IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 12-cv-0480-BH-PAB
*
MALIBU MEDIA, LLC
*
Plaintiff,
v.
*
John Does 1-16

Defendants

Declaration of Doe #8

Defendant, Internet Protocol Number 98.245.119.25 (January 30, 2012)(Doe#8), states as follows:

1. I received a letter delivered in a package by United Parcel Service from my Internet Service Provider Comcast stating that the IP address of 98.245.119.25 was used on January 30, 2012 to upload or download a movie without permission (letter attached as Exhibit 1 with my name and address redacted).

2. I understand the Complaint states that the IP address is associated with an Allegedly illegal file sharing of an 11-minute adult movie entitled, “Angel Seaside Romp.”

3. I have a wireless router for Internet access. No one but me has access to my laptop computer or other device of mine that uses my wireless router. My computer is password-protected.

4. I have never downloaded this movie onto my computer or onto any other device.

5. I have never seen this movie.

6. I have never downloaded any pornographic movies onto my computer or onto any other device.

7. I have never downloaded any movies using BitTorrent.

8. I do not know who might have been in range of my wireless router on January 30, 2012 that might have downloaded a movie.

9. I usually shut off my computer overnight although the router remains on

10. Involving me further in this lawsuit will be detrimental to my finances and cause me needless worry and anxiety.

11. I am embarrassed and troubled that I may be listed as a named defendant in a lawsuit being accused of having downloaded some portion of a pornographic movie.

12. I am concerned that being named as a defendant in a suit accusing me wrongfully of downloading a pornographic movie will appear on the internet and be a permanent presence on the internet and will damage my reputation needlessly.

13. I am very concerned that there are no restrictions on the use of my personal data if it is released by Comcast. If this subpoena is granted without any protection, my name, IP address, computer number, e-mail address and other personal information will be on the internet in court records and in the public domain and could be used by anyone for any purpose, such as identity theft.

14. I understand that a representative of Plaintiff has offered that I will not be named in the lawsuit, regardless of whether or not I did anything wrong, in return for payment to the Plaintiff of thousands of dollars. I also understand that Plaintiff has refused an offer to have an expert look at my computer to demonstrate to Plaintiff that I did not download any piece of Plaintiff's movie.

15. I have an expectation of privacy and expect that my identify, my personal information such as my telephone number, computer number and e-mail address will be kept private and confidential by Comcast when I access the internet for lawful purposes through my wireless router.

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

Executed on this 15th day of June, 2012

/Doe#8/

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 12-cv-0480-BH-PAB
*
MALIBU MEDIA, LLC
*
Plaintiff,
v.
*
John Does 1-16

Defendants

Motion to Quash, Sever Defendants 2—16, and/or for Protective Order

Doe #8, through his attorney, David A. Klibaner, respectfully submits this Motion to Quash Subpoena and/or Sever Defendants 2-16 and/or for Protective Order. The subpoena was issued by Plaintiff and was delivered to Doe#8 via the internet service provider Comcast. A copy of the subpoena with the heading " U.S. District Court for the State of New Jersey" was attached to the letter Doe #8 received from Comcast and is attached as Exhibit 1.

Background

A tidal wave of litigation has been filed by a number of attorneys across the country on behalf of various business entities that sell pornography over the internet claiming copyright infringement against persons allegedly using peer to peer networks seeking statutory penalties. These companies claim that various Doe defendants, identified by only IP addresses have violated copyright law by using peer to peer file sharing programs such as Bit Torrent.

Each Defendant in this case is claimed to have downloaded the exact same piece of an 11- minute video entitled "Angel Seaside Romp." Said video is alleged to have been made in 2012 and was registered for copyright on January 4, 2012. The John Doe Defendants allegedly downloaded a portion of said video over a period of 6 weeks in early 2012 according to Plaintiff.

Defendant Doe has filed the foregoing Declaration with this motion, along with the Declaration of his attorney (Exhibit 2). Defendant Doe has not illegally downloaded said video. His attorney has offered to make Defendant Doe's computer available for an expert inspection, but was turned down because, "He probably isn't the downloader, but that's why we need to keep him in the litigation."

I. Doe#8 has standing to challenge the subpoena

Defendant Doe#8 has standing to challenge the subpoena issued by the Plaintiff to Comcast. Comcast notified Doe #8 that he is about to be identified to Plaintiff as a result of the subpoena, his personal and private information, beyond his name and address, is to be disclosed to Plaintiff and that Defendant's modem was assigned the Internet Protocol number 98.245.119.25 (January 30, 2012). By providing Defendant with the notice and subpoena, Comcast has effectively transferred to Defendant the right and obligation to object to the subpoena since Comcast has no legal obligation provide an objection on Defendant's behalf.

The general rule is that a party has no standing to quash a subpoena served upon a third party, except as to claims of privilege relating to the documents being sought. *Oliver Cannon and Son, Inc. v. Fidelity and Cas. Co. of N.Y.,* 519 F.Supp. 668 (D.Del.1981). However, a party may move to quash a subpoena upon a showing that there is a privacy interest applicable. *Windsor v. Martindale*, 175 F.R.D. 665 (D. Colo. 1997); *Broadcort Capital Corp. v. Flagler Securities, Inc.,* 149 F.R.D. 626 (D.Colo.1993); *Smith v. Midland Brake, Inc.,* 162 F.R.D. 683, 685 (D.Kan.1995). Absent a specific showing of a privilege or privacy, a court cannot quash a subpoena duces tecum.

In the present case, the Defendant has legitimate interests which would be infringed upon if the subpoena is not quashed as to him, namely, his First Amendment right to privacy, his personal privacy and the **unique identifying information on his computer**, which should remain private and confidential and should not be released to the public domain lest that information be used by others for illicit purposes.

II. The subpoena must be quashed since Plaintiff had no authority to issue or obtain a New Jersey subpoena from a court order issued in Colorado

Federal Rule of Civil Procedure 45 governs the issuance of subpoenas for the production of documents by nonparties. *See* Fed. R. Civ. P. 34 (c) ("As provided in Rule 45, a nonparty may be compelled to produce documents and tangible things or to permit an inspection."). Among other matters, "[Rule] 45 governs the territorial limitations regarding where [non-party] depositions are to be taken or where documents are to be produced." *Ariel v. Jones,* 693 F.2d 1058, 1060 (11th Cir. 1982). Rule 45(a)(2)(C) requires that a subpoena for the production of documents "must [be] issue[d] ... from the court for the district where the production or inspection is to be made."

Denver, Colorado, is not located within the District of New Jersey and this court has no power to authorize Plaintiff to issue a New Jersey subpoena that requires Comcast, to produce documents in Denver. Fed.R.Civ.P. 45(a)(2)(C); *see also Natural Gas Pipeline Co. of America v. Energy Gathering, Inc.*, 2 F.3d 1397, 1406 (5th Cir. 1993) ("[A] federal court sitting in one district cannot issue a subpoena duces tecum to a non-party for the production of documents located in another district."). Therefore, regardless of whether the plaintiffs are otherwise entitled to discovery of the documents in question, the subpoena is invalid on its face and must be quashed. *See* Fed. R. Civ. P. 45(a)(2)(C); *see also James v. Booz-Allen & Hamilton, Inc.*, 206 F.R.D. 15, 19 (D.D.C. 2002) ("Because the place of production and inspection in this case is outside of the judicial district of this court, the subpoena is improper and is therefore quashed.").

Here, Magistrate Hegarty issued his order permitting service of the subpoenas on the Internet Service Provider, Comcast, thus allowing the Does time to move to quash the subpoenas or seek other relief.[1]. However, the subpoena that was issued by

[1] Magistrate Judge Hegarty was only provided with one-side of the story – that of the Plaintiff – and was not made aware of the law that contraverts Plaintiff's claims. Nor was he made aware of the significant interests that the putative Defendants have in their personal and confidential information. (In other jurisdictions, some courts have appointed attorneys to represent the significant First Amendment and

Plaintiff was a subpoena issued by the District Court for the District of New Jersey. [2] Magistrate Judge Hergarty has authority only to issue subpoenas on ISPs located within the District of Colorado. This may be a technicality, but clearly, a Colorado magistrate cannot authorize a federal subpoena to be issued in New Jersey. The subpoena is fatally deficient and must be quashed as a matter of law . See, eg. *Weekes-Walker v. Macon County Greyhound Park, Inc*., 3:10-cv-895-MEF (WO) (ALMDC) (June 11, 2012).

III. Plaintiff's Use of IP Addresses to Identify Putative Defendants Is Inherently Unreliable, Violates the Privacy Rights of Innocent People and May Be Accomplished By Other Means

Plaintiff's claim that identifying alleged infringers and then suing them in federal court is the only remedy available to it is false. Here, Plaintiff has made no showing that it has attempted to obtain any remedy against the largest violators, the websites displaying access to its claimed work. Nor has it had to even show that it sent a cease and desist letter or a letter demanding payment to any of these alleged copyright infringers.

If Plaintiff's true purpose was to stop the illegal copying of its video porn, it could (1) identify Bit Torrent websites and send letters demanding payment and that the websites cease and desist from displaying the copyrighted material or (2) simply notify the service providers of its copyright infringement concerns and ask the Internet service providers to issue a takedown notice to the websites displaying the alleged pilfered material. See eg. http://www.nppa.org/memberservices/advocacy/dmca_takedown_procedure.pdf. Under this procedure, aggrieved copyright holders under the Digital Milennium Copyright Act

---

privacy interests of the unidentified Doe Defendants; See eg.,*Mick Haig Productions v. Does 1-670*, No. 3:10-cv-1900-N (TXNDC)(Sept.9, 2011)

[2] It is unclear why Plaintiff obtained the issuance of a New Jersey subpoena, other than to make it harder for Defendants to move to quash the subpoena. But as Comcast itself stated in *AF Holdings LLC v. Comcast*, Comcast is a national company with operations in all 50 states. Its subscriber information is stored electronically and would be available in all 50 states, including in the District of Colorado.

may ask the Internet Service Provider to remove materials from users websites that appear to constitute copyright infringement. Monitoring Bit Torrent websites that allow and/or encourage illegal copying or downloading would be a much better us of limited resources to stop copyright infringement, However, from the porn purveyor's perspective, what these alternatives lack is the ability to quickly collect settlements against individuals who likely cannot afford to mount an effective defense against a legalized shakedown operation..

In a recent case in which Comcast successfully refused to furnish the identifying information of 88 internet subscribers, Comcast (the ISP for this Doe) made a similar argument:[3]

> Plaintiffs should not be allowed to profit from unfair litigation tactics whereby they use the offices of the Court as an inexpensive means to gain Doe defendants' personal information and coerce 'settlements' from them,
>
> It is evident in these cases – and the multitude of cases filed by plaintiffs and other pornographers represented by their counsel – that plaintiffs have no interest in actually litigating their claims against the Doe defendants, but simply seek to use the Court and its subpoena powers to obtain sufficient information to shake down the Doe defendants."

AF Holdings, LLC v. Comcast Cable Corporation, No.1:12-cv-03516 Document #: 11 Filed: 06/01/12 (Exhibit 3)

Comcast countered the "swarm" joinder argument by pointing out the defendants could not have acted in concert given the wide time period over which Defendant's accessed portions of the "work." Comcast pointed out that since joinder was improper in the underlying actions, compelling the discovery of the alleged swarm members

[3] 3 As a party defendant in a case seeking subscriber names and addresses for 88 of its subscribers, Comcast argued that 4 companies purveying porn had no grounds to join numerous defendants under a swarm theory in one lawsuit and that the discovery being sought was overbroad and exceeded the bounds of fair discoverydue to the improper joinder of multiple individual defendants in 3 lawsuits pending in Florida and one lawsuit pending in Texas.

Comcast accused copyright holders of exploiting the federal court system in order to coerce defendants into coughing up money and the District Court agreed, quashing the requested subpoenas. *AF Holdings, LLC v. Comcast Cable Corporation,*

constituted an undue burden under Rule 45. The Court agreed, quashing all of the subpoenas requested.

This lawsuit is one of dozens, if not hundreds that have been filed by the Kotzker Law Firm in Colorado, New York and other locations across the country on behalf of Malibu Media, LLC, Patrick Collins, Inc. and other producers/distributors of pornographic videos. In these cases, dozens to hundreds of Doe defendants are joined in a single action, the Plaintiff files a motion for expedited discovery, obtains court authorization to service subpoenas on ISPs who then notify their customers that unless the customer files a legal motion, the ISP will release confidential identifying information to the Plaintiff's attorneys. The Plaintiff's attorneys then use this information to coerce the identified person to "settle" the litigation by paying several thousands of dollars, before being publicly named as downloading pornographic materials. See description by Judge Holderman in *Pacific Century International, Ltd v. John Does 1-27 (and others)*, 12 C 1057 (N.D. IL Docket #23 at page 6, March 30, 2012) (Exhibit 4).

Courts are becoming increasingly dismayed by these suits, with critical decisions being rendered in many jurisdictions, in addition to the foregoing decisions of Judge Holderman. *In re Bittorrent Adult Firm Copyright Infringement Cases,* 2:12-cv-01147-JS-GRB (E.D. N. Y., May 1, 2012) (Exhibit 5) and *AF Holdings LLC v. Does 1-135*, 5:11-cv-03336-LHK (N.D. CA, February 23, 2012) (Exhibit 6). The Courts are recognizing that these lawsuits are part of an overall pattern or business plan of extorting "settlement" money from identified Does, and there is no intent to actually move forward with the litigation after the "Does" have been identified.

An IP address provides only the location at which any number of computer devices may be used, much like a telephone number can be used for any number of telephones. It is even less likely that the subscriber of an IP address carried out a computer function such as downloading a movie that to say the individual who pays the telephone bill made a specific telephone call.

Over 60% of households now have a wireless router, making it possible for various users and devices access the internet from a particular IP address including

users who have accessed the IP address who do not reside at the address of the subscriber and who may not be known to the subscriber.

However, bringing claims against innocent Defendants anxious to settle so as to avoid any association with Plaintiff's business of producing porn videos provides a lucrative business model for the Plaintiff. If only a fraction of the multiple defendants identified in this Internet dragnet settle out of court, plaintiffs can walk away with enormous sums of money without ever having to prove up a single individual case. Who is to stop producers of porn from initiating their own Bit Torrent cascade to distribute their work over the internet, then rounding up hundreds of IP addresses in only a few court cases (saving on individual filing fees) and then settling with a fraction of Internet subscribers in a scheme of legalized extortion?

The Magistrate in *In re:Bitttorrent* stated that the likelihood that the payer of the bill sent by ISPs was the actual downloader/infringer in these cases is not high. Consequently, the danger in allowing Plaintiffs to engage in this wide net type of discovery, especially to discover private information beyond that required to identify potential defendants and serve them with a Summon and Complaint ***is significantly increased*** (see Exhibit 5, pp 6-8). In that case the Court severely limited the type of information that the Plaintiff was entitled to seek from the ISP (as well limiting the subpoena to only a single Defendant per case).

The Plaintiff here has cast a wide net in an attempt to identify the owners of various internet connection devices, such as modems and routers that were allegedly associated with the transfer of portions of an adult video. Although the Plaintiff identifies IP address 98.245.119.25 as participating in the transfer, the person who Comcast has notified as owning a router being the assignee of that IP Address at that time has provided a declaration that establishes that neither he, nor any authorized user of his computer equipment, was involved in the complained of activity. Since Plaintiff cannot establish that the subscriber with IP address was the person that actually was involved in the activity complained of in the Complaint, the subpoena seeking to have Comcast reveal the identity of that subscriber should be quashed.

In an effort to resolve this matter quickly, fairly and conclusively, Defendant's counsel sent an e-mail to the Jason Kotzker of the Kotzker Law Group. Defendant Doe offered to make his computers available to a computer expert to confirm that the alleged downloaded movie was not on Defendant's computer. Mr. Kotzker declined stating that Plaintiff could not agree due to the fact that someone other than Defendant might have performed the downloading. In other words, Mr. Kotzker would not agree to dismiss this Defendant because someone other than this Defendant might be the real infringer. An associate of Mr. Kotzker's, offered that this Defendant could be dismissed from the action by payment of thousands of dollars regardless of his culpability.

The Magistrate in the *In re Bittorrent* found such refusal to investigate the innocence of an IP subscriber quite problematic (Exhibit 5 at pp 8-11), stating the evidence shows that Plaintiff's litigation strategy is to collect as many settlements as possible from non-culpable "Does" as quickly as possible before dismissing the cases.

In light of the above, Defendant submits that this Court should quash the subpoena to Comcast with respect to Doe #8.

IV. Joinder of the 16 Doe Defendants is Improper and Does 2-16 Should Be Severed

Plaintiff's allegations that Defendant Does acted in concert is without merit and legally insufficient to permit joinder of these unrelated defendants. Plaintiff attempts to justify combining the lawsuits of these 16 Does by claiming that they acted in concert. Yet Plaintiff cannot explain how Defendant Does acted in concert if Plaintiff's allegation is true, namely that each of them downloaded the same piece of an internet video file at different times and from different locations.

This allegation has allowed Plaintiff to avoid paying the filing fees that would be due if each IP address was identified and sued separately, allowing for consideration of the inevitable multitude of defenses that invariably come up in such mass filings against internet subscribers that do not share common questions of fact.

Plaintiff's allegations are based upon the use of the internet to infringe a single work. That does not change the legal analysis. Whether the alleged infringement concerns a single copyrighted work or many, it was allegedly committed by unrelated defendants at unrelated times, at unrelated locations, using different Internet service providers. Undoubtedly, Defendants will assert many unrelated defenses including failure to exhaust administrative remedies, bad faith on the part of Plaintiff, unclean hands, misidentification of IP addresses, and others.

The individual Does have no knowledge of each other, nor do they control how the alleged Bit Torrent protocol works. There is no allegation that any portion of a work allegedly downloaded came jointly from any of the Defendants. Nor is there any allegation that any of the Does provided the initial link to the copyrighted material without the authorization of the copyright holders, without which no allegedly illegal copying could have taken place. [4]

Joining unrelated defendants in one lawsuit may make litigation less expensive for the Plaintiff by enabling it to avoid the separate filing fees required for individual cases, but that does not justify violating well-established joinder principles.

Joinder based on separate but similar behavior by individuals allegedly using the internet to commit copyright infringement has been rejected by courts across the country. In *LaFace Records LLC v. Does 1-38*. No. 5:07-CV-298-BR, 2008 WL 544992 (E.D.N.C. Feb. 27, 2008), the court ordered severance of lawsuit against thirty-eight defendants where each defendant used the same ISP as well as some of the same peer to peer (P2P) networks to commit the exact same violation of the law in exactly the same way. The court explained: "[M}erely committing the same type of violation in the

---

[4] Plaintiff has chosen to focus its copyright infringement cases on individual internet subscribers who may have downloaded a piece of an 11 minute video that may or may not have been identified as a copyrighted work. Yet a Google search of "Angel Seaside Romp" provides a plethora of websites posting the torrent content as well as several websites providing free access to Plaintiff's "work."

If Plaintiff has limited resources to address the issue of copyright would it not make more sense to go after the free websites that post Plaintiff's video or the torrent websites or file servers that make the alleged illegal copying possible? Plaintiff's choice of targets suggests that its primary goal is to quickly collect as many settlements as possible against users who access the content for a non-commercial purpose rather than proceeding against infringers reaping a commercial benefit from the unauthorized reproduction of Plaintiff's work.

same way does not link defendants together for purposes of joinder." LaFace Records, 2008 W: 544992, at *2. Courts in this District have embraced the same principles. See eg., Orders to Show Cause and Orders re Third Party Subpoenas Duces Tecum issued June 4, 2012, *Malibu Media, LLC v. John Does 1-54*, No. 12-CV-1407-WJM and *Malibu Media, LLC v. John Does* (attached here to as Exhibits 7 and 8).

In *In re BitTorrent* decision recommending severing all ut the first Doe Defendants, May 1, 2012 decision recommending severing all but the first Doe Defendants, Magistrate Judge Gary R. Brown noted the leverage to gain settlements encourages mass filings against internet subscribers, particularly given the porn purveyors's ability to avoid filing fees that might make filing claims solely on the basis of an IP address less likely:

> Thus, the Plaintiffs file a single case, and pay one filing fee, to limit their expenses as against the number of settlements they are able to negotiate. Postponing a decision on joinder in these cases results lost revenue of perhaps millions of dollars (from lost filing fees) and only **encourages plaintiffs in copyright actions to join or misjoin, as many defendants as possible.** (emphasis supplied)

Order, Malibu Media v. John Does 11 and 26, Patrick Collins

A growing number of federal courts have found that participating in a Bit Torrent "swarm" does not constitute a single transaction or series of transactions necessary for proper joinder under Rule 20(a). Order of Judge G. Murray Snow, *Patrick Collins, Inc. v. John Does 1-54*, 2012 WL 911432 at *5 (D. Ariz. March 19, 2012)(order severing John Doe Defendant for lack of proper joinder). Absent allegations that any particular defendant copies a piece of the digital file from or to any other particular defendant, a court could not conclude that the users "were engaged in the single transaction or series of closely-related transactions recognized under Rule 20." Order of Judge Samuel Conti, *SBO Pictures, Inc. v. Does 1-3036*, 2011 WL 6002620 at *3 (N.D. Cal. Nov. 30, 2011) (order severing Doe Defendants 2-3036 due to improper joinder;"… the Court finds that the potential for coercing unfair settlements from innocent defendants trumps Plaintiff's interest in low litigation costs.")

Because the improper joining of these Doe defendants into one lawsuit raises serious questions of individual fairness and individual First Amendment privacy rights, the Court should sever the Defendants and drop Does 2-16 from the case.

V. F.R.C.P. 26(c)(1) requires that this Court enter a Protective Order And Restrict Public Access to Protect the Personal and Confidential Information of Defendant Doe

Rule 26(c)(1) provides in pertinent part

The court may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense, including one or more of the following:

(B) specifying terms, including time and place, for the disclosure or discovery;

(D) forbidding inquiry into certain matters, or limiting the scope of disclosure or discovery to certain matters;

The presumption of public access recognized and promoted by the local rule finds its root in the common law rights of access to judicial proceedings and to inspect judicial records-rights which are " beyond dispute." *Publicker Industries, Inc. v. Cohen,* 733 F.2d 1059, 1067 (3d Cir.1984). The reason for the presumption of open access to court proceedings is easily understood. " People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing." *Press-Enterprise Co. v. Superior Court,* 464 U.S. 501, 509, 104 S.Ct. 819, 78 L.Ed.2d 629 (1984). The public has a fundamental interest in understanding the disputes presented to and decided by the courts, so as to assure that they are run fairly and that judges act honestly. *Crystal Grower's Corp. v. Dobbins,* 616 F.2d 458, 461 (10th Cir.1980).

However, there are limits on what is important for the public to know. Privacy interests have been found to be sufficiently compelling to overcome the presumption of openness. *See Seattle Times Co. v. Rhinehart,* 467 U.S. 20, 32-36, 104 S.Ct. 2199, 81 L.Ed.2d 17 (1984)(noting that liberal pretrial discovery " may seriously implicate privacy interests of litigants and third parties" and holding that courts have broad discretion to

issue protective orders to prevent abusive use of information obtained through the discovery process.)

F.R.C.P. Rule 26(c) authorizes a court, "for good cause shown," to make "any order which justice requires to protect a party or person from annoyance, embarrassment, oppression, or undue burden." In addition, local rule of practice 47.1(B), D.C.COLO.LCivR, governs motions to seal. It provides in relevant part:

> **Motions to Restrict Access.** Any motion to restrict public access will be open to public inspection or as otherwise ordered. It shall identify the document or the proceeding for which restriction is sought. It shall be accompanied by a brief that will be filed as a restricted document (Level 1 or 2). The brief must:
> 1. Address the interest to be protected and why such interest outweighs the presumption of public access (stipulations between the parties or stipulated protective orders with regard to discovery, alone, are insufficient to justify restricted access); 2. Identify a clearly defined and serious injury that would result If access is not restricted; 3. Explain why no alternative to restricted access is practicable or why only restricted access will adequately protect the interest in question (e.g.,redaction, summarization, restricted access to exhibits or portions of exhibits); and 4. Identify the restriction level sought (i.e., Level 1 = access limited to the parties and the court; Level 2 = in a multi-defendant case access limited to the affected defendant, the filing party, government and the court; Level 3 =access limited to the filing party and the court; Level 4 = access limited to the court).

The decision as to access is one best left to the sound discretion of the trial court, a discretion to be exercised in light of the relevant facts and circumstances of the particular case. *Huddleson v. City of Pueblo, Colorad*o, 270 F.R.D. 635 (D.Colo. 2010)

The U.S. Supreme Court upheld a protective order issued under a state rule modeled on Federal Rule 26(c) in *Seattle Times Co.v.Rhinehart*, 467 U.S. 20, 104 S.Ct. 2199, 81 L.Ed.2d 17 (1984), stating

> There is an opportunity, therefore, for litigants to obtain -- incidentally or purposefully -- information that not only is irrelevant but, if publicly released, could be damaging to reputation and privacy. The government clearly has a substantial interest in preventing this sort of abuse of its processes.. . .The prevention of the abuse that can attend the coerced production of information under a State's discovery rule is sufficient justification for the authorization of protective orders.

Seattle Times Co., infra, at 36. where it concluded the First Amendment was not infringed by a protective order prohibiting the disclosure of information obtained through judicially compelled discovery of otherwise private information.

Disclosure of personal information linking public information such as name and address and telephone number with other more private aspects of a person's life, such as an individual's ISP Provider, IP address, personal computer number known as Media Access Control address, and e-mail address all pose problems. Identity theft has become rampant and the particular grouping of information requested to be disclosed to Plaintiff and the general public without any restrictions on what Plaintiff does with the information at the conclusion of this case is inviting trouble. Plaintiff not only has a right to privacy with respect to personal information, but certain IP addresses and telephone numbers are protected by federal law pursuant to the Telecommunications Act of 1996, as amended. These rights may only be protected by not allowing public disclosure of Defendant's name, address and telephone number to the general public pending a decision on whether joinder is proper in this case;(3) restricting linkage of Defendant's name, telephone number, e-mail address and computer Identifying information including IP address and MAC address solely to Defendant, the Court and the Plaintiff (Level 2).

Comcast, while not a party to this lawsuit, is aware of Defendants privacy rights to certain information. On its website, Comcast states,

> Section 702 of the federal Telecommunications Act of 1996, as amended, (the "Telecommunications Act") provides additional privacy protections for certain information related to our phone services. . .
>
> That phone information, when matched to your name, address, and telephone number is known as **customer proprietary network information** or CPNI for short. This notice, which includes our CPNI Policy, describes what CPNI information we obtain, how we protect it, and how it may be used. If you are a customer of our phone services, **you have the right, and Comcast has a duty, under the Telecommunications Act and applicable state law, to protect the confidentiality of CPNI.** We also honor any restrictions applied by state law, to the extent applicable

http://www.comcast.com/Corporate/Customers/Policies/CustomerPrivacy.htm (emphasis supplied)

Therefore, Defendant Doe requests that (1) no public disclosure of his personal information prior to a decision on whether joinder is proper, (2) that if and when joinder is determined to be proper, that any public disclosure be restricted to only his name and address and telephone number; (3) Any other information disclosed such as e-mail address, telephone number, MAC address should remain confidential and under level 2 access, that Plaintiff's use of this information is restricted to solely this matter, may not be distributed to anyone outside this case and Plaintiff should be directed to destroy such information at the conclusion of the case.

Respectfully submitted this 15th day of June, 2012.

The Klibaner Law Firm, P.C.

/David Klibaner/_____

David Klibaner
899 Logan, Suite 200
Denver, Colorado 80203
(303) 863-1445
david@dklawfirm.com

CERTIFICATE OF SERVICE

I hereby certify that on the 15th day of June 2012 I electronically filed the foregoing Declaration, Motion and Exhibits 1-8 with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following e-mail addresses:

Jason Kotzker
Kotzker Law Group
9609 South University Blvd.,
P. O. Box 632124
Highlands Ranch, CO 801163

/Pam Pritzel/
_____
Pam Pritzel