consequently, Plaintiff proposes that an image or "clone" of the hard drive be made— but Plaintiff wants Defendant to pay for that.

As the United States Supreme Court has acknowledged, under Rule 26(c), a "district court [has the] discretion . . . to grant orders protecting [a party] from 'undue burden or expense' in [complying with discovery requests], including orders conditioning discovery on the requesting party's payment of the costs of discovery." *Oppenheimer Fund, Inc., v. Sanders*, 437 U.S. 340, 358 (1978). Incredibly, Plaintiff argues to this Court that making Defendant bear a cost estimated by Plaintiff to be \$4,000 is not substantial enough to be an undue burden for purposes of shifting the cost to Plaintiff—simply because, in *other* cases-- where the dollar amounts at issue and financial resources of the parties were different— such a figure may have been determined to not be big enough.

However, in this case, Plaintiff itself has evaluated its case as being worth \$6,000.00, having made a written demand for that figure to settle this case on May 16, 2014 at 10:36 am. (see Exhibit A--Consequently, with a straight face, Plaintiff is arguing to this Court that Defendant (an individual who has no liability for any copyright infringement) should be put to the choice of either paying Plaintiff's demand for \$6,000, or paying \$4,000 to create images of his hard drive so that Plaintiff can learn what Defendant already knows— that Defendant did not infringe Plaintiff's copyrights.

The inquiry in a cost-shifting analysis is not necessarily whether the cost is substantial but whether it is "undue." *Oppenheimer Fund*, 437 U.S. at 358; *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 428-29 (S.D.N.Y 2002). Undue burden is decided on a case-

by-case basis. *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 463 (D. Utah 1985). Here, Plaintiff is a multi-million dollar corporation, Defendant is an individual. Plaintiff values its case at \$6,000, but wants to require Defendant to pay \$4,000 in costs if he will not buckle under. And Defendant is not the one who allegedly infringed Plaintiff's copyrights

**Licensing/Copyright Violations.** As noted, under Michigan law, persons who engage in "computer forensics" (as that term is defined by MCL 338.822[b]) "to be used as evidence before a court, board, officer, or investigating committee," MCL 338.822(e)(viii), must hold a license to do so, and doing so without a license is a felony punishable by up to four years in prison. MCL 338.823(1). Therefore, any expert who engages in computer forensics with respect to Defendant's hard drive should be licensed pursuant to MCL 338.821 *et seq.* To the extent that Defendant's hard drive contains authorized copies of other works that are subject to copyrights (e.g. computer programs), Plaintiff should be compelled to indemnify and hold Defendant harmless for any infringement of said copyrights resulting from the imaging of his hard drive.

**II. ABSENT A PROTECTIVE ORDER LIKE THE ONE PROPOSED BY DEFENDANT, THIS COURT SHOULD ENTER ONE LIKE THAT ENTERED BY JUDGE ROBERTS IS A SIMILARLY SITUATED CASE.**

In addition to the principal issue of the examination of Defendant's hard drives, Plaintiff takes issue with certain objections that Defendant asserted to requests for production that Defendant deemed to be overly broad, unduly burdensome and not relevant. With regard to the one request where Plaintiff has complied with WD Mich LR 7.1(b) (see Plaintiff's Motion to Compel, p 5), Plaintiff wants any document, receipt, purchase, credit card statement etc., for more than a four-month period, even though the alleged acts of infringement occurred during a six-day period in February of 2013. Moreover, after Defendant obtained documentation (mostly in the form of texts of electronic messages sent by him from his IP address in Grand Rapids), Plaintiff's counsel

expressed the position that it does not matter if Mr. Raleigh was in Grand Rapids when the infringement was occurring in Petoskey, because he could have set his computer to have automatically download or upload the copyrighted works while he was away.

In other words, Plaintiff's discovery requests amount to a "wild goose chase" that is clearly intended simply to run up Defendant's legal bills in order to make it more likely that Defendant would cave in and pay a coerced settlement demand of \$6,000 rather than incur the costs of defending himself. Plaintiff's request was unduly burdensome (particularly given the value that Plaintiff places on it. Why ask for documents regarding a period of two months before and two months after the alleged infringement, when only a six-day period in February 2013 is relevant? Why ask for proof that Defendant was away from home at all, if Plaintiff takes the position that said fact is irrelevant?

Defendant submits that, if this Court declines to enter the protective order he requests, this Court should instead enter an order similar to that entered on July 21, 2014 by Judge Roberts in *Malibu Media v Shekoski*, USDC ED Mich 13-12217, (Exhibit B). Under that order, Plaintiff must pay for the production of the image or clone of Defendant's hard drive. The person doing so could then be a Michigan-licensed computer professional. The information on the hard drive would be subject to a further protective order (to which counsel have already reached agreement in the *Shekoski* case), and if no evidence of copyright infringement or deletion is found, Plaintiff must dismiss its case. In addition, and importantly, all other discovery in the case would be stayed until the forensic examination of Defendant's computer hard drive is complete. This would prevent the unduly burdensome and coercive effect of Plaintiff's broad requests for documents and things that even Plaintiff believes are not relevant.

#### **CONCLUSION and RELIEF REQUESTED**

For the reasons stated above, Defendant seeks a protective order of this Court under Fed. R.

Civ. P. 26(c)(1) with regard to Plaintiff's request for a complete copy of the hard drive on his computer. To wit:

Plaintiff and Defendant shall mutually agree upon the selection of an independent expert in "computer forensics" (as that term is defined by MCL 338.822[b]), who is licensed in Michigan under MCL 338.821 *et seq.* If Plaintiff and Defendant cannot agree on the selection of such an expert, then one shall be selected by the Court from nominees provided by the parties. Plaintiff will bring his computer, and any other video games or equipment within his custody and control and identified in these requests as being sought by Plaintiff for inspection, to the offices of Blanco Wilczynski at a mutually agreed upon time, where it/they can be examined by the independent expert in computer forensics. Said expert may make copies of the information stored on any such device, subject to the following conditions. Said expert shall expressly agree to be bound by this protective order. Said expert will not reveal to Plaintiff (or any other person) any of the information obtained from Defendant's computer or devices that is not relevant to this action under FRE 401. The parties will assist said expert in that regard by submitting to him or her mutually agreed upon interrogatories about the contents of Defendant's computer. The computer forensic expert must destroy and not retain, or permit anyone else (other than Defendant) to retain information obtained from Defendant's computer after the close of this case. In addition, Plaintiff will be required to pay the computer forensic expert's fees, but the computer forensic expert must agree to maintain his or her independence, rather than maintaining a client relationship with Plaintiff.

**Alternatively**, Defendant would request that this Court issue an order similar in all respects to the one issued by Judge Roberts on July 21, 2014 in *Malibu Media v Shekoski*, which is attached hereto as Exhibit B.

**WHEREFORE**, Defendant respectfully requests a protective order from this Court as set forth above.

Respectfully submitted,

**Blanco Wilczynski, PLLC**

s/ Derek W. Wilczynski  
By: Derek W. Wilczynski (P57079)  
Attorneys for Defendant  
2095 E. Big Beaver Rd., Suite 400  
Troy, Michigan 48083  
(248) 519-9000  
[dsw@blancopc.com](mailto:dsw@blancopc.com)

**Lincoln G. Herweyer, PC**

s/ Lincoln G. Herweyer  
By: Lincoln G. Herweyer (P55742)  
Co-Counsel for Defendant  
35054 Twenty-Three Mile Rd., Suite 115  
New Baltimore, Michigan 48047  
[lgherweyer@netscape.net](mailto:lgherweyer@netscape.net)



**CERTIFICATE OF SERVICE**

I certify that on July 25 2014, I electronically filed the foregoing paper with the Clerk of the Court using the ECF system which will send notification of such filing to: Paul J. Nicoletti, Attorney for Plaintiff.

s/Lincoln G. Herweyer

Lincoln G. Herweyer  
35054 Twenty-Three Mile Rd., Suite 115  
New Baltimore, MI 48047  
(586) 716-1562  
[lgherweyer@netscape.net](mailto:lgherweyer@netscape.net)