EXHIBIT M

Fotokopie

No du dossier de la Cour : T-

COUR FÉDÉRALE

ENTRE :

VOLTAGE PICTURES LLC

Demanderesse

-ET-

M. OU MME UNTEL

Défendeurs

AFFIDAVIT OF DANIEL ARHEIDT

I, Daniel Arheidt, a consultant of IPP Limited, of the City of Hamburg, Germany,

AFFIRM THAT:

1. I am a consultant in the litigation support department of IPP Limited ("IPP"), a German company that provides forensic investigation services to copyright owners.

2. As part of my duties for IPP, I routinely identify the Internet Protocol ("IP") addresses used by people who download, reproduce and distribute copyrighted works using the BitTorrent Protocol.

3. IPP has developed a proprietary technology platform that provides an effective means to detect the unauthorized distribution of movies and other audiovisual content over P2P networks by members of those networks who use a BitTorrent protocol.

4. Voltage Pictures LLC hired IPP to determine whether its film, *Hurt Locker*, was being copied and distributed by Canadian members of peer-to-peer ("P2P") online networks.

The BitTorrent Protocol

5. The BitTorrent protocol allows even small computers with low bandwidth to participate in large data transfers across a P2P network.

6. The initial file-provider will choose to share a file with a P2P network. This initial file is called a "seed."

7. Other P2P network users ("peers") connect to the seed file if they wish to copy it.

8. The BitTorrent protocol breaks a file into packets, which are individually downloaded to a peer. The protocol also directs each new peer to the most readily available packet. In this way, a peer will not copy a file directly and solely from the seed but may download individual packets from any peer who has previously copied the file and who has made it available to the P2P network.

9. As more and more peers request the same file, each additional peer automatically becomes a source for those packets of a file that he has copied. This speeds up the time it takes to download a file and frees up the capacity of a computer or server that would otherwise have to send a complete, large file to each peer.

10. Every peer who is copying or who has copied a file is simultaneously distributing it to every other peer.

Hurt Locker

11. Voltage Pictures LLC retained IPP to identify the IP addresses being used to reproduce and/or distribute Plaintiff's copyrighted works using the BitTorrent Protocol.

12. IPP asked me to implement, monitor, analyze, and attest to the results of, the investigation.

13. I ran forensic software named INTERNATIONAL IPTRACKER v1.2.1 and related technology, which scans P2P networks for the presence of copyrighted material.

14. The software searched P2P networks for files corresponding to *Hurt Locker* and then identified the peers who were offering the file for transfer or distribution. This information is available to anyone that is connected to the P2P network.

15. Once the software identified that *Hurt Locker* was being distributed over a particular P2P network, we obtained the internet protocol ("IP") address of each peer who was reproducing and/or distributing the movie. When available, we also obtained the peer's pseudonym or network name and examined the peer's publicly available directory for other files that lexically match *Hurt Locker*.

16. We then downloaded the copy of *Hurt Locker* that the peer was offering to the P2P network and distributing via the BitTorrent protocol.

17. At the same time, we downloaded other publicly available information to assist in identifying the peer. For instance, for every file we download, we are able to

record: (a) the date and time at which the file was distributed by the peer; (b) the IP address assigned to the peer by his internet service provider at the time of the distribution; (c) the video file's metadata, such as title and file size, that is not part of the video content but that is attached to the digital file.

18. We then created evidence logs for each peer and stored this information in a central database.

19. Schedule A to this affidavit ("Schedule A") lists those IP addresses and related information that was discovered during the *Hurt Locker* investigation.

IP Addresses

20. An IP address is a unique numerical identifier that is automatically assigned to an internet user by the user's Internet Service Provider ("ISP").

21. ISP's are assigned blocks or ranges of IP addresses. The range assigned to any ISP can be found in publicly available databases on the internet.

22. ISP's keep track of the IP addresses assigned to its customers at any given moment and retain "user logs" for a limited amount of time. These user logs provide an accurate means to match an IP address with a specific customer.

23. IPP can use IP addresses to track a peer to a particular ISP and, sometimes, to a particular geographic region. We determined that the defendants listed at Schedule A were customers of three Canadian ISP's: Bell Canada, Cogeco Câble inc., and Videotron s.e.n.c.

24. Once provided with the IP address, plus the date and time of the detected and documented activity, ISPs can use their subscriber logs to identify the names and addresses of their clients who acted as peers to copy and distribute unauthorized versions of *Hurt Locker*.

25. Only an ISP can correlate the IP address to the real identity of its subscriber.

Confirmation of Copied and Distributed Material

26. I personally extracted the data gathered from this *Hurt Locker* investigation.

27. After reviewing the evidence logs, I isolated the transactions and the IP addresses being used on the BitTorrent P2P network to reproduce and distribute *Hurt Locker*.

28. The IP addresses, hash values and hit dates contained in Exhibit A correctly reflect what is contained in the evidence logs.

29. In addition to identifying the labels and metadata attached to the P2P files to determine that a peer identified at Schedule A has copied and distributed *Hurt Locker*, IPP analyzed each BitTorrent "piece" distributed by the IP addresses listed at Exhibit A and verified that reassembling the pieces results in a fully playable digital motion picture.

30. I was provided with a control copy of the *Hurt Locker*, which members of my team viewed side-by-side with the digital media files set forth at Exhibit A and confirmed that they were the same.

Affirmed before me at the City of)
Karlsruhe, Germany, on 08-24-2011)
_____.)
)
)
)
)
)
)
)
)
Dr. Joachim Mellmann)
Notar)
_____)
Commissioner for Taking Affidavits)

DR. JOACHIM MELLMANN · NOTAR IN KARLSRUHE ·

Daniel Arheidt

This is Exhibit "A" referred to in the Affidavit of Daniel Arheidt, affirmed before me this 24th day of August, 2011.

Dr. Joachim Mellmann
Notar

A Commissionner for Taking Affidavits

DR. JOACHIM MELLMANN · NOTAR IN KARLSRUHE ·

EXHIBIT N

British pornographer Jasper Feversham was fed up. The Internets were sharing his films, quality work like Catch Her in the Eye, Skin City, and MILF Magic 3. He wanted revenge—or at least a cut. So Feversham signed on to a ...

Business
People and Technologies That Matter
- Intellectual Property
- Internet Culture & Etiquette

The 'Legal Blackmail' Business: Inside a P2P-Settlement Factory

- By Nate Anderson, Ars Technica
- 10.03.10
- 10:30 AM

British pornographer Jasper Feversham was fed up. The Internets were sharing his films, quality work like *Catch Her in the Eye*, *Skin City*, and *MILF Magic 3*. He wanted revenge—or at least a cut. So Feversham signed on to a relatively new scheme: track down BitTorrent infringers, convert their IP addresses into real names, and blast out warning letters threatening litigation if they didn't cough up a few hundred quid.

"Much looking forward to sending letters to these f—ers," he wrote in an email earlier this year.

The law firm he ended up with was ACS Law, run by middle-aged lawyer Andrew Crossley. ACS Law had, after a process of attrition, become one of the only UK firms to engage in such work. Unfortunately for Crossley, mainstream film studios had decided that suing file-sharers

brought little apart from negative publicity, and so Crossley was left defending a heap of pornography, some video games, and a few musical tracks.

Crossley parleyed the porn into national celebrity—or perhaps "infamy" would be a better word. Earlier this year, Crossley was excoriated in the House of Lords by Lord Lucas of Crudwell and Dingwall—yes, I know—for what "amounts to blackmail... The cost of defending one of these things is reckoned to be £10,000. You can get away with asking for £500 or £1,000 and be paid on most occasions without any effort having to be made to really establish guilt. It is straightforward legal blackmail."

Lord Lucas went on to offer an amendment to the (now-passed) Digital Economy Bill, titled "Remedy for groundless threats of copyright infringement proceedings."

But the Lords were just getting started. Lord Young of Norwood Green likened firms such as ACS Law to "rogue wheel-clampers, if I can use that analogy," while the Earl of Erroll railed against the way that "ACS Law and others threaten people with huge costs in court unless they roll over and give lots of money up front, so that people end up settling out of court. The problem is the cost of justice, which is a huge block. We have to remember that."

Lord Clement-Jones also called out Crossley's work. "Like many noble Lords, I have had an enormous postbag about the activities of this law firm. It is easy to say 'of certain law firms,' but this is the only one that I have been written to about... ACS seems to specialize in picking up bogus copyright claims and then harassing innocent householders and demanding £500, £650, or whatever—a round sum, in any event—in order to settle."

May go for a Lambo or Ferrari. I am so predictable!

That was only the start of Crossley's problems. In the last 12 months, Crossley has been targeted by the Blackpool municipal government, dogged by journalists, hounded by a major consumer group, and hauled up before the Solicitors Regulation Authority for disciplinary proceedings. Baffled, angry people write his office daily, denying any knowledge of his charges. He has blacklisted his own ex-wife in his e-mail client, demanding that she cut off all contact with him forever. Clients press him to pay up. His own data suppliers are, he fears, out to screw him, and Crossley harbors the suspicion that he could make far more money in America, where fat statutory damage awards mean he could demand even more cash from his targets.

And, just to put a ridiculous cherry atop his plate of problems, the streets department in Westminster, London—where Crossley keeps his office—went after ACS Law because some of their office waste mysteriously "ended up in the public highway."

"We are a tightly resourced small firm," Crossley complained as he wheedled the fine in half. But not *that* tightly resourced. Crossley bragged over e-mail earlier this year that he "spent much of the weekend looking for a new car. Finances are much better so can put £20-30k down. May go for a Lambo or Ferrari. I am so predictable!" He began looking at new homes, including a gated property with "five double bedrooms, three bathrooms, modern kitchen and four reception rooms."

Keeping track of all the details might not be Crossley's strong suit. As he wrote (one assumes in jest) when a dispute about financial issues came up, "I am not an accountant, true. But I am a genius and everything I do is brilliant. You must understand that!"

He's also dogged. With all the hate, a lesser man might have buckled—as did other law firms like Tilly Bailey & Irvine, which dropped its own "settlement letter" business in April 2010 after "adverse publicity." Instead, Crossley plows ahead, defending work like *To the Manner*

Porn and *Weapons of Mass Satisfaction*; indeed, he seems rather philosophical about his lot in life.

"Sorry to bombard you with more things to deal with," he wrote recently to a colleague, "but this business seems to have its share of complications." Indeed it does—and the complications get even more complicated when you anger the anonymous masses at 4chan, who promptly crash your website, expose your private e-mail, and in doing so shed a powerful and unflattering light on the real practice of P2P lawyering. Drawing on thousands of personal e-mails, Ars takes you inside the world of ACS Law, reveal its connections to the US Copyright Group, and discovers just what Andrew Crossley thinks of *Godfather 3*.

Spoiler: "*Godfather 3* is not quite as bad as I remember."

Operation Payback

"This will be a calm, coordinated display of blood," said the initial call to action. "We will not be merciful. We will not be newfags."

Users of the free-wheeling (to put it mildly) Internet community 4chan last week implemented "Operation Payback," a distributed denial of service attack against various anti-piracy groups the chanologists didn't like. The RIAA was hit. The MPAA was hit. But after some big targets, Operation Payback moved on to smaller firms, including ACS Law.

I have far more concern over the fact of my train turning up 10 minutes late or having to queue for a coffee than them wasting my time with this sort of rubbish.

After the group's data flood knocked the ACS Law website offline for a few hours, UK tech site The Register called up Andrew Crossley to ask him about the attack. The site was "only down for a few hours," Crossley said. "I have far more concern over the fact of my train turning up 10 minutes late or having to queue for a coffee than them wasting my time with this sort of rubbish."

He has something to be concerned about now. After these comments, Operation Payback hit ACS Law a second time, knocking out the site. In the process of bringing it back up, someone exposed the server's directory structure through the Web instead of showing the website itself. Those conducting Operation Payback immediately moved in and grabbed a 350MB archive of ACS Law e-mails, then threw the entire mass up on sites like The Pirate Bay.

This is more than a matter of mere embarrassment. The UK has tougher data protection laws than the US, and the country's Information Commissioner has already made it clear that ACS Law could be on the hook for hundreds of thousands of pounds. That's because, in addition to his iTunes receipts ("Hooray for iPads. I love mine," Crossley says at one point) and Amazon purchase orders, the e-mails include numerous attachments filled with all manner of private information: names, addresses, payment details, passwords, revenue splits, business deals. All of which is horrible, terrible, awful news—unless you want to know how a firm like ACS Law actually works.

Continue Reading ...

Meet the Accused

After reading through many hundreds of e-mails, one thing becomes clear: ACS Law operates a rather boring business. That is, there's no juvenile gloating, no sinister cackling, no profanity-laced tirades (OK, there are a few tirades). The dominant picture is of a sober operation that spends most of its time in mind-numbing scanning and database work. They even reply personally to letters. Sure, all this work is in the service of dreck like *Granny F—*,

but this is just a *business*, and Crossley is just a middle-aged solicitor trying to run an efficient operation.

But the effects of this operation on those accused of infringement are remarkable. The e-mail trove is stuffed with anguished pleas like this:

I was in total shock after receiving the letter I received from you today as explained in the telephone conversation. I will say that I was not the person responsible for this infringement. The only person who it could have been would be my son who is [name redacted]. I would never entertain the idea of downloading such a thing—in fact I do not even know how to download any type of software. I only use the internet for Ebay and emails. I also go on dating sites and facebook. This is where my knowledge of computers stops. I do not understand what P2P is....

At the time of the download, to my knowledge my son was visiting my home. I have no idea what he was looking at on my computer. I must add that I do not tolerate any such pornographic material. This letter has upset me greatly and I have spoken to my ex husband who also called yourself with regard to this matter.

Most of the notices seem to have gone to parents, as one would expect from a program targeting ISP account holders. But many of the parents seem baffled:

I have today received a legal notification from you that a pornographic film was downloaded from my internet connection in October 2009.I immediately phoned your contact number and was told to put my comments in writing. I am obviously shocked both at this alleged illegal activity and the fact that the title appears to be of an offensive nature. I can confirm that i have no knowledge of this download being carried out at my home address. I have checked my computer and my sons computer for any reference to this file (using windows search function) and have found no trace.I have spoken to my two sons about downloads (They are 8 and 12) but obviously not about the nature of this file and to be honest they know even less than me. My oldest child has used i tunes and downloaded games from a site called friv.com but these claim to be free. Is this true? or will it also result in copyright issues ?

Others are offended at the titles they are accused of sharing:

I am no prude and can see what type of material something entitled *Granny F*— is. I am the father of 5 children, 3 of these under the age of 7, and to suggest i would have such material on a computer is what i find offensive. May i also add that i am very anti pornography, having been abused as a child by someone who would use porn films before abusing me .this is why i am totally anti porn.

Then come the "innocent infringers," though some of these explanations can feel a bit... strained.

on the date 16-11-2009 at 16.35 i was browsing the internet namely bt junkie ,without going into a long story i accidentely pressed the download button for the copyright protected file british granny f— 5@6 which then opened my bittorrent client on my pc which the torrent is sent to with the forementioned file is attached. It normally takes a few minutes for the file to start downloading and before it did i realised what i had done and canceled the file preventing any copyright infringement from taking place. just by starting the download process would have been enough to leave my ip address listed. I hereby appologise for any inconvienience i have caused yourself or your client and can swear at no time was any part of the forementioned copyright protected file downloaded onto my pc or shared with anyone else.

(I mean, haven't we all, at one time or another, accidentally been browsing BitTorrent sites

and accidentally clicked on a film called *Granny F*—?)
Others took responsibility for their actions:
I am writing in response to the recent letter my father [name redacted] received on the 13.04.2010 based on the subject of infringement of copyright. I would firstly like to state that I am solely responsible for this and I [name redacted] take full responsibility. I have read through all the information that you have supplied and I understand how serious the matter is—since last year 2009 I have not downloaded any material as I understood how it was a bad thing to do and how it is killing out industry.
I do take responsibility for this issue and I would very much like to ask if the required payment of £495 could somehow possibly be reduced. The reason i am asking this is because I am currently a student and money is a big factor and getting by generally is a hard thing to do.
Indeed, many of the guilty appear to be kids. Some parents figured it out:
"I would also like to also say that it was not my sons intention to fileshare this music and was unaware of how file sharing works as am I—I appreciate that this is no excuse but ask you to bear this in mind. As mentioned in previous correspondence from myself I am writing to again explain that my financial circumstances make it impossible for me to pay £400 in one go or even at £40 per month I am in extreme financial hardship with mounting debts and do not have any spare money – if you were to take this to court I would be unable to even pay the basic utility bills or even the necessary food bills.
If there's one great theme running through these letters, it's the poverty of the respondents. One is a "a single mum living of state benefits who cannot afford to pay any kind of money my daughter is very sorry for any problems caused," while another lives "in the hold of my bank overdraft my money is never my own. We at present find it very hard to make ends meet, at the moment I am trying to amass funds to pay our utility bills for this month and can not see any change in the near future." Students plead hardship due to school fees; many people claim to be unemployed.
But perhaps most creative are the letters that make no attempt at argument. These are sheer vitriol. One stands out among the rest:
Go f— your mum you stupid pakistani black jew. You zimbabwean immigrant.
So listen up fat f—, don't send me another letter. If you do send me another f—ing letter, I will rape your mum against the wall and I will blow up your house and kill you all in a terrorist attack.
In addition, I want a £3500 cheque written to me for the inconvinience [sic] you have caused me.
If you do not reply to this email with a confirmation that you will pay me, I will hunt you down and stab you in the back and blow your d— up.
Creative, in an unhinged way. If you had thoughts about going into P2P litigation, consider the sheer migraine-inducingness of getting such messages on a daily basis. Indeed, after reading the correspondence, it's not hard to see why one paralegal who worked at ACS Law during the summer of 2010 told a friend there was "no chance in hell" she would go back.
Continue Reading ...

In Which Everyone Complains

When you make people this angry, they tend to complain—and that's just what happened to Crossley. Earlier this year, UK Consumer group Which? noted that it had "heard from more than 150 consumers who believed they had been wrongly accused." One letter writer said, "My

78 year-old father yesterday received a letter from ACS law demanding £500 for a porn file he is alleged to have downloaded. He doesn't even know what file sharing or bittorrent is so has certainly not done this himself or given anyone else permission to use his computer to do such a thing."

Reporters began following up on such stories. One reporter, from the *Daily Echo* in Bournemouth, e-mailed Crossley about a particular local case—an Aberdeen man who spent most of his time near Bournemouth caring for an ill relative.

"He is accused of downloading the track '*Evacuate the Dancefloor*' on October 2 last year," write the reporter. "Mr [name redacted] says he was in Dorset at the time, not in Aberdeen where his IP address is registered, and that he has airline tickets and medical appointment records to prove it. He says he leaves his internet connection switched off when he's away and no one else has access to it. He has no interest in pop music."

There were other problems. One of the firms providing Crossley with data on infringers then began to get balky, wanting more money than Crossley wanted to pay before turning over its information. "This guy is stupid," Crossley noted in an email to a colleague. "And he MUST release ALL data to us. It is ours. We have a deal. I will go to court this afternoon if he does not give it to us."

As if this wasn't enough, Crossley was subject to repeated, probing questions from the Solicitors Regulatory Authority, which controls lawyers in England and Wales. The group had received 400+ complaints about his firm's behavior. This was a big deal; the SRA could put Crossley out of business, and he had been in trouble with them before.

Back in 2002 and 2006, Crossley was disciplined by the Solicitors Disciplinary Tribunal, which ordered him to pay around £5,500 in fines and penalties. In both of these cases, Crossley had not submitted an accountant's yearly report on his firm—needed under UK rules to show that a lawyer does not improperly hang on to client funds.

The problem appeared to stem from a lack of cash. At one point, he told the tribunal handling his case that his lack of paperwork was "because he had been unable to raise the money to pay the accountant who retained the papers."

Crossley suffered "an extended period of clinical depression in 1999″ and then a stroke in 2000. "The effect of the stroke, which caused him to lose his sight altogether for a brief period, was that the Respondent could not work full-time for a period and as a consequence he quickly got into financial difficulties."

Any bundle of documents sent by a law 'firm' headed with the words 'Letter of claim; Infringement of Copyright' is likely to cause distress

The new investigation wasn't about accounting, but about claims that Crossley was shaking down his targets. Things were bad enough that one of his ACS Law employees noted, "We are constantly being reminded by infringers that we are under investigation by the SRA."

To defend himself, Crossley secured the services of another lawyer. "I am meeting with my retained lawyer today regarding the sra," he wrote. "He is Andrew Hopper QC and he literally wrote the sra rules!"

But Andrew Hopper, QC couldn't save Crossley from the SRA, even if he did write their rules. On August 20, the SRA referred Crossley—once more—to the disciplinary tribunal.

"Absolutely predictable political decision to 'fast track' and give the problem to someone else; therefore SRA is seen by Which etc to be 'doing the right thing' without them actually having to think at all or justify the decision," sniffed Hopper.

The Blackpool municipal government also objected to Crossley's tactics. ACS Law was contacted by Blackpool, which complained that local citizens "have been significantly distressed by your letter and feel compelled to pay. You say that your letters are not demands but compromise agreements, but any bundle of documents sent by a law 'firm' headed with the words 'Letter of claim; Infringement of Copyright' is likely to cause distress and mislead the consumer into making a transactional decision they would not otherwise make... None of the complainants have any recollection of having downloaded the tracks in dispute."

The Blackpool official then notes that under UK law, damages are fixed at "economic loss, either realized or potential." When it comes to music tracks, the loss equals "the approximate market value of the track as a single download—79p. Without further transparency as to the legal costs mentioned above, I would imagine that this would be sufficient to bring the matter to a close."

Meet the U.S. Copyright Group

Indeed, the justice of this remark about damages haunts Crossley. One of his own legal advisers tells him that "establishing damages beyond the value of the gross profit of one copy of the work is problematic." In other words, a few pence for music. The advisor goes on to note that the one court case which would seem to prove the opposite "has, in my opinion, about as much legal force as a *Sun* newspaper headline regarding the licentious behavior of a D list celebrity."

We should get to work on this, I have massive copyright in the US. And in the US there is minimum statutory damages

"Therefore, it is my belief that the rights holder can only rely on the damage resulting from making a single copy of the work in infringement," he concludes, because of the difficulty in proving just how much (if any) "sharing" of the material with others took place. Lawyers are of course free to ask the courts for huge awards, but this carries the risk "that, in a defended case with competent opposing expert witnesses, the court will reject the application."

In other words, actually *going to court* would net very little money. Sending out letters and collecting a few hundred pounds is a much better business, which may explain why Crossley doesn't seem to sue people who refuse to settle. Yes, he promises to do so at some point, and the emails do show that he's considering hiring a litigator, but the campaign has been going over for quite some time now with no court action. (This is a common theme in the complaints against him; Crossley insists he's just trying to help everyone stay out of court.)

If only Crossley lived in America! "What is interesting is that it is the US model I want," he wrote earlier this year after hearing the news that the US Copyright Group was now filing mass Doe lawsuits against alleged movie pirates. "We should get to work on this, I have massive copyright in the US. And in the US there is minimum statutory damages."

Yes, statutory damages—under which copyright holders don't need to prove actual economic harm at all. The idea was that some infringement was simply too hard to quantify, but a system designed for commercial use has now been turned against US college students, leading to $1.92 million judgments in one case and $675,000 in another. (Both were so egregious that the judges involved tossed out the monetary amounts.) This is the system Crossley wants to profit from.

So he contacted Tom Dunlap of the Virginia law firm Dunlap, Grubb, and Weaver (DGW). DGW helped put the "US Copyright Group" together and does all the litigation on its cases, which include films like *The Hurt Locker* and *Far Cry*. Crossley wanted some kind of

partnership.

"I own and operate the most prolific firm in the UK that identifies and pursues copyright infringements committed through peer to peer networks," he bragged to Dunlap. "I have a growing number of clients, existing and potential, including US based copyright owners and are actively looking to expand our work into the US, especially because of the ability to receive statutory damages for infringement and jury-awarded assessments of damages. I note that you act for Guardaley, a client of the person who introduced the file sharing work previously carried out by Davenport Lyons in the UK to my firm. It is a small world!

"I have substantial amounts of data, which I wish to exploit appropriately in the US and would very much like to speak with you with a view to exploring the possibility of an ongoing working relationship, to our mutual benefit. If this is of interest to you, please let me know."

The lawyers did a call. Later, they met up in Cannes, France at a conference. Crossley later booked a table at Le Baoli, which he described in another email to someone else as "the best club I have ever been in in my life! Le Baoli in Cannes! a million models in one place!" But the club was not serving dinner that night, and in the confusion over rescheduling, Crossley missed the DGW lawyers for dinner. But he did email later to say that "we are mailshotting all major uk film and music companies with the ucg [US Copyright Group] so you should get some calls soon." He seems to have believed a partnership was in the offing.

In a blog post soon after, Crossley announced his return from Cannes and said that "a new joint working relationship with US-based attorneys has opened up the North American region to our clients for identification and pursuit of illegal file sharing of their products." He was going to begin "cooperation with a newly-formed organization, the United Copyright Group." That reference was scrubbed from the post two days later; Crossley had apparently been a bit too exuberant. Tom Dunlap told Ars that his firm was not working with ACS Law. He also told CNET this week that "the IT company [which the law firm uses to track file sharers] does not do anything for ACS Law."

But is that true?

Continue Reading ...

The Mysterious "Guardaley"

The "IT firm" Dunlap mentions appears to be Guardaley, the BitTorrent detection company cited in US Copyright Group court filings. Guardaley identifies the IP addresses of suspected infringers, logs all necessary data, and turns this information over the lawyers. But the firm is deeply implicated in the US Copyright Group, not just a mere contractor.

Guardaley is based in Germany, where it is run by Bejamin Perino and Patrick Achache, though the firm has registered itself as a UK business, too, with an unlikely address in an Aldermaston office park.

In a document (PDF) filed with the White House's new "IP Czar" earlier this year, Perino is listed as the "managing director" of Guardaley, and Dunlap called on the expertise of his subordinate Achache as an expert witness who swore to the accuracy of the company's data in court filings. But then, in April of this year, another court filing appeared in the *Far Cry* case. Here, Perino declared that he was "one of four Managers of the US Copyright Group (USCG) which is a private company dedicated to anti-piracy efforts in the motion picture industry involving unlawful torrent downloading."

Virginia state records seen by Ars show that DGW set up "US Copyright Group" as a legal entity, though it appears to be some sort of partnership between the law firm and the techies

at Guardaley.

Here's where it gets weird: this summer, after falling out with his detection company, Crossley turned to a young man named Terence, who is referenced above and who helped Crossley get into the settlement letter business. Terence then helped Crossley sign on with... Guardaley. Crossley writes about a "guy I know called Patrick who is good friends with Terence. Patrick is based in Germany with a high quality system. We get no hidden charges and I will drop my charges to fully absorb the extra cost."

He needed to rush the deal through, because the pornographer Jasper Feversham was upset that detection of his works had stopped; Crossley needed a new data supplier as soon as he could get one.

The deal, for 15 percent gross, was done through Terence; no emails emerge from Guardaley at all. Even Crossley found the situation odd. "Also, I note that Guardaley in the UK is registered as a dormant company. That needs to be changed if that is the contracting company. And why is there a company in the UK and why its it registered in Aldermaston? What's all that about? (as Peter Kay would say)."

In response, Terence offers some intriguing details. "GL [Guardaley] has a number of companies for monitoring and different ones are used depending on content and jurisdiction. The data supplier for [ACS Law client] Mediacat will be a Swiss company to manage PR (you know how it is!)."

Despite using the same tech, Guardaley apparently operates under numerous names. This means that each of the entities it creates needs a separate "expert's report" verifying that the system is accurate. The one drafted for Guardaley itself wouldn't work; a new expert must be found.

"An independent expert's report is in place for Guardaley, but your monitoring will be done through a different legal entity," wrote Terence. "This will mean that we will need to get a new one created. There will be no problems, as the technology used will be exactly the same as Guardaley's." And later: "We are in correspondence with an expert and the report can be finalised fairly quickly, well in advance of the first court order."

So, while Tom Dunlap suggests that "Guardaley" doesn't work for ACS Law, some other company with a new name and the same tech is. This gives Guardaley a hand in the two major "settlement letter" factories in the United States and Britain.

Follow the Money

Why bother with all these hassles, all the vitriol, all the criticism from the House of Lords? Money, for one. Despite Crossley's claim that he runs a "tightly resourced small firm," he appears to be doing alright for himself. After bragging about getting a "Lambo or Ferrari," Crossley instead settled on a Jeep Compass 2.4CVT.

He spent the summer looking for a new high-end home to rent; one property send over for his consideration was "a contemporary mansion with breath taking views in an elevated position on this exclusive gated estate. Arranged over three floors the accommodation comprises entrance hall, cloakroom, kitchen/breakfast room, utility room, large dining room, lounge with doors out onto patio and balcony and double bedroom suite. Stairs down to family room, four double bedrooms, shower room, family bathroom. Stairs down to indoor swimming pool, bar area/gym with doors out onto patio, double bedroom suite and storage room, double garage." Such places go from £6,000 to £8,000 a month; not a modest sum.

And he's looking to buy a bulldog puppy.

But despite the expenditures, there are also some signs that cash does not flow steadily in this business. “You seem to have ignored my previous e-mail, I am not happy and want some revenue in account,” demands one client. “Everyone is getting their bit and I am owed £17k ffs.”

He also pleads with one of his data suppliers to do some work for him, and quickly. “We need to run that data to maintain cashflow,” he wrote. “Meanwhile, we have come under considerable pressure from [UK Internet provider] O2 to pay an outstanding invoice of £13,107.00 in respect of the supply of that data. As we have not been able to send any letters out we have not been able to collect any income from that data to meet ISP costs. This matter is very pressing as O2 have said that unless it is paid straight away they will release all their staff that they have retained to provide the data. This will have the effect of delaying very considerably the time for the provision of the finished data from the ISP. This will impact on al of us, most importantly for cashflow.”

In an operation like this, the letters need to keep flowing out for the money to keep flowing in. As Crossley noted after seeing all the confusion among alleged infringers, “I have an idea. We should send a factsheet.... answering all the usual questions and dispelling some common misapprehensions as I think it will better inform people and increase revenue.”

But that revenue comes from confused people like the accountant who wrote ACS Law, claiming utter bafflement and innocence. “Due to a lack of detail in your letter, I had to Google search the title to find information on what I’m being accused of downloading. I was astounded to find it to be PORN of pregnant women. Sick!”

“I am an Accountant who works normal office hours. There is NO CHANCE I would be at home downloading porn at 11:43 in the morning. Furthermore, on the date stipulated, I was in Brighton for the day with a client. I am the owner of my home, I live alone and have being doing so at the current address for the past 4 years. No-one has access to my property unless I’m present.”

But the attitude at ACS Law is, as one legal advisor put it, “I sometimes think that we try to be too nice. That is not our purpose. If our clients want nice then they are likely to go to a priest or social worker.”

So the Lords can say what they like, the consumer groups can rail, and Westminster can levy fines for trash in the streets, but the letters for *Pump Fiction* will continue.

Pages: 1 2 3 4 View All

Nate is a senior editor at Ars Technica, where he covers technology law, politics, and culture. He holds an MA in English literature from the University of North Carolina, where he also taught freshmen how to craft sentences, think clearly, and use semicolons. (Surprisingly, the

semicolons proved most difficult.) In his free time, Nate has written a pair of novels and read plenty more; he one day hopes to meet in the flesh another reader of twelve volumes of Anthony Powell's Dance to the Music of Time.
Read more by Nate Anderson, Ars Technica

Tags: P2P
Post Comment | 21 Comments | Permalink
Back to top

Comments for this thread are now closed.

21 Comments Wired: Business Login

Sort by Best Share Favorite

smithjohn0880 • 3 years ago
In my perception that article has a grade theme which reflect about he wrote in an email earlier this year.
****
smith
Conveyancing Solicitors
• Share ›

eMacPaul • 3 years ago
He's looking to buy a bulldog puppy?! Say it ain't so! Seriously, is that something that only evil, exorbitantly wealthy lawyers can do?
• Share ›

LandShark • 3 years ago
What I pity the most is all those grannies performing for naught.
• Share ›

thefixer • 3 years ago
Anon=FAIl, and 4 the record, they did NOT deface teaparty.org, they just flooded the uploads section with random anonfaggotry
• Share ›

luckystriker • 3 years ago
Is page 2 broken for anyone else?
• Share ›

neverseenthesun • 3 years ago
The problem that these morons will have is that most intelligent people us a program like hotspot shield to hide their ip... so guess what if 4chan starts using their office ips to download these titles they might start to understand what they are really upagainst.
• Share ›

nautilus68 • 3 years ago
Sounds like P2P is another cash cow for them. Its appalling what he does is not a crime. basically sending out blackmail, pay me $500 or lose $10,000 in court cost. Its legal fraud. I can see this will be the a new con scheme coming from people from Nigeria. Just send

EXHIBIT O

UNITED STATES DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

ACHTE/NEUNTE BOLL KINO BETEILIGUNGS GMBH & CO KG	)	
Plaintiff,	)	
v.	)	**CA. 1:10-cv-00453-RMC**
DOES 1 – 2,094	)	
	)	**Next Deadline: N/A**
Defendants.	)	

DECLARATION OF PATRICK ACHACHE IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO RULE 26(f) CONFERENCE

I, Patrick Achache, declare:

1. I am Director of Data Services for Guardaley, Limited ("Guardaley"), a company incorporated in England and Wales under company number 06576149, where I have been employed since January of 2007. Guardaley is a leading provider of online anti-piracy services for the motion picture industry. Before my employment with Guardaley, I held various software developer and consultant positions at companies that developed software technologies. I have approximately ten (10) years of experience related to the protocols, technical architecture and operation of the Internet.

2. I submit this declaration in support of Plaintiff's Motion for Leave to Take Discovery Prior to Rule 26(f) Conference. This declaration is based on my personal knowledge, and if called upon to do so, I would be prepared to testify as to its truth and accuracy.

3. At Guardaley, I am the head of the department that carries out evidence collection and provides litigation support services. I work closely with our development team to create credible techniques to scan for, detect, and download copies of copyrighted material on multiple network protocols for use by copyright owners.

4. Guardaley has developed a proprietary technology platform that provides an effective means to detect the unauthorized distribution of movies and other audiovisual content and files over online media distribution systems, or "peer-to-peer" ("P2P") networks. Guardaley's technology enables it to detect and monitor the unlawful transfer and distribution of files amongst the P2P network by a "BitTorrent protocol" or "torrent" which is different than the standard P2P protocol used for such networks as Kazaa and Limewire. The BitTorrent protocol makes even small computers with low bandwidth capable of participating in large data transfers across a P2P network. The initial file-provider intentionally elects to share a file with a torrent network. This initial file is called a "seed". Other users ("peers") on the network connect to the seed file to download. As yet additional peers request the same file, each additional user becomes a part of the network from where the file can be downloaded. However, unlike a traditional P2P network, each new file downloader is receiving a different piece of the data from each user who has already downloaded the file that together comprise the whole (this piecemeal system with multiple pieces of data coming from peer members is called a "swarm"). So every downloader is also an uploader. This means that every "node" or peer user who has a copy of the infringing copyrighted material on a torrent network must necessarily also be a source of download for that infringing file.

5. This distributed nature of BitTorrent leads to a rapid viral spreading of a file throughout peer users. As more peers join the swarm, the likelihood of a successful download increases. Because of the nature of a BitTorrent protocol, any seed peer who has downloaded a file prior to the time a subsequent peer downloads the same file is automatically a source for the subsequent peer so long as that first seed peer is online at the time the subsequent peer downloads a file. Essentially, because of the nature of the swarm downloads as described above, every infringer is

simultaneously stealing copyrighted material from many ISPs in numerous jurisdictions around the country.

6. The Plaintiff in this action is producer and distributor of motion pictures. The Plaintiff engaged the United States Copyright Group to, among other tasks, document evidence of the unauthorized reproduction and distribution of the copyrighted motion picture to which Plaintiff holds the exclusive distribution and licensing rights, *"Far Cry"*, within the United States of America, including the District of Columbia.

7. USCG, in turn, retained Guardaley to monitor and identify copyright infringement of Plaintiff's copyrighted motion picture on P2P networks. On behalf of Plaintiff, we engaged in a specific process utilizing Guardaley's specially designed software technology to identify direct infringers of Plaintiff's copyright using BitTorrent protocol on P2P networks.

8. All of the torrent infringers named as Doe Defendants were identified in one of two ways. We either: (1) searched for files corresponding to Plaintiff's motion picture title *"Far Cry"* and then identified the users who are offering the files for unlawful transfer or distribution; or (2) reviewed server logs obtained from P2P networks to determine the users who were offering the files of this copyrighted movie. In the first identification method, we used the same core technical processes that are used by the P2P users on each respective network to identify users who are offering the *"Far Cry"* motion picture files on the network, or to directly locate the files of the film. In the second identification method, we reviewed the same data that would be available to the operator of a server that is part of the P2P network. Under the first method of identification, any user of a P2P network can obtain the information that is obtained by us from the P2P network. Under the second method of identification, any operator of a server that is part of the P2P network can obtain the information that is obtained by us from the P2P network.

9. Once Guardaley's searching software program identifies a file that is being offered for distribution using BitTorrent protocol that corresponds to the motion picture for which Plaintiff owns the exclusive licensing and distribution rights, *"Far Cry", or* once such a file is identified directly from our search or our review of server logs, we obtain the Internet Protocol ("IP") address of a user offering the file for download. When available, we also obtain the user's pseudonym or network name and examine the user's publicly available directory on his or her computer for other files that lexically match Plaintiff's motion picture. We then download the motion picture that the user is offering using BitTorrent Protocol. In addition to the torrent file of the motion picture itself, we download or otherwise collect publicly available information about the network user that is designed to help Plaintiff identify the infringer. Among other things, we download or record for each file downloaded: (a) the time and date at which the file was distributed by the user; (b) the IP address assigned to each user at the time of infringement; and, in some cases, (c) the video file's metadata (digital data about the file), such as title and file size, that is not part of the actual video content, but that is attached to the digital file and helps identify the content of the file. We then create evidence logs for each user that store all this information in a central database.

10. An IP address is a unique numerical identifier that is automatically assigned to a user by its Internet Service Provider ("ISP") each time a user logs on to the network. Each time a subscriber logs on, he or she may be assigned a different IP address unless the user obtains from his/her ISP a static IP address. ISPs are assigned certain blocks or ranges of IP addresses. ISPs keep track of the IP addresses assigned to its subscribers at any given moment and retain such "user logs" for a very limited amount of time. These user logs provide the most accurate means to connect an infringer's identity to its infringing activity.

11. Although users' IP addresses are not automatically displayed on the P2P networks, any user's IP address is readily identifiable from the packets of data being exchanged. The exact manner in which we determine a user's IP address varies by P2P network.

12. An infringer's IP address is significant because it is a unique identifier that, along with the date and time of infringement, specifically identifies a particular computer using the Internet. However, the IP address does not enable us to ascertain with certainty the exact physical location of the computer or to determine the infringer's identity. It only enables us to trace the infringer's access to the Internet to a particular ISP and, in some instances, to a general geographic area. Subscribing to and setting up an account with an ISP is the most common and legitimate way for someone to gain access to the Internet. An ISP can be a telecommunications service provider such as Verizon, an Internet service provider such as America Online, a cable Internet service provider such as Comcast, or even an entity such as a university that is large enough to establish its own network and link directly to the Internet.

13. Here, the IP addresses Guardaley identified for Plaintiff enable us to determine which ISP was used by each infringer to gain access to the Internet. Publicly available databases located on the Internet list the IP address ranges assigned to various ISPs. However, some ISPs lease or otherwise allocate certain of their IP addresses to other unrelated, intermediary ISPs. Since these ISPs consequently have no direct relationship -- customer, contractual, or otherwise -- with the end-user, they are unable to identify the Doe Defendants through reference to their user logs. The intermediary ISPs' own user logs, however, should permit identification of the Doe Defendants. We determined that the Doe Defendants here were using those ISPs listed in Exhibit A to the Complaint filed in this matter together with various other ISPs operating both

within and outside the District of Columbia, to gain access to the Internet and distribute and make available for distribution and copying Plaintiff's copyrighted motion picture.

14. We downloaded the motion picture file and other identifying information described above and created evidence logs for each Doe Defendant. Once we identified the ISP used by the Doe Defendants to gain access to the Internet from the IP address, USCG sent an e-mail to the relevant contact at each ISP informing them of the Doe Defendant's IP address and the date and time of the infringing activity. That e-mail message requested that each ISP retain the records necessary to identify its subscriber who was assigned that IP address at that date and time. Once provided with the IP address, plus the date and time of the infringing activity, the Doe Defendant's ISPs quickly and easily can use their respective subscriber logs to identify the name and address of the ISP subscriber who was assigned that IP address at that date and time.

Confirmation of Downloaded Material

15. I am also responsible for identifying on-line piracy of motion pictures for Guardaley, including gathering evidence of on-line piracy to support counsel's copyright protection enforcement efforts.

16. As part of my responsibilities at Guardaley, I have been designated to confirm that the digital audiovisual files downloaded by Guardaley are actual copies of the motion picture entitled *"Far Cry"*. It is possible for digital files to be mislabeled or corrupted; therefore, Guardaley (and accordingly, Plaintiff) does not rely solely on the labels and metadata attached to the files themselves to determine which motion picture is copied in the downloaded file, but also to confirm through a visual comparison between the downloaded file and the motion picture itself.

17. As to Plaintiff's copyrighted motion picture entitled *"Far Cry"*, as identified in the Complaint, I or one of my assistants have watched a DVD or VHS copy of the motion picture provided by Plaintiff. After Guardaley identified the Doe Defendants and downloaded the motion pictures they were distributing, we accessed the downloaded files using Guardaley's proprietary software application, which stores the files downloaded. We opened the downloaded files, watched them and confirmed that they contain a substantial portion of the motion picture identified in the Complaint.

18. Plaintiff's motion picture entitled *"Far Cry"* continues to be made available for unlawful transfer and distribution using BitTorrent protocol, in violation of Plaintiff's exclusive licensing and distribution rights, and rights in the copyright. USCG and Guardaley continue to monitor, on an on-going and continuing basis, such unlawful distribution and transfer of Plaintiff's motion picture and to identify infringers by the unique Internet Protocol ("IP") address assigned to them by their respective ISPs on the date and at the time of the infringing activity.

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

Executed on 31.12.09, ____, at Karlsruhe.

P. Achache

Patrick Achache

databot economic data - Patrick Achache

Patrick Achache
Of Germany in **Karlsruhe, DE**

Facts

Home	Germany
Location	Karlsruhe, DE
GL mandates	3 seats
Investments	CHF 20'000 .00 (1 company)

Feedback / Error Report

Location

Overview | Investments 1 | 2 companies | Publications 3 | Composition 3

SOGC publications

SHAB No 42 of 1.3.2011 p. 35 Publ 6.055 million

BP Equity GmbH, in Walchwil, CH-170.4.009.565-1 , a limited liability company (SHAB No. 48 of 10.03.2010, p. 21, Publ 5,533,518)
new. Statutes Amendment 1.28.2011.: Company
IP Equity GmbH . translations of the new company: (IP Equity Sarl) (IP Equity Sagl) (IP Equity Co Ltd liab.). New Releases: Releases made to the shareholders by mail, e-mail or fax. [Further modification not requiring publication facts]. [With amendments to the articles of 01.28.2011 was secondary aim of the company changed
the.]. Registered persons new or mutating
Bolliger, Stephan , of Zurich, Dietikon, managing director with single signature; Achache, Patrick , a German national, in Karlsruhe (DE), Chairman of the Board, with single signature and shareholders, with single signature, with 200 ordinary shares of CHF 100.00 [previously: in train, managing director with single signature and members with individual signature].

SHAB No 48, 03.10.2010 p. 21 Publ 5,533,518

BP Equity GmbH (BP Equity Sarl) (BP Equity Sagl) (BP Equity Ltd liab co.), In Walchwil, CH-170.4.009.565-1 , Wihelstrasse 9, 6318 Walchwil, limited liability company (new
registration). statutes Date
02:03 . .2010
Purpose: To
fund projects in software and entertainment, and provision of insurance services; whole purpose of description according to
statutes. Share capital
20,000 .00. CHF
Publication organ:
SHAB. Notices to the shareholders in writing or by e-mail. According to statement by the company on 18/01/2010 under the Company no regular audit and dispense with a limited
audit. Registered persons
Achache, Patrick , a German national, in train, managing director with single signature and shareholders, with single signature, with 200 ordinary shares of CHF 100.00.

SHAB No 196 from 09.10.2009 p. 24 Publ 5,285,866

Intersda GmbH (Intersda Sarl) (Intersda Sagl) (Intersda Co Ltd liab.), In Walchwil, CH-170.4.009.208-8 , Wihelstrasse 9, 6318 Walchwil, limited liability company (new
registration). statutes Date
9/29/2009
purpose. :
provision of services in information technology, including advice and support; whole purpose of description according to
statutes. Share capital
20,000 .00. CHF
Publication organ:
SHAB. Notices to the shareholders in writing or by e-mail. According to corporate statement dated 29.09.2009 under the Company no regular audit and dispense with a limited
audit. Registered persons
Achache, Patrick , a German national, in train, managing director with single signature and shareholders, with single signature, with 200 ordinary shares of CHF 100.00.

Google Translate

http://translate.google.com/translate?u=http%3A%2F%2Fswiss-registers.info%2Fcompany_detail.aspx%2FCH17040095651--BP-Equity-GmbH--W

Google

Social Justic...) at Discogs | Freeze! You ...- Mobiledia | Miami-Dade ...nformation | Haute-Law.com | The Copyrig... of the USA | Class Action...of Contents | A Tale of Tw...| DuetsBlog

Google translate http://swiss-registers.info/company_detail.aspx/CH17040095651--

View: Translation Original

From: Detect language To: English Translate

swiss-register.ch

> Home
> News
> Business
> People
> Domain
> Contact

AdChoices

Google™ Benutzerdefinierte Suche Search

Equity GmbH BP (BP SA Equity) (Equity Sagl BP) (BP Equity Ltd liab. Co) Walchwil

, 6318 Walchwil

current people / interests

03/01/2011 Patrick Achache German national
03/01/2011 Stephan Bolliger Zurich
10/03/2010 Patrick Achache German national
all people ...

Web results for Equity GmbH BP (BP SA Equity) (Equity Sagl BP) (BP Equity Ltd liab. Co)

Web Search

Equity GmbH BP BP BP SA Equity Equity Equity Sagl BP Ltd. liab. Co in CH-170.4.009.565-1 Walchwil Wihelstrasse 9 6318 Walchwil limited liability company ...
Ups on 10/03/2010 - ZG http://www.moneyhouse.ch/shab/2010_048/neugruendungen_ZG.htm

BP Equity GmbH, CH-170.4.009.565-1 Walchwil ... New company IP Equity GmbH. Translations of the new company equity Sàrl IP IP IP Sagl Equity Equity Ltd liab. Co.
Commercial register of 01.03.2011 - I http://www.moneyhouse.ch/shab/2011_042/publikationen_i.htm

All-Tech Services SA in Lutry GmbH CH-550.1.054.222-4 ... BAVERI Financial Services Ltd liab. Co wound up in ... BP Service GmbH Hodi Emmen North Branch ...

1598

from the Swiss Commercial Register

last update 03/03/2011 register.ch **swiss-HR-6055000.xml 20,110,301** - New Releases: Notices to the shareholders by mail, e-mail or fax. [Also not change the facts subject to publication]. [With the amendment of Articles of Incorporation was amended 28/1/2011 secondary aim of the society.]. Peoples registration new or modified: Bolliger, Stephan, of Zurich, Dietikon, managing director with single signature; Achache, Patrick, a German national, in Karlsruhe (DE), Chairman of the Board, with single signature and shareholders, with single signature, with 200 ordinary shares to of CHF 100.00 [previously: train, managing director with single signature and members with single signature]. **HR-20100310-5533518.xml** - CH-170.4.009.565-1, Wihelstrasse 9, 6318 Walchwil, limited liability company (new registration). Statutes Date: 02.03.2010. Purpose: To fund projects in the areas of software and entertainment and the provision of insurance services; whole purpose according to paraphrase statutes. Share capital: CHF 20 000.00. Official publication: SOGC. Notices to the shareholders in writing or by e-mail. According to statement by the company on 18/01/2010 under the company is no regular audit and waives a limited audit. Registration: Achache, Patrick, a German national, in train, directors, and shareholders with an electronic signature, with single signature, with 200 ordinary shares of CHF 100.00.

More Domains
Reverse Whois
History Details
Get Notified
Trademark Monitor
Screenshot History

Whois Record For IntersDa.com

Whois Record Site Profile Registration Server Stats My Whois Like 2K

Reverse Whois: **"InterSDA GmbH" owns about 3 other domains**
Email Search: achache@intersda.com is associated with about **4 domains**
info@webspace-verkauf.de is associated with about **7,562 domains**

Registrar History: **2 registrars**
NS History: **1 change** on **2** unique name servers over **5** years.
IP History: **4 changes** on **3** unique name servers over **5** years.
Whois History: **67 records** have been archived **since 2007-10-23** .
Reverse IP: **568 other sites** hosted on this server.


```
DOMAIN: INTERSDA.COM

RSP: heXoNet Support GmbH
URL: http://www.hexonet.net/

created-date: 2006-02-14 14:38:33
updated-date: 2010-03-15 10:01:21
registration-expiration-date: 2012-02-14 14:38:33

owner-organization: InterSDA GmbH
owner-name: Patrick Achache
owner-street: Wihelstrasse 9
owner-city: Walchwil
owner-state:
owner-zip: 6318
owner-country: CH
owner-phone: +41.417581082
owner-fax:
owner-email: achache@intersda.com

admin-organization: InterSDA GmbH
admin-name: Patrick Achache
admin-street: Wihelstrasse 9
admin-city: Walchwil
admin-state:
admin-zip: 6318
admin-country: CH
admin-phone: +41.417581082
admin-fax:
admin-email: achache@intersda.com

tech-organization: Webspace-Verkauf.de
tech-name: Markus Thumerer
```

```
tech-street: Lichtenfelser Strasse 17 a
tech-city: Grub am Forst
tech-state: Bayern
tech-zip: 96271
tech-country: DE
tech-phone: +49.9560981690
tech-fax: +49.95609816929
tech-email: info@webspace-verkauf.de

billing-organization: Webspace-Verkauf.de
billing-name: Markus Thumerer
billing-street: Lichtenfelser Strasse 17 a
billing-city: Grub am Forst
billing-state: Bayern
billing-zip: 96271
billing-country: DE
billing-phone: +49.9560981690
billing-fax: +49.95609816929
billing-email: info@webspace-verkauf.de

nameserver: ns1.webspace-verkauf.de
nameserver: ns2.webspace-verkauf.de
nameserver: ns3.webspace-verkauf.de
```

HOOVERS™
A D&B COMPANY

IP Equity GmbH Profile

Wihelstrasse 9
6318 Walchwil 6318 Zg Switzerland
Phone : +41-417581082

WELCOME

Hoover's is the business information resource that delivers a unique combination of up-to-date data, broad coverage, and comprehensive information about companies, decision makers, and industries - along with powerful tools to put this information to work for your business. Hoover's offers everything you need to successfully:

* Identify and evaluate potential sales leads, markets, and business partners
* Deepen relationships with current customers
* Assess competitive risks and eliminate threats
* Build presentation-ready reports and customized lists of companies, industries, and decision makers

Unlike other business information providers, only Hoover's has a full-time, in-house editorial and research team dedicated wholly to investigating, pinpointing, authenticating, and analyzing data to provide the most comprehensive, up-to-date information available on companies, industries, and executives.

Table of Contents

Company Overview

Wihelstrasse 9
6318 Walchwil 6318 Zg Switzerland
Phone : +41-417581082

Miscellaneous business credit institution

Key Information

DUNS Number	485494194
Location Type	Single Location
Subsidiary Status	No
Manufacturer	No
Total Employees	1
1-Year Employee Growth	0.00%
Year of Founding or Change in Control	2010
Primary Industry	1317:Agricultural Lending
Primary SIC Code	61590100:Agricultural credit institutions
Primary NAICS Code	522293:International Trade Financing

Key Financials

Fiscal Year-End	December
Sales ($ M)	$0.27M

Key People

Name	Title
Stephan Bolliger	Managing Director
Patrick Achache	

People

Employees

Title	Name	Age	Salary	Bonus
Managing Director	Stephan Bolliger		--	--
	Patrick Achache		--	--

Biographies

Stephan Bolliger

Current Company Titles

Unknown - Present : Managing Director

Patrick Achache

Current Company Titles

Unknown - Present :

databot economic data - Patrick Achache

IP Equity GmbH, Walchwil
CH-170.4.009.565-1

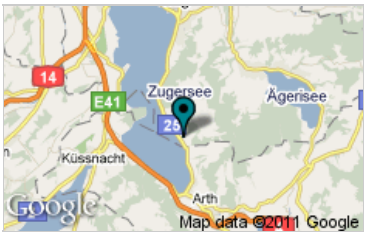
Facts

Status	Active
Establishing	4. March 2010
Seat	Walchwil
Legal form	Limited Liability Company
Capital	CHF 20'000

SOGC News	2
Last Change	1. March 2011
Procuration	4 people

Address

IP Equity GmbH
Wihelstrasse 9
CH - 6318 Walchwil



Overview | Authorised 2 | Persons 2 | Publications 4

IP Equity GmbH
Limited liability company in Walchwil

Purpose

Financing projects in the areas of software and entertainment, and provision of insurance services; whole purpose description According to the statutes

Translation of Company Name

BP Equity Ltd liab. Co
BP Equity Sagl
BP Equity Sàrl
IP equity Ltd liab. Co
IP equity Sagl
IP equity Sàrl

Former company name

BP Equity GmbH in March 2011

Management

Patrick Achache from Germany in Karlsruhe, DE
Stephan Bolliger , Zurich Dietikon
Patrick Achache from Germany in Karlsruhe, DE

Latest Releases

01. March 2011	**Reason for Deletion** Company: IP Equity Inc.
10. March 2010	**Note** According to statement by the company on 18/01/2010 under the Company no regular audit and dispense with a limited audit

Last SOGC News

01. March 2011	**SHAB No 42 of 1.3.2011 p. 35 Publ 6.055 million** BP Equity GmbH, in Walchwil, CH-170.4.009.565-1 , a limited liability company (SHAB No. 48 of 10.03.2010, p. 21, Publ 5,533,518) **new. Statutes Amendment 1.28.2011.: Company** IP Equity GmbH . translations of the new company: (IP Equity Sarl) (IP Equity Sagl) (IP Equity Co Ltd liab.).

New Releases: Releases made to the shareholders by mail, e-mail or fax. [Further modification not requiring publication facts]. [With amendments to the articles of 01.28.2011 was secondary aim of the company changed **the.]. Registered persons new or mutating**
Bolliger, Stephan , of Zurich, Dietikon, managing director with single signature; Achache, Patrick , a German national, in Karlsruhe (DE), Chairman of ...

10. March 2010

SHAB No 48, 03.10.2010 p. 21 Publ 5,533,518
BP Equity GmbH (BP Equity Sarl) (BP Equity Sagl) (BP Equity Ltd liab co.), In Walchwil, CH-170.4.009.565-1 , Wihelstrasse 9, 6318 Walchwil, limited liability company (new
registration). statutes Date
02:03 . .2010
Purpose: To
fund projects in software and entertainment, and provision of insurance services; whole purpose of description according to
statutes. Share capital
20,000 .00. CHF
Publication organ:
SHAB. Notices to the shareholders in writing or by e-mail. According to statement by the company on 18/01/2010 under the Company no regular audit and dispense with a limited
audit. Registered persons
Achache, Patrick , a German national, in train, managing director with single signature ...

databot economic data - Patrick Achache

Patrick Achache
Of Germany in Karlsruhe, DE

Facts

Home	Germany
Location	Karlsruhe, DE
GL mandates	3 seats
Investments	CHF 20'000 .00 (1 company)

Feedback / Error Report

Location

Overview | Investments 1 | 2 companies | Publications 3 | Composition 3

Investments

Company	CH Number	Number	Currency	Amount	From	Up
IP Equity GmbH in Walchwil	CH-170.4.009.565-1	200	CHF	100.00	10. March 2010	1. March 2011
Intersda GmbH in Walchwil	CH-170.4.009.208-8	200	CHF	100.00	9. October 2009	-

databot economic data - Patrick Achache

Patrick Achache
Of Germany in Karlsruhe, DE

Facts

Home	Germany
Location	Karlsruhe, DE
GL mandates	3 seats
Investments	CHF 20'000 .00 (1 company)

Feedback / Error Report

Location

Overview | Investments 1 | 2 companies | Publications 3 | Composition 3

Mandates

Managing Director
Shareholders
CEO
Only current mandates

Original German text: Google
Firmen 2
Contribute a better translation

Company	Function	Authorised	From	Up
IP Equity GmbH in Walchwil	CEO	Single signature	1. March 2011	-
IP Equity GmbH in Walchwil	Shareholders	Single signature	10. March 2010	-
IP Equity GmbH in Walchwil	Managing Director	Single signature	10. March 2010	-
Intersda GmbH in Walchwil	Shareholders	Single signature	9. October 2009	-
Intersda GmbH in Walchwil	Managing Director	Single signature	9. October 2009	-

EXHIBIT P

Scott Hervey, State Bar No. 180188
Scott M. Plamondon, State Bar No. 212294
weintraub genshlea chediak
a law corporation
400 Capitol Mall, 11th Floor
Sacramento, CA 95814
(916) 558-6000 – Main
(916) 446-1611 – Facsimile

Attorneys for Plaintiff
Camelot Distribution Group, Inc.

IN THE UNITED STATES DISTRICT COURT

IN AND FOR THE CENTRAL DISTRICT OF CALIFORNIA

WESTERN DIVISION

CAMELOT DISTRIBUTION GROUP, INC., Plaintiff, vs. DOES 1 through 5,865, inclusive, Defendants.	Case No.: CV11-01949 DDP (FMOx) DECLARATION OF TOBIAS FIESER IN SUPPORT OF RESPONSE TO ORDER TO SHOW CAUSE

I, Tobias Fieser,, declare as follows:

1. I am the Technical Administrator of IPP International UG and have personal knowledge of the facts set forth in this declaration except as to matters stated upon information and belief, and as to those matters I believe them to be true and if called upon to do so, I could and would competently so testify under oath.

2. Each of the Doe Defendants have effectuated the illegal transfer of Plaintiff's Movie through the use of the "BitTorrent protocol" (or "torrent") in connection with a peer-to-peer ("P2P") network. This architecture is significantly different in form from the older P2P

protocols which were employed on networks such as Napster, Kazaa, Limewire, and Gnutella.

3. The BitTorrent protocol allow computers to exchange large amounts of data across a network while consuming minimal bandwidth on the network. With the BitTorrent protocol an initial file-provider elects to share a "seed" file via a BitTorrent network. Thereafter, other users ("peers") connect to the seed file and begin downloading data from the seed, while simultaneously sharing the downloaded data with other peers.

4. As additional peers request the same file, each additional user becomes a part of the network (or "swarm") and begins sharing its data with other peers, which means that each additional user's computer is connected not only to the seeder/uploader but also is connected to myriad other peer/downloaders.

5. The BitTorrent protocol used to download Plaintiff's Movie would have each new file downloader receive a different piece of the data from each user who has already downloaded that piece of data, all of which pieces together comprise the whole. This means that every peer user who has a copy of the infringing copyrighted material on such a network—or even a portion of a copy—can also be a source of download for that infringing file, potentially both copying and distributing the infringing work simultaneously.

6. The distributed nature of the BitTorrent protocol leads to a rapid spreading of a file through a huge number of peer users all of whom are both uploading and downloading portions of the file simultaneously. The propagation of copying files employing the BitTorrent protocol is similar to that of a computer virus. As more peers join the swarm, more parts of the original file become readily available, and the likelihood of a successful download increases.

7. Because of the nature of the swarm downloads as described above, every infringer is simultaneously stealing copyrighted material through collaboration with multiple other infringers, through a number of ISPs, in numerous jurisdictions around the country. One difference between this BitTorrent protocol and the older P2P network protocols Employed by networks such as Napster, Grokster, Limewire, and Gnutella is how those networks locate and trade bits of the files.

8. Napster, Kazaa, Limewire, Gnutella, and similar first generation P2P networks

are simple file sharing networks. Through use of a common interface, infringers are interconnected to a variety of people each of whom are sharing a variety of files. Users search the P2P network to locate other users who have files that are being sought by. Thereafter an individual chooses a specific user from whom to download a file, and begins the process of copying the entire file from the particular user who has offered the file for copying.

9. BitTorrent is fundamentally different. Instead of being user-focused, BitTorrent is file-focused. The person seeking to share a file creates a "tracker" and makes the tracker available. Rather than finding that tracker by sending out search requests along a file sharing network, infringers find it in various location on the internet, including without limitation, websites, via recommendations in chat rooms, and in links posted to mailing lists. Once a tracker has been made available anyone interested in sharing that specific file can use the tracker to essentially create a network dedicated to sharing just that specific file.

10. The most important characteristic of BitTorrent is the concept of the swarm, which is a group of peers who are using the BitTorrent protocol to transfer a single file amongst themselves. Peers engaged in downloading a file as part of a torrent cooperate to replicate the file among each other using swarming techniques. A user joins an existing torrent by downloading a ".torrent" file, adding it to its client and connecting to the specified tracker. The ".torrent" file contains data regarding the file to be downloaded (e.g., the number of pieces, encryption and error checking data called "SHA-1 hash values") and the IP address of the "tracker" of the torrent. The tracker is the only centralized component of the BitTorrent protocol, however it is not involved in the actual distribution of the file. Rather, the tracker only keeps track of the peers who are currently members of the swarm and directs a downloader's computer to the other peers to facilitate the downloading of the pieces of the file.

11. When joining a swarm, a new peer receives from the tracker a list of IP addresses of peers who are available to connect to and cooperate with. For a typical file, such as Plaintiff's Movie, 50 or more peers are chosen at random in the list of peers currently involved in the torrent. This group of peers forms the peer set of the new user joining the swarm. The group of peers will then distribute the file among each other. Each peer knows

what pieces each other peer has, and each peer helps the other to successfully download the entire file.

12. There are a very few original copies of Plaintiff's Movie being tracked through the use of BitTorrent trackers. Because of the nature of the BitTorrent protocol, it is a near certainty that each of the infringers who have copied and distributed Plaintiff's movie have been involved with the copying and distribution of the exact same infringing file from the time of its initial seeding up to and including the present day. The coordinated actions of the Doe Defendants have caused a single copy of the Movie to be distributed to thousands of individuals without Plaintiff's consent, and without compensation to Plaintiff.

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

Executed this 12 day of May, 2011, at Karlsruhe.

Dated: May 12, 2011

By: Fieser
Tobias Fieser

EXHIBIT Q

EXHIBIT A

TO: DECLARATION OF TOBIAS FIESER IN SUPPORT OF PLAINTIFF'S MOTION FOR LEAVE TO TAKE DISCOVERY PRIOR TO A RULE 26(f) CONFERENCE

IPP international LTD.

FUNCTIONAL DESCRIPTION

IPP international IPTRACKER v1.2.1

Table of contents

1 Introduction

The following disquisition introduces the software IPP international IPTRACKER. The software was developed to determine copyright violations in peer-to-peer networks (called P2P networks) and to preserve evidences during illegal distribution of copyright protected material.

P2P allows spreading data of every kind (software, music, video etc.) via the Internet fast. The data is saved on the computers of the participants and is distributed by common P2P software products which are available on the internet for free. The Data is usually copied from foreign computers (called download) while other data is sent at the same time (called upload). Every participant can release files on his computer and make it available to others, comparable to the file release function within a local network. The files are copied via direct connection between the computers. P2P networks have millions of users and offer an enormous variety of files.

The procedure itself is legal for data which is not under copyright.

A common description of the operation of most commonly used P2P peer-to-peer techniques used to exchange data on the Internet can be found in the addendum.

2 The program IPP international IPTRACKER v1.2.1

2.1 Description of Action

2.1.1 Filesearch

Once a file is downloaded, verified and definitely allocated to a Rights holder, the hash value is used to determine possible sources on the internet. Different servers, trackers and clients provide lists of IPs where the specific file could or still can be downloaded.

2.1.2 Summarization of the procedure

These lists are downloaded from the providing system and computed sequentially. Each IP found in these lists is requested using the common P2P protocol functions. If the requested P2P client confirms the existence of the file on the local hard disc (in the shared folders), the download is started.
If the part downloaded is sufficient to be verified and compared to the original, the IP address and exact time and date is stored in a secure database.
The download process is continued.

After completion of the download process and before the stored information is used for further steps the downloaded data is compared with the original (complete already downloaded and verified file) bit by bit.

2.1.3 Safety of IP and other connection data

A direct and continuous connection between the IPTRACKER-server and the uploader of the file is established and exists at least 10 seconds before, during and at least 10 seconds after the capture sequence i.e. during the whole download process.

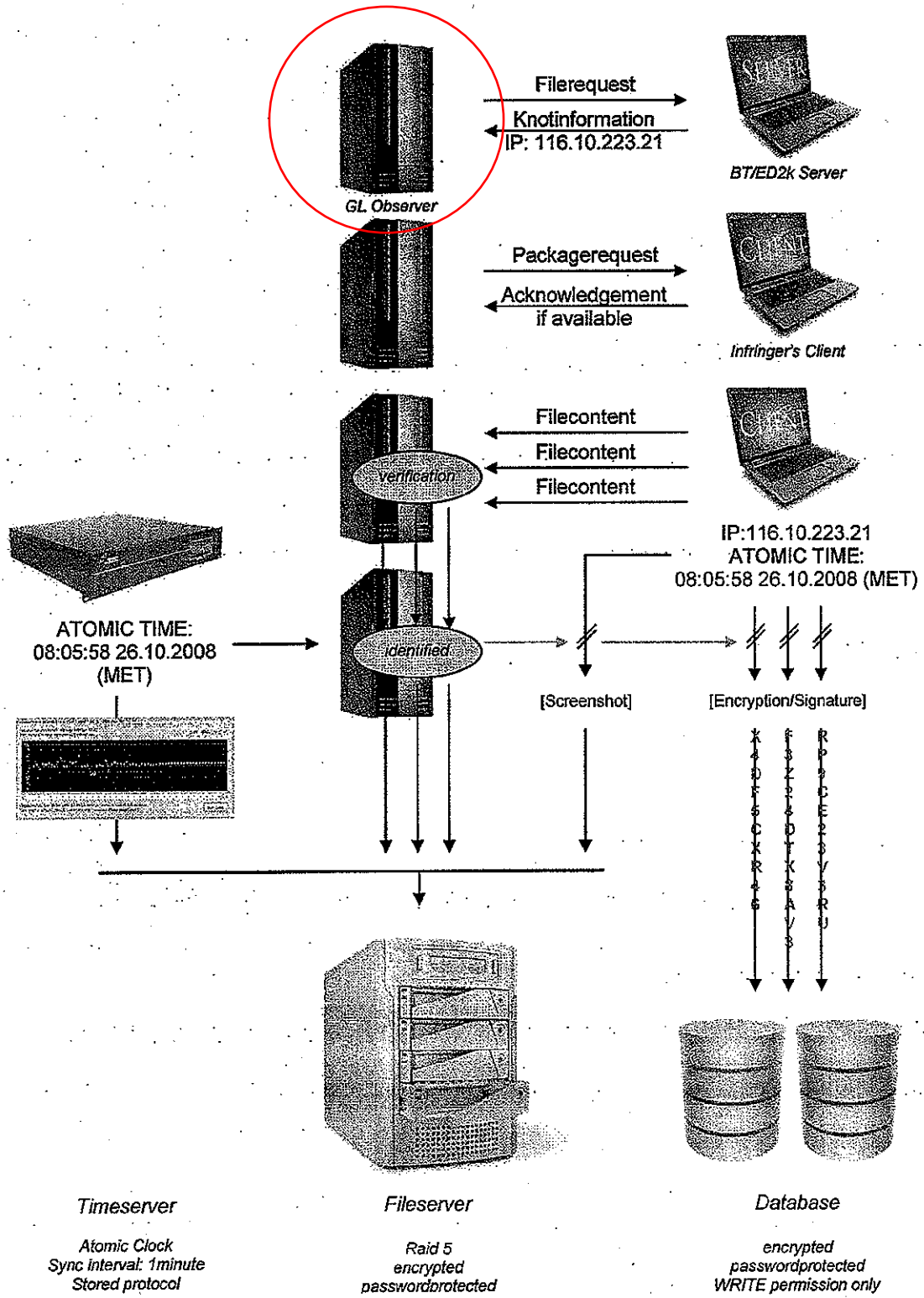
Optionally the screen can be capture automatically to backup another evidence.

2.1.4 The date and time

The (IPTRACKER-) server date and time is synchronised every minute via Network time protocol (NTP). This function is provided by an additional program (Dimension 4 v5.0 http://www.thinkman.com/dimension4).
The synchronization report is saved frequently and redundantly stored on a file server. The time is received from the Federal technological Institute in Brunswick (Physikalisch-Technische Bundesanstalt in Braunschweig) and has a maximum deviation of for 1/10 second (atomic clock).

Several other redundant institutes providing the exact time are stored in an internal database of the program: Dimension 4.

2.2 Visualisation of the process



2.3 Description of the most important program functions

The IPP international IPTRACKER is based on the hybrid Filesharing client Shareaza 2.4.0.0. All communication interfaces correspond to the specifications of the P2P protocols Bittorrent, Gnutella 1 and 2 as well as ED2k. These interfaces were left invariably in the filesharing client.

The function of the upload in addition was reduced to a minimum (handshaking).
The IPP international IPTRACKER merely stores the data of the hosts connected with, if the package verification succeeds.

- IP address
- port
- exact capture time
- name of the protocol
- filename
- file size
- hash values of the file (SHA1, ED2k, BITH)
- GUID
- username
- clientname
- content downloaded

A screenshot of the host can be made by the IPTRACKER program. The host is marked automatically during the download phase to safeguard another evidence. Not relevant entries are masked. The name of the screenshot is also stored in the database.

To guarantee the immutability of the data, IP, date and time is signed with a private 4096 bit RSA key. The RSA key is included internally in the IPTRACKER program using a precompiled library and can be not read or used elsewhere.

RSA is a recognized asymmetrical encoding procedure which can be used both for the encoding and for the digital signature. It uses a key pair consisting of a private key which is used decode or sign data and a public key with which decoding or signature checks are made possible. Both keys are kept secret.

3 Logdata database

The data is stored in a MySQL database. The database server runs locally as a service on the respective server. The connection is established via ODBC driver: MyODBC-3.51.11. The query language is SQL. The IPTRACKER program accesses the database exclusively writing. The entries right-related cannot be changed.

The data is exclusively submitted as data sheets for the assertion of the injured rights.

3.1 Protection of data privacy and data security

The rack-servers are stored in a room which is locked and protected with most current security mechanisms.

The database is password protected and stored on an encoded hard disk. The hard disk is encoded with TrueCrypt 6.0 using AES encyption. The password is not saved on any computer, only known by two people and has more than 25 signs. It must be entered manually at every system startup. When the hard disk is removed from the computer or the power supply, it has to be mounted again using the password.

If the hard disk should be reached by unauthorized people, the data security is therefore ensured at any time.

To maximize data security, the IPTRACKER program offers an implemented program function which permits not only to sign but also to encode completely relevant data. So the data cannot be seen or changed even by persons with direct access to the server.

To create valid entries the secret key pair is necessary. It is not possibly to store data manually at any time.

Only the IPTRACKER program is able to create valid data.

The data can only be decoded and used by the responsible lawyer, only his software contains the deciphering method and this one in this case also secret (called "public") key.

4 Addendum

Basic Knowledge

P2P networks can be subdivided into several groups using their structure and operation.

Centralized P2P systems
These systems are using a central server to which all knots are connected. All search enquiries from the knots are processed by the server. The basis of P2P systems is the data transmission between the individual knots. A direct connection between the knots is established when the file is found on a specific knot.

The server is the bottle of the neck in this process.

Nowadays centralized P2P systems are of more minor importance.

Pure P2P systems without a central instance
There are networks without a central server which do not manage any central data stock (Gnutella1 and Gnutella2 network).

P2P-Filesharing networks via server client protocol
There are networks with one or several central servers which manage information about the users connected at present. This is provided by the Bittorrent and eDonkey network. With the installation of Emule the users receive a list of all users (file: server.met) attached to a server and all released files. Bittorrent and eDonkey cover currently 95% of the exchange activity.

Gnutella

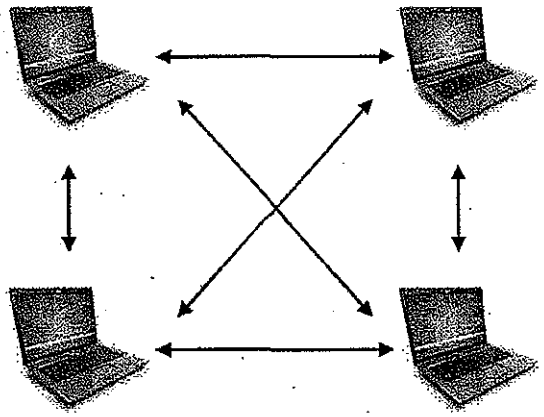
Gnutella is a P2P network decentralized completely which can be observed by the IPP international IPTRACKER software. "Decentralized" means that every knot uses a similar software and there are no central servers which process search enquiries.

A search query is passed to the neighbouring systems at first. These systems refer the query to their neighbours until the requested file was found. After that a direct connection for the data transmission can be established between searching and offering knot

Gnutella 2

Gnutella 2 works most largely like the original Gnutella network with a similar connection system but Unicode2 search function with extensive metadata, TigerTree Hashing, and generally faster link speed. A "Partial file Sharing" function was implemented which divides files into parts. It's possible to download these parts from different knots instead of downloading the whole file from one knot.

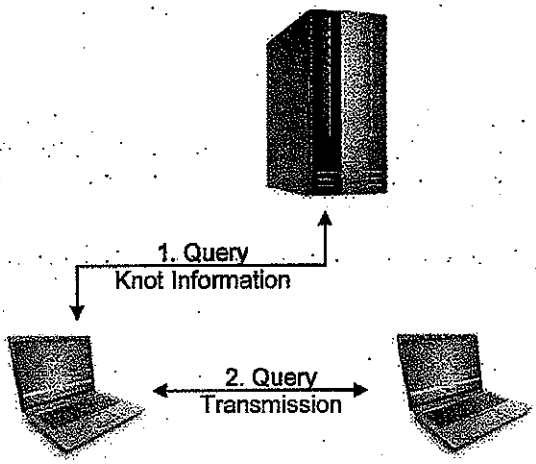
Some known Gnutella2 clients are:
Shareaza, Morpheus, Gnucleus, adagio, MLDonkey



eDonkey2000 (Ed2k)

The eDonkey2000 peer to peer network needs server to connect the knots. The server only provides lists of files which are available on the individual knots.

Some Edonkey2000 clients are: eMule, eMulePlus, aMule, xMule, MLDonkey, Lphant



Bittorrent (BT)

BitTorrent is used for the fast distribution of large amounts of data in which central servers are controlling the location of the files.

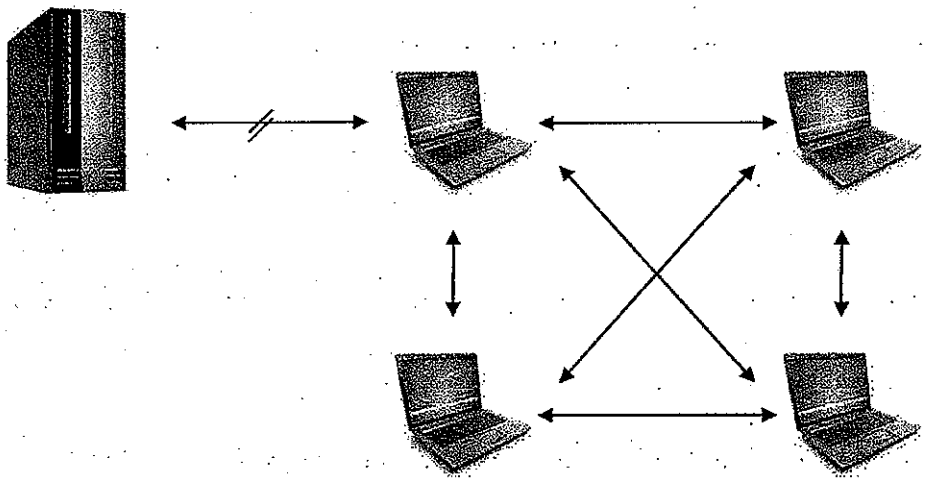
BitTorrent does not behave like a usual P2P network. There is no search function like it is available it at EDonkey or Gnutella clients.

To get all necessary information for a download, a .torrent file is downloaded (from another network or an internet page). It contains all information to start the download.

The Bittorrent participants connect with the so-called tracker of this file and with that with other users who also are interested in at this file. A private network is built.

Trackerless systems were developed in new versions. The tracker function is done by the client software. This avoids some of the previous problems (e.g. the missing failure safety of the trackers).

Some Bittorrent clients are: Shareaza, BitComet, Azureus



Globally Unique Identifier (GUID)

Every P2P user receives a unique identification which consists of a 32-digit hexadecimal number. The user receives the identification at the moment of the installation of the P2P program. The program generates the GUID from user-specific data. So it is possible that a user has several GUID identifications (e.g. he gets a new GUID at the installation of a network client), however, it is not possible that an allocated GUID is allocated to another user again.

The hash value

The hash value is necessary to identify a file.

A special advantage of Bittorrent, eDonkey and Gnutella networks is the fault-free data transmission between the users. Bigger files are subdivided into little packages. For every package a single identification value is generated using known algorithms. The hash value is frequently described as a fingerprint since it is unique similarly like a fingerprint.

i.e. each file exceeding the size of 2 megabytes owes more than one hash value - one for the whole file and one for each package.

Standard operation of common P2P-client programs during the filesharing process:

The client software must guarantee that the received content is always the queried one. Therefore only hash values are requested – filenames are unimportant during the transmission.

After a client received a data package the content has to be verified. Therefore the hash value of the package is generated by the client and compared to the hash value provided before. If the two keys are identical, the downloaded package is accepted. If there are deviations at the comparison, then the package is declined and requested again. The package can also be downloaded from another knot.

All mentioned programs are able to split bigger files into packages and to identify these using hash values independently which program is used for the data exchange. With this it is possible to assign small parts of a file to the original file. It is made sure that the part of the file always belongs to the requested file.

After the whole file is downloaded it will be verified on the whole before the download process is finished and the file is signed as "VERIFIED".

Every network uses different hash algorithms. Bittorrent the so-called "BiTH", eDonkey this one "ED2K", and Gnutella the "SHA1" algorithm.

The IPP international IPTRACKER is able to generate and compare each hash algorithm listed above.

EXHIBIT R

Court File No. T-2058-12

FEDERAL COURT

BETWEEN:

VOLTAGE PICTURES LLC

Plaintiff

and

JOHN DOE and JANE DOE

Defendants

SUPPLEMENTARY AFFIDAVIT OF BARRY LOGAN

(Sworn on May 27, 2013)

I, **BARRY LOGAN**, of the City of Stratford, in the province of Ontario, **MAKE OATH AND SAY AS FOLLOWS:**

1. On December 7, 2012, I swore an affidavit describing my involvement in the Internet Protocol investigation conducted for the Plaintiff in the herein matter.

2. In paragraph 8 of my original affidavit I stated the following:

> Between September 1 and October 31, 2012, forensic software called GuardaLey Observer v1.2 (the "Forensic Software") was used to scan BitTorrent networks for the presence of Voltage's copyrighted works.

3. The software used in my investigation was GuardaLey Observer v.1.47, not v.1.2. This was simply a typographical error in my original affidavit that I had neglected to correct.

SWORN BEFORE ME at the City of)
Toronto, in the Province of Ontario,)
this 27th day of May, 2013)
)
)
)

A Commissioner of Oaths, etc.

BARRY LOGAN

Court File No. T-2058-12

VOLTAGE PICTURES LLC
Plaintiff

and

JOHN DOE and JANE DOE
Defendants

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at Toronto

AFFIDAVIT OF BARRY LOGAN

(Sworn on May 27, 2013)

BRAUTI THORNING ZIBARRAS LLP
151 Yonge Street, Suite 1800
Toronto, ON M5C 2W7

P. James Zibarras
LSUC No. 48856F

John Philpott
LSUC No. 60246U

Tel: 416.362.4567
Fax: 416.362.8410

Lawyers for the Plaintiff,
VOLTAGE PICTURES LLC

8

Court File No. CV-

FEDERAL COURT

BETWEEN:

VOLTAGE PICTURES LLC

Plaintiff

and

JOHN DOE and JANE DOE

Defendants

AFFIDAVIT OF BARRY LOGAN

(Sworn on December 7, 2012)

I, **BARRY LOGAN**, of the City of Stratford, in the province of Ontario, **MAKE OATH AND SAY AS FOLLOWS:**

1. I am the owner and principal forensic consultant of Canipre Inc. ("Canipre"), an Ontario based corporation that provides forensic investigation services to copyright owners. As part of my duties at Canipre, I routinely identify the Internet Protocol ("IP") addresses used by individuals who download and distribute copyrighted works over peer to peer ("P2P") networks using the BitTorrent Protocol.

2. The Plaintiff, Voltage Pictures LLC ("Voltage"), is a movie production company based in Los Angeles, California. Voltage retained Canipre to investigate whether its films were being copied and distributed by Canadian members of P2P online networks and to support the associated litigation. I was directly involved in the investigation and as such

have knowledge of the matters to which I hereinafter depose. Where I do not have personal knowledge, I have stated the source of my information and believe it to be true.

Background – The BitTorrent Protocol

3. The BitTorrent Protocol is a P2P file sharing protocol that facilitates the distribution of large amounts of data over the internet through networks.

4. When a file is initially uploaded to a BitTorrent network, that is referred to as "seeding". Other P2P networks users, called "peers", can then connect to the user seeding the file in order to copy it.

5. The BitTorrent Protocol breaks a file into numerous small data packets, each of which is identifiable by a unique hash number created using a hash algorithm. Once a file has been broken into numerous packets, other network users or peers are able to download different sections of the same file from multiple users. Each new peer is directed to the most readily available packet of the file they wish to download. In other words, a peer does not copy a file from one user, but from any peer who previously downloaded the file and has it available on the BitTorrent network. The peer then becomes a seeder as it distributes the data packet to other peers connected to the BitTorrent network.

6. Once a packet is downloaded by a peer, that peer automatically becomes a download source for other peers connected to the BitTorrent network who are requesting the file. This speeds up the time it takes to download a file and frees up the capacity of a computer or server to simultaneously download and upload files. Unless the settings on the user's BitTorrent program are changed, every user who is copying or who has copied a file is

simultaneously distributing it to every other user or peer connected to the BitTorrent network. This allows even small computers with low bandwidth to participate in large data transfers across a P2P network.

Canipre's Forensic Investigation

7. Voltage retained Canipre to identify the Internet Protocol ("IP") addresses used on the BitTorrent network to copy and distribute copyrighted works which Voltage has the rights to in Canada. A list of such works which Canipre monitored as part of this investigation is attached as **Exhibit "A"**.

8. Between September 1 and October 31, 2012, forensic software called GuardaLey Observer v1.2 (the "Forensic Software") was used to scan BitTorrent networks for the presence of Voltage's copyrighted works.

9. I was tasked with monitoring, analyzing, reviewing and attesting to the results of the investigation.

10. The Forensic Software was run between September 1 and October 31, 2012. The Forensic Software searched BitTorrent networks for files corresponding to Voltage's copyrighted works and identified the IP address of each seeder or peer who was offering any of these files for transfer or distribution. This information is available to anyone that is connected to the P2P network.

11. The Forensic Software then downloaded the copies of Voltage's copyrighted works available for distribution on the P2P networks, and for each file downloaded recorded the following identifying information:

a. the IP address assigned to the peer by his or her internet service provider ("ISP") at the time it distributed the file;

b. the date and time at which the file was distributed by the seeder or peer;

c. the P2P network utilized by the peer; and

d. the file's metadata, which includes the name of the file and the size of the file (collectively, the "File Data").

12. The File Data is stored in a secure central database. I have personally reviewed the File Data. After reviewing the File Data, I identified the transactions associated with IP addresses geographically limited to Ontario and to customers of TekSavvy Solutions Inc. ("TekSavvy") that used the BitTorrent network to reproduce and distribute Voltage's copyrighted works during the period of September 1 to October 31, 2012. A copy of the File Data for these transactions is attached as **Exhibit "B"**.

Identifying the IP Addresses

13. An internet service provider or ISP, such as TekSavvy, is an organization which provides access to the Internet to its customers. Peers, seeds, and users access the BitTorrent network through the internet access provided by their ISP.

14. An IP address is a unique numerical identifier that is automatically assigned to an internet user by that user's ISP.

15. ISPs are assigned blocks or ranges of IP addresses. The range assigned to any ISP can be found in publicly available databases on the internet.

16. ISPs track the IP addresses assigned to their customers at any given time and retain "user logs" of that information.

17. Through the Forensic Software, I am able to track a peer by its IP address to a particular ISP and to their geographic location. This is how I was able to limit the IP addresses and related File Data in Exhibit B to customers of TekSavvy in the province of Ontario.

18. Once provided with the IP address and the corresponding File Data, ISPs can review their user logs to identify the name, address, email address, and phone number of their clients who acted as peers to copy and distribute unauthorized versions of Voltage's works.

19. Only an ISP can correlate the IP address to the real identity of its subscriber. Without the involvement of the ISPs, Voltage will be unable to determine the identities of those persons who are distributing their copyrighted works.

Confirmation of Data

20. I personally reviewed the File Data gathered from this investigation.

21. After reviewing the File Data, I verified that the transactions contained in Exhibit B are associated with IP addresses geographically limited to Ontario and to customers of TekSavvy. I have also verified that the IP addresses and related File Data contained in Exhibit B hereto correctly reflect what is contained in the secure central databases.

13

22. In addition, I have analyzed each of the BitTorrent packets distributed by the IP addresses listed in Exhibit B and verified that reassembling the pieces results in a fully playable digital motion picture that is one of Voltage's copyrighted works.

23. I was provided with a control copy of each of Voltage's copyrighted works, which I have viewed side by side with the digital media files set forth in Exhibit B and confirmed that they were the same.

SWORN BEFORE ME at the City of Toronto, in the Province of Ontario, this 7 day of December, 2012

A Commissioner of Oaths, etc.

Nanci Elizabeth McFadden-Fair,
a Commissioner, etc., Province of Ontario,
for Michael F. Fair, Barrister and Solicitor.
Expires November 26, 2015.

BARRY LOGAN

Court File No.

VOLTAGE PICTURES LLC
Plaintiff

and

JOHN DOE and JANE DOE
Defendants

ONTARIO
SUPERIOR COURT OF JUSTICE

Proceeding commenced at Toronto

AFFIDAVIT OF BARRY LOGAN

(Sworn on December 2012)

BRAUTI THORNING ZIBARRAS LLP
151 Yonge Street, Suite 1800
Toronto, ON M5C 2W7

P. James Zibarras
LSUC No. 48856F

John Philpott
LSUC No. 60246U

Tel: 416.362.4567
Fax: 416.362.8410

Lawyers for the Plaintiff,
VOLTAGE PICTURES LLC

This is **Exhibit "A"** referred to in the affidavit of **BARRY LOGAN** sworn before me this 7 day of December, 2012.

A COMMISSIONER FOR TAKING AFFIDAVITS

Nanci Elizabeth McFadden-Fair,
a Commissioner, etc., Province of Ontario,
for Michael F. Fair, Barrister and Solicitor.
Expires November 26, 2015.

Voltage's Cinematographic Works as Monitored by Canipre

09.01.12 – 10.31.12

Generation Um ... (2012)

Tucker & Dale vs Evil (2010)

True Justice (The Complete First Season) (2010)

The Third Act aka The Magic of Belle Isle (2012)

The Good Doctor (2011)

Rosewood Lane (2011)

Another Happy Day aka The Reasonable Bunch (2011)

Killer Joe (2011)

Escapee (2011)

This is **Exhibit "B"** referred to in the affidavit of **BARRY LOGAN** sworn before me this day of December, 2012.

A COMMISSIONER FOR TAKING AFFIDAVITS

Nanci Elizabeth McFadden-Fair,
a Commissioner, etc., Province of Ontario,
for Michael F. Fair, Barrister and Solicitor.
Expires November 26, 2015.

EXHIBIT S

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

MALIBU MEDIA, LLC,	*	
Plaintiff,	*	**CASE NO. 8:13-cv-00360-RWT**
v.	*	
JOHN DOE subscriber assigned IP address 68.50.250.243,	*	
Defendant.	*	

PLAINTIFF'S WRITTEN RESPONSE TO THE COURT'S MEMORANDUM/ORDER [CM/ECF 9]

I. INTRODUCTION

Malibu Media, LLC ("Malibu Media") appreciates the opportunity to discuss the issues raised in this Court's order dated March 1, 2013. For the reasons set forth in Plaintiff's Memorandum Explaining Why It Has a Clear and Undeniable Right to Issue a Rule 45 Subpoena, Plaintiff has a clear, absolute, and undeniable right to subpoena the identities of the Doe Defendants in the subject cases.[1] Indeed, since this case was filed, Plaintiff has received orders allowing it to subpoena Internet Service Providers ("ISP"s) in 80 individual John Doe suits throughout the country. *See* Exhibit A. No court has *ever* denied Plaintiff's motion to subpoena the identity of a John Doe Defendant who was sued individually in a BitTorrent copyright infringement lawsuit. Here, it is Plaintiff's sincere hope that once leave is granted to issue the subpoenas, that this process will reduce the number of frivolous motions attempting to quash the subpoenas. Plaintiff also appreciates that the scheduled hearing, wherein defense counsel and ISPs have been invited to discuss their concerns and to collaborate on an efficient

[1] If the Court denies Plaintiff the right to subpoena the ISP in order to obtain the Doe Defendant's identity, Plaintiff respectfully requests the Court certify the issue to the Fourth Circuit.

process for managing these cases, has the potential of reducing the amount of work for all concerned. And, Plaintiff looks forward to working cooperatively the Court, the ISPs and the defense counsel to establish efficient case management procedures.

II. RESPONSE TO THE COURT'S QUESTIONS

A. Malibu Media's affiliation with Patrick Collins, Inc., Third Degree Films, Inc., K-Beech, Inc., Hard Drive Productions, Inc., Raw Films, Ltd., and/or AF Holdings, LLC

Malibu Media, Patrick Collins, Inc., Third Degree Films, Inc., K-Beech, Inc. and Raw Films, Ltd. *have* used the same attorneys, investigator and litigation support personnel. These movie studios are not related in any other way. Going forward, undersigned only intends to file suits on behalf of Plaintiff. Accordingly, Plaintiff will soon have *no* connection with the other studios.

Plaintiff has no connection with Hard Drive Productions, Inc., AF Holdings, LLC, the Copyright Enforcement Group or any other group that has or is filing BitTorrent copyright infringement suits in the United States.

Plaintiff is keenly aware that other enforcement groups have tarnished the reputation of copyright owners who sue for BitTorrent copyright infringement. Indeed, AF Holdings, LLC is currently under investigation for fraudulently using its founder, John Steele's, gardener's name as AF Holdings, LLC's manger, with the gardener's knowledge. Evan Stone was sanctioned by a District Court in Texas for sending a subpoena to an ISP after the court denied his client the right to do so except as to Doe 1 in a joined suit. And, that sanction was upheld on appeal. Almost all of the other groups who have litigated BitTorrent copyright infringement cases began their enforcement efforts by relying on long-arm jurisdiction to sue 100s or 1000s of infringers in one federal court suit brought in a district where the majority of the Doe Defendants did not reside. Neither Plaintiff nor anyone with whom it has worked has relied on federal long arm

jurisdiction to sue Doe Defendants for copyright infringement in jurisdictions where those Defendants do not reside. Instead, Plaintiff has scrupulously adhered to the most stringent interpretations of the law as articulated by the majority of the District Courts across the country. And, informed Courts across the country have recognized and appreciated that Plaintiff has acted within the law and ethically during these cases.

One of the bedrock principals of the entire social structure of the United States and the Judeo-Christian ethics upon which that structure was founded is that we are to evaluate every person by his or her actions, without allowing our opinions of person A to be affected by the actions of person B.[2] That is particularly true when, as here, Person A and Person B have no affiliation with each other. With this in mind, Plaintiff respectfully requests that the Court not allow the alleged bad acts of some other lawyers, copyright owners or copyright enforcement groups to color its opinion of Plaintiff or the propriety of Plaintiff's copyright enforcement efforts.

Regarding the propriety of Plaintiff's enforcement efforts, during her tenure as the U.S. Register of Copyrights, Mary Beth Peters explained the rights of adult entertainment companies to proceed with these suits against the individual infringers by stating: "[t]he law is unambiguous. Using peer-to-peer networks to copy or distribute copyrighted works without permission is infringement and copyright owners have every right to invoke the power of the courts to combat such activity. Every court that has addressed the issue has agreed that this activity is infringement." See Pornography, Technology, and Process: Problems and Solutions on Peer-to-Peer Networks Statement of Marybeth Peters The Register of Copyrights before the Committee on the Judiciary 108th Cong. (2003), available at

[2] "You reward everyone according to what they have done." Psalm 62:12
"I the LORD search the heart and examine the mind, to reward each person according to their conduct, according to what their deeds deserve." Jeremiah 17:10

http://www.copyright.gov/docs/regstat090903.html (emphasis added). Ms. Peters concluded that copyright owners have no reason to apologize for enforcing their rights in this manner. *Id*. Plaintiff has consistently and without exception striven to make sound legal and factual arguments and has no reason whatsoever to apologize for its enforcement activities. To the contrary, Plaintiff is extremely proud of the good and honorable work it is doing enforcing its copyrights and deterring infringement.

B. Other Methods to Determine if a John Doe as a Subscriber is the Infringer

1. A Rule 45 Subpoena is the Only Federal Procedure for Obtaining the John Doe Defendants' Identities

A Rule 45 subpoena is the only legal process available under federal law to ascertain the identities of the John Doe defendants. To explain, "[i]n June 2003, the RIAA (Recording Industry Association of America) announced a nationwide effort to identify and sue individuals committing copyright using P2P systems." In re Charter Communications, Inc. Subpoena Enforcement Matter, 393 F.3d 771, 774 (8th Cir. 2005). Just as is the case here, the RIAA could identify the IP Addresses of the alleged infringers but could not identify the infringers by name without the assistance of the ISP that assigned the infringers their IP Addresses. The RIAA began its enforcement campaign by requesting federal Clerks of Courts to issue subpoenas pursuant to Section 512(h) of the Digital Millennium Copyright Act ("DCMA" or the "Copyright Act"). The RIAA would then serve a Section 512(h) subpoena on the ISP that assigned the Doe Defendant his or her IP address.

Section 512(h) provides for a comparatively easy process for obtaining the names of infringers vis-à-vis John Doe copyright infringement suits. Indeed, under Section 512(h)(2)(A)-(C), a copyright owner need only file three items with the Clerk of Courts along with its request for a 512(h)(2) subpoena: "(A) a copy of a notification described in subsection (c)(3)(A) [of

Section 512]; (B) a proposed subpoena; and (C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to discover the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title." If the Clerk finds that all three items are present then the Clerk must issue a Section 512(h) subpoena.

a. Verizon and Charter Challenge the 512(h) Subpoena Process

Several of the ISPs to whom the RIAA served Section 512(h) subpoenas moved to quash the subpoenas. These ISPs, including Charter and Verizon, appealed their district court losses to the D.C. and 8th Circuits. The central issue of these two cases was the propriety of serving a Section 512(h) subpoena on an ISP that merely "transmits" as opposed to "stores" data. See RIAA v. Verizon Internet Services, Inc., 351 F.3d 1229 (D.C. Cir. 2003); and In re Charter Communications, Inc., Subpoena Enforcement Matter, 393 F.3d 771 (8th Cir. 2005). "The stakes [were] large for the music, motion picture and software industries. . . ." the D.C. Circuit opined, because the Section 512(h) process was so much easier than a copyright infringement Doe suit. RIAA v. Verizon at 1238; accord In re Charter at FN3 (same.)

In the Verizon and Charter cases, the ISPs argued that a copyright owner cannot serve a Section 512(h) subpoena on an ISP that merely "transmits" data because the copyright owner cannot satisfy the condition precedent required by Section 512(h)(2)(A). Section 512(h)(2)(A) requires that the copyright owner deliver to the Clerk of Courts a copy of the notification described in Section 512(c)(3)(A). And, the ISPs argued, the notification to the ISP must contain "an identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material." (Emphasis added.) The ISPs argued that the copyright owner cannot provide them with notice of where the infringing data is located because the infringing data is not located on the ISPs servers; instead,

the infringing data is located on the infringers' computers over which the ISPs have no control. Put another way, the ISPs argued that copyright owners cannot send an ISP that merely "transmits" data a DMCA take down notice, which they contended is a condition precedent of using the 512(h) subpoena process.

b. The D.C. and Eighth Circuits Held Section 512(h) Subpoenas Cannot Be Served On ISPs that Merely Transmit Data

Rightly or wrongly, both the D.C. Circuit and the 8th Circuit, over the dissent of several esteemed jurists, agreed with the ISPs. After both Circuits ruled in favor of the ISPs, Section 512(h) subpoenas have not been used.

c. The ISPs in this Case Merely Transmit Data

Almost all of the internet service providers currently in existence, including all of the ones which Plaintiff desires to serve with subpoenas in this case merely "transmit" data. Put another way, Time Warner, AT&T, Cox, Charter, Cable One, Qwest, Clearwire, Verizon, etc. do not keep a copy of the movie on their servers and stream it to the Doe Defendants. Instead, the subject internet service providers merely provide the Doe Defendants with internet access, the cabling and other services necessary for the Doe Defendants to surf and use the internet. For this reason, under the Verizon and Charter decisions, Plaintiff cannot use the easy subpoena process provided by Section 512(h) of the DMCA to obtain the identity of the Doe Defendants from these ISPs.

2. Section 512(h) Does Not Preempt a Copyright Owner's Right to Ascertain the Identity of Infringers through a Subpoena Issued Pursuant to Fed.R.Civ.P. 45

Section 512(h) of the Copyright Act affords copyright owners an easy process to obtain the identities of internet users from ISPs that "store" data. Section 512(h) does not preempt a copyright owner's ability to obtain the identity of infringers through a Rule 45 subpoena from those ISPs that merely "transmit" data.

a. Appellate Courts Hold that the Use of Rule 45 Subpoenas in On-Line Infringement Cases to Identify Anonymous Doe Defendants is Permissible

Both the Eighth and Second Circuits have approved the use of Rule 45 subpoenas in on-line infringement cases to identify anonymous Doe Defendants. The Eight Circuit, during the great debate over whether a Section 512(h) subpoena could be used, held "organizations such as the RIAA can file a John Doe suit, along with a motion for third-party discovery of the identity of the otherwise anonymous 'John Doe' defendant." *In re Charter Communications, Inc., Subpoena Enforcement Matter,* 393 F.3d 771, FN3 (8th Cir. 2005). The Eighth Circuit's confirmation that a John Doe suit is proper was the express consolation prize for copyright owners when denied the right to use the easy process afforded by Section 512(h). Similarly, in *Arista Records, LLC. v. Doe 3,* 604 F.3d 110 (2d Cir. 2010) the Second Circuit upheld the District Court's denial of a motion to quash after Arista obtained leave "to serve a subpoena on defendants' common ISP, the State University of New York at Albany." By so holding, the Second Circuit approved the process of issuing a Rule 45 subpoena to an ISP to identify anonymous Doe Defendants.

b. Prior to Discovery, Plaintiff Cannot Know With 100% Certainty that the Subscriber is the Infringer

At the onset of a lawsuit, Plaintiff knows that the John Doe defendant's Internet was used to infringe Plaintiff's copyrights. In each of its complaints, Plaintiff alleges that the subscriber is the infringer. For the reasons set forth below, this allegation is plausible. While the subscriber is the infringer in the majority of instances, it is possible that someone other than the subscriber is the infringer. Indeed, the subscriber could be renting his or her house to a person using the subscribers internet to commit an infringement. Alternatively, the subscriber may have relatives or friends living with him or her who use the subscriber's internet and are the infringers. The probability of these occurrences is greatly diminished in the subject suits, however, because the

quantum of infringement committed by each of the Doe Defendants expands over of long period of time, and the Doe Defendants likely received DMCA notices from their ISPs alerting them to the instances of infringement. Presumably, a subscriber who is not the infringer but who receives a DMCA notice would reach out to any other person using the subscriber's internet service and cause the infringement to stop. Nevertheless, since there is a possibility that the subscriber is not the infringer, Plaintiff routinely agrees to refrain from publically identifying the John Doe Defendant by name in court papers until after the discovery period has concluded.

C. Plaintiff's Complaint States a Claim that is Plausible.

Every court to rule on whether Plaintiff's claims are "plausible" has found in Plaintiff's favor. *See e.g. Malibu Media, LLC v. John Doe 1*, 2013 WL 30648 (E.D. Pa. Jan. 3, 2013) ("Accepting all factual allegations in the Amended Complaints as true, *Iqbal*, 556 at 678, the Court concludes Plaintiff has stated a claim upon which relief can be granted under the Copyright Act."); *Malibu Media, LLC v. Pelizzo*, 2012 WL 6680387 (S.D. Fla. Dec. 21, 2012) ("[T]aking the allegations in the light most favorable to Plaintiff, the Complaint adequately states a claim of copyright infringement"); *Patrick Collins, Inc. v. Does 1-22*, 2011 WL 5439005 (D. Md. 2011) ("[T]he Court finds that Plaintiff has adequately stated a claim for copyright infringement.") Plaintiffs' complaints have *never* been dismissed pursuant to Rule 12(b)(6).

Further, the Second Circuit found that a copyright holder's suit against an online infringer is "plausible" through a detailed and well thought out analysis under the *Twombly* and *Iqbal* standards. *See Arista Records, LLC v. Doe 3*, 604 F.3d 110, 120 (2d Cir. 2010). In *Arista*, the Court specifically analyzed the requirements asserted by Twombly for pleading an inference of illegal conduct noting "[a]sking for plausible grounds to infer an agreement does not impose a probability requirement at the pleading stage; it simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of illegal[ity]." *Id*. citing *Bell Atl.*

Corp. v. Twombly, 550 U.S. 544, 127 S. Ct. 1955, 167 L. Ed. 2d 929 (2007).

> [Although *Twombly* and *Iqbal* require " 'factual amplification [where] needed to render a claim plausible,' " *Turkmen v. Ashcroft*, 589 F.3d 542, 546 (2d Cir.2009) (quoting *Ross v. Bank of America, N.A (USA)*, 524 F.3d 217, 225 (2d Cir.2008)), we reject Doe 3's contention that *Twombly* and *Iqbal* require the pleading of specific evidence or extra facts beyond what is needed to make the claim plausible.

Id. at 120-121. Likewise, here, Plaintiff's factual allegations in its Complaint are supported by factual assertions in its Exhibits. In support of its Motion for Leave, Plaintiff filed a sworn declaration from its investigator that the technology used to identify the Doe Defendant's IP address is accurate. *See* CM/ECF 4-2. On Exhibit A of Plaintiff's Complaint, Plaintiff demonstrates the dates and time the infringement occurred, the hash files, and the names of the movies infringed. On Exhibit B of Plaintiff's Complaint, Plaintiff demonstrates that its copyrights are properly registered. And on Exhibit C of Plaintiff's Complaint, Plaintiff provides evidence of all the other infringing activity that has taken place through Defendant's Internet. Plaintiff has provided enough factual support for it to be reasonable that the Defendant is the subscriber and the infringer. As stated above, based on the time period and abundance of infringement, causing high bandwidth usage, slow Internet speeds, DMCA notices, and other evidence of infringement taking place on the network, it is reasonable to believe the subscriber, who owns, pays for and is control of the Internet services, would not allow that activity to happen on his or her network unless he or she was committing the infringement.

It is without question that copyright infringement on the Internet is actionable. The Supreme Court in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* 545 U.S. 913, 125 S.Ct. 2764 (2005), found that Grokster was liable for contributory infringement because it materially aided and induced its users to commit direct infringement via its peer-to-peer file sharing service. Similarly, the First, Second, Seventh, Eighth, Ninth and D.C. Circuits have all held that peer-to-

peer infringement is actionable. *See Sony v. Tennenbaum,* 660 F.3d 487 (1st Cir. 2011) holding in a twenty-six (26) page opinion that Tennenbaum was liable for infringement committed through a peer-to-peer network, that peer-to-peer infringement is not "fair use" nor would any other defense shield Tennenbaum's tortious conduct, and that the statutory damages clause set forth in the Copyright Act is constitutional; *Arista Records, LLC. v. Doe 3*, 604 F.3d 110 (2d Cir. 2010) denying an individual John Doe Defendant's motion to quash a subpoena issued to an internet service provider in response to an allegation that the John Doe Defendant infringed Arista's copyrights through a peer-to-peer file sharing network; *In re Aimster Copyright Litigation*, 334 F.3d 643 (7th Cir. 2003) upholding a preliminary injunction because Aimster was contributorily liable for its users' direct infringements; *In re Charter Communications, Inc. Subpoena Enforcement Matter*, 393 F.3d 771, 774 (8th Cir. 2005) opining that copyright owners have a right to identify peer-to-peer file sharers through a Rule 45 subpoena because those file sharers *are* infringing the owners' copyrights; *A&M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004, 1013 (9th Cir. 2001) "[w]e agree that the plaintiffs have shown that Napster users infringe at least two of the copyright holders' exclusive rights: the rights of reproduction, § 106(1); and distribution, § 106(3);" and *RIAA v. Verizon Internet Services, Inc.*, 351 F.3d 1229, 1238 (D.C. Cir. 2003) repetitively acknowledging that file sharing is infringement. Significantly, "District courts . . . agree . . . that downloading music from the internet, without paying for it or acquiring any rights to it, is a direct violation of the Copyright Act." *UMG Recording, Inc. v. Alburger*, 2009 WL 3152153, *3 (E.D. PA. 2009).

D. *Patrick Collins, Inc. v. Doe 1*, No. 12-cv-1154 (ADS) (GRB), __ F.R.D. __ , 2012 WL 5879120, at *4-*5 (E.D.N.Y. Nov. 20, 2012) and Plaintiff's Citations

Plaintiff respectfully suggests that the case cited by this Court, *Patrick Collins, Inc. v. Doe 1*, No. 12-cv-1154 (ADS) (GRB), __ F.R.D. __ , 2012 WL 5879120, at *4-*5 (E.D.N.Y.

Nov. 20, 2012) is not contrary authority, nor is it controlling authority to this Court. In *Patrick Collins, Inc.* the Eastern District of New York upheld a magistrate's ruling that ***allowed*** Patrick Collins to subpoena an ISP to receive the identifying information of one John Doe defendant. *See Patrick Collins, Inc. v. Doe 1*, 12-CV-1154 ADS GRB, 2012 WL 5879120 (E.D.N.Y. Nov. 20, 2012) ("**ORDERED** that Judge Brown's Report and Recommendation is adopted in its entirety.") Judge Brown's Report and Recommendation granted the plaintiff the ability to subpoena a doe defendant's ISP to receive the doe defendant's identity, because without doing so, a copyright plaintiff would be without a remedy. Indeed, Judge Brown specifically stated, "these plaintiffs are allegedly the owners of copyrighted works who should not be left without any remedy." *In re BitTorrent Adult Film Copyright Infringement Cases*, CIV.A. 11-3995 DRH, 2012 WL 1570765 (E.D.N.Y. May 1, 2012). Likewise, Plaintiff is asking the Court to not leave it without a remedy.

Further, in every single copyright BitTorrent case cited in *Patrick Collins, Inc. v. Doe 1*, a court granted a copyright plaintiff its motion to subpoena at least one John Doe defendant, when personal jurisdiction was proper, as in this case. *See Next Phase Distribution, Inc. v. John Does 1-27*, 284 F.R.D. 165, 172 (S.D.N.Y. 2012) ("**ORDERED** that Motion for Discovery (Docket No. 5) is **GRANTED** with respect to John Doe 1"; *DigiProtect USA Corp. v. Does*, 10 CIV. 8760 PAC, 2011 WL 4444666 (S.D.N.Y. Sept. 26, 2011) (dismissed on the basis of improper personal jurisdiction); *Media Products, Inc. v. John Does 1-26*, 12 CIV. 3719 HB, 2012 WL 3866492 (S.D.N.Y. Sept. 4, 2012) ("ORDERED that the ISPs shall not turn over any further personal information to Plaintiffs other than as to John Doe 1"); *Patrick Collins, Inc. v. John Does 1 through 37*, 2:12-CV-1259-JAM-EFB, 2012 WL 2872832 (E.D. Cal. July 11, 2012) ("Plaintiff may immediately serve a Rule 45 subpoena on Charter Communications (the ISP listed for the first John Doe in Exhibit A to plaintiff's complaint and in plaintiff's proposed order

on the application for expedited discovery) to obtain the following information about that John Doe (based on the IP address listed for him/her—24.182.55.21): name, address, telephone number, and email address); *Digital Sins, Inc. v. John Does 1-245*, 11 CIV. 8170 CM, 2012 WL 1744838 (S.D.N.Y. May 15, 2012) ("I hereby *sua sponte* quash any subpoena that may be outstanding to any internet service provider seeking information about the identity of any John Doe defendant other than John Doe 1"); *Patrick Collins, Inc. v. Does 1-6*, 12 CIV. 2964 JPO, 2012 WL 2001957 (S.D.N.Y. June 1, 2012) ("ORDERED that Plaintiff is allowed to conduct immediate discovery on the ISPs listed in Exhibit B to the Declaration of Tobias Fieser"); *SBO Pictures, Inc. v. Does 1-20*, 12 CIV. 3925 SAS, 2012 WL 2034631 (S.D.N.Y. June 5, 2012) ("As to discovery regarding both Doe 1 and any other Doe defendants against whom claims are re-filed, I adopt the procedures of Judge McMahon and Magistrate Judge Brown"); *Digital Sin, Inc. v. Does 1-176*, 279 F.R.D. 239, 244 (S.D.N.Y. 2012) ("**IT IS HEREBY ORDERED** that Digital Sin may immediately serve a Rule 45 subpoena on the ISPs listed in Exhibit A to the Complaint to obtain information to identify Does 1–176, specifically her or his name, address, MAC address, and email address"); *Media Products, Inc. v. John Does 1-26*, 12 CIV. 3719 HB, 2012 WL 3866492 (S.D.N.Y. Sept. 4, 2012) ("ORDERED that the ISPs shall not turn over any further personal information to Plaintiffs other than as to John Doe 1 in each named case and in accordance with my earlier orders."); *Arista Records LLC v. Does 1-16*, 1:08-CV-765 GTS/RF, 2009 WL 414060 (N.D.N.Y. Feb. 18, 2009) *aff'd sub nom. Arista Records, LLC v. Doe 3*, 604 F.3d 110 (2d Cir. 2010) ("The discovery information sought by the Plaintiffs is specific and reasonable. The Subpoena seeks the IP user's name, address, telephone number, email address, and MAC, and nothing else that would be considered intrusive. All of this information will reasonably facilitate Plaintiffs' efforts to serve process upon the alleged offenders in order to bring suit against them for their alleged conduct. Once again, this is another element that tips in

Plaintiffs' favor"); *AF Holdings, LLC v. Doe*, C 12-2049 PJH, 2012 WL 3835102 (N.D. Cal. Sept. 4, 2012) (granting a Motion to Dismiss on the basis of a negligence claim which has not been pled here by Plaintiff); *Patrick Collins, Inc. v. Does 1-4*, 12 CIV. 2962 HB, 2012 WL 2130557 (S.D.N.Y. June 12, 2012) ("ORDERED that Plaintiff is allowed to conduct immediate discovery on the ISPs listed in Exhibit B to the Declaration of Tobias Fieser").

Some of the courts listed above have used the joinder rule to limit a plaintiff's ability to identify Doe defendants on a large scale basis. That judicial strategy has worked insofar as plaintiff does not have to sue everyone in the same swarm the plaintiff can look at all the movies the defendants have downloaded and only sue the most egregious infringers. That is what Plaintiff has done here.

Plaintiff was not obligated to cite *Patrick Collins, Inc. v. Doe 1*, No. 12-cv-1154 (ADS) (GRB), __ F.R.D. __ , 2012 WL 5879120, at *4-*5 (E.D.N.Y. Nov. 20, 2012). The Maryland Rules of Professional Conduct state: "A lawyer shall not knowingly ... fail to disclose to the tribunal legal authority in the controlling jurisdiction known to the lawyer to be directly adverse to the position of the client and not disclosed by opposing counsel[.]" MD R CTS J AND ATTYS Rule 16-812, MRPC 3.3. This case was not controlling on this Court because it arose in the Eastern District of New York which is not a court within the Fourth Circuit. Further, it is not controlling because it was an opinion of a District Court and therefore not binding on this Court. Finally, as stated above, the holding in that case is consistent with the holding Plaintiff urged upon this Court. Namely, that Plaintiff should be allowed to subpoena the identity of one John Doe Defendant per lawsuit filed. A large amount of case law exists on the subject of copyright infringement suits on the Internet. Indeed, a search on Westlaw of "bittorrent", "copyright" and "subpoena" reveals over 300 cases. Undersigned, in both its original Motion for Leave and its

Memorandum Explaining Why it has a Clear and Undeniable Right to Issue a Rule 45 Subpoena made an effort to cite as much case law as possible.

E. <u>If Malibu Media is granted a subpoena to serve on an ISP and determines the name and address of the IP subscriber, what does Malibu Media intend to do with that information?</u>

Plaintiff is going to litigate its case. Attached as Exhibit B is a 26(f) report from *Malibu Media, LLC v. John Does 1, 6, 13, 14, and 16*, Case No. 2012-2078, in the Eastern District of Pennsylvania, which sets forth how Plaintiff litigates its cases.

In its Complaint, Plaintiff has provided every Defendant with an exculpatory evidence form and the opportunity to provide evidence of non-infringement to Plaintiff. With any Defendant that fails to provide a credible basis for non-infringement, Plaintiff will serve the Defendant and proceed to litigate. Should the Court desire Plaintiff to do so, Plaintiff will file any identifying information by the Defendants under seal or anonymously, in order to prevent any unnecessary leverage or pressure to settle. After that, Plaintiff will serve Defendant. Plaintiff will depose the ISPs to lay the foundation of its records into evidence, depose search engines to evaluate certain key words and whether the defendant was searching for Plaintiff's content, and depose the defendant. If a "someone else used my internet" defense is presented, Plaintiff will depose the other potential users. Plaintiff has an expert on retainer to look at the computers. This expert is also in the process of preparing a report that demonstrates that IPP's software is accurate and works exactly the way IPP testifies that it works. Plaintiff will file this report in its cases once it is completed. Copies of the experts' CVs will be attached.

Plaintiff will prove beyond a preponderance of the evidence that the infringement was committed through the internet service reflected by the Internet Protocol Address ("IPA") subscribed to by each John Doe Defendant. Although unlikely, Plaintiff may also substitute a person other than the ISP subscriber from whose internet service infringement took place. This

is the reason Plaintiff is saying in the first instance that the John Doe defendant can remain anonymous through the end of discovery.

Plaintiff's expectation is that probably about one third of its cases will not proceed past receiving the identity of the Defendant from the ISP. This is because in some cases the ISP does not have records of an IPA because of its limited data retention. Also, in some cases a Defendant will prove to be active duty military, or unable to pay a judgment. In these cases, Plaintiff does not pursue the Defendant. Should a Defendant want to settle early in the litigation process, Plaintiff will consider any offers and may in turn propose its own settlement offer.

F. Limitation of Subpoenas to Curb Unwarranted Pressure to Settle

Plaintiff suggests that a protective order requiring that Court filings not contain the Doe Defendant's name prior to the end of the discovery period will enable fair litigation by both parties and remove any potential for exploitation. Plaintiff does not suggest that any other limitations be imposed on the scope of the subpoena or that any of the regular rules of procedure which govern all cases be modified.

G. The Effect of the "Six Strikes" Program on Issuing a Subpoena

The "Six Strikes" program does not alleviate the need for copyright holders like Plaintiff to request subpoenas. First, "Six Strikes" is for MPAA and RIAA affiliate members only. Plaintiff has not been provided the benefit of participating in this program. Further, those involved in creating the "Six Strikes" program have made it clear that it is not intended to deter the most consistent and extreme infringers, whom Plaintiff is suing[3]. Indeed, Thomas Dailey, the senior VP of Verizon, stated, "this [] system is not going to stop hardcore infringers" and that it

[3] http://www.broadcastingcable.com/article/492241-Six_Strikes_Alerts_Get_Once_Over_on_Hill.php "She said she expected that people after a couple of warnings will get the message, but conceded it won't stop the hard-cores"

is instead about changing behavior, "where it can be corrected."[4] This process is not designed by Congress or enacted into law and therefore does not supersede the Copyright Act which grants a copyright holder the right to sue an individual for copyright infringement and does not replace Plaintiff's right to subpoena the identity of a John Doe defendant to prosecute a claim for infringement.

H. IPP Ltd's Reliability

Adverse counsel raise issues regarding Plaintiff's technology and investigator, IPP Ltd. Respectfully, these critiques have absolutely no basis in fact. IPP, Ltd.'s detection technology is 100% accurate and the process of detection is unimpeachable. As stated above, Plaintiff is currently in the process of having independent expert witnesses with computer forensic backgrounds evaluate IPP's software in order to provide testimony that the software works. These experts have already thoroughly tested the software and orally reported to Plaintiff that the software does work as described. Plaintiff anticipates this report will be completed in the next few weeks and will file the report in these proceedings at the appropriate time.

1. An Internet Protocol Address Cannot Be Spoofed

In the letter by John C. Lowe [CM/ECF 14-6] adverse counsel suggests that Plaintiff's identification of an Internet Protocol Address ("IPA") may be inaccurate because it is possible to spoof the IPA. "In computer networking, the term IP address spoofing or IP spoofing refers to the creation of Internet Protocol (IP) packets with a forged source IP address, called spoofing, with the purpose of concealing the identity of the sender or impersonating another computing system."[5] While this may be possible with some software, in each case before this Court, Plaintiff is certain that the IPA was not spoofed. Indeed, IPP's software established a direct

[4] Id.
[5] http://en.wikipedia.org/wiki/IP_address_spoofing citing http://66.14.166.45/sf_whitepapers/tcpip/IP%20Spoofing%20-%20An%20Introduction.pdf

Transmission Connection Protocol/Internet Protocol ("TCP/IP")[6] connection with the John Doe Defendants' IP address. *See* Complaint ¶17. When a direct TCP/IP connection is established, it is impossible for an individual to hide, mask, or spoof his or her IP address because that individuals computer directly connects with IPP's server. This fact was attested to by the MPAA, RIAA and the ISPs during the hearings for Six Strikes and there are several academic journals that reach the same conclusion.

2. IPP'S Relationship with Guardaley and the German High Court

In the letter by Jason Sweet [CM/ECF 14-3], adverse counsel suggests that IPP Limited (1) may not exist; (2) if it does exist is the same as the German investigators Guardaley; and (3) that the State Court of Berlin found flaws regarding Guardaley's technology. Adverse counsel sets forth these conspiracy theories with little evidence.

First, IPP's expert Tobias Fieser will be a fact witness. Second, IPP, Ltd. and Guardaley have no common ownership or clients. Occasionally, the two companies work with each other, mainly because they are in the same common field and location. Further, adverse counsel's

---

[6] "TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

"TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination." http://searchnetworking.techtarget.com/definition/TCP-IP

letter misidentifies Guardaley's owner as Patrick Achache, further demonstrating that it is based simply on conjecture.

The German investigative company Guardaley has not reinvented itself as IPP, Ltd. Indeed, Guardaley is still filing declarations in several cases. See e.g. *Studio West Productions, Inc. v. Does 1-14*, Case No. 2:13-cv-00370-AB (E.D. Pa., January 28, 2013); *Studio West Productions, Inc. v. Does 1-237, Case No. 4:12-cv-03690* (S.D. Tex., January 8, 2013); *Studio West Productions, Inc. v. Does 1-205*, Case No. 4:12-cv-03691 (S.D. Tex., January 8, 2013); *Nu Image, Inc. v. Does 1-91*, Case No. 4:12-cv-00331-RH-CAS (N.D. Fla., October 26, 2012). Finally, adverse counsel misstates the proceedings which took place in Berlin regarding Guardaley's technology. The findings adverse counsel suggests were *not* proven in court or by a third party expert but by merely alleged by a competitor. The judgment which adverse counsel refers to is not legally binding, and most importantly Guardaley's case has no bearing on IPP, Ltd. With each John Doe Defendant in this case, Plaintiff can provide Defendant with a packet sniffer demonstrating the piece of the BitTorrent file that the Defendant was distributing. As Plaintiff's experts will testify, the packet sniffer and direct TCP/IP connection simply cannot be manipulated or spoofed. Put simply, the detection technology employed by IPP, Ltd. is simply not a major concern of Plaintiff's. It is infallible and the process is not impeachable. If challenged, Plaintiff will prove these points.

1. CONCLUSION

For the foregoing reasons Plaintiff respectfully requests that the Court grant Plaintiff's motion for leave to subpoena the John Doe Defendants identities.

Dated: March 23, 2013

Respectfully submitted,
MALIBU MEDIA, LLC.
PLAINTIFF

By: /s/*Jon A. Hoppe*
Jon A. Hoppe, Esquire #6479
Counsel
Maddox, Hoppe, Hoofnagle & Hafey, L.L.C.
1401 Mercantile Lane #105
Largo, Maryland 20774
(301) 341-2580

CERTIFICATE OF SERVICE

I hereby certify that on March 23, 2013, I electronically filed the foregoing document with the Clerk of the Court using CM/ECF and that service was perfected on all counsel of record and interested parties through this system and to both adverse and amici counsel through the following electronic mail addresses:

lholzman@theholzmanlawfirm.com;

jsweet@boothsweet.com;

johnseiver@dwt.com;

bhuffman@lockelord.com;

johmlowe@johmlowepc.com

irasiegel@earthlink.net.

By: /s/*Jon A. Hoppe*

EXHIBIT T

Vacancies24.de
Alle Stellenangebote auf einen Blick!

Suchen

Linux Administrator/ Programmierer in Vollzeit Arbeitsort: Karlsruhe, Baden
IPP Int. / Systemplaner und systemanalytiker / Baden-Württemberg
Bitte beachten Sie, dass die Bewerbungsfrist abgelaufen ist.

Alle Jobs für systemplaner und systemanalytiker in Baden-Württemberg
Alle Jobs bei IPP Int. in Baden-Württemberg

IPP Int. ist abgestimmt auf die Bedürfnisse von Unternehmen aus den Bereichen der Software- und Unterhaltungsindustrie. Die Basis unseres Portfolios sind Software Eigenentwicklungen sowie unsere globale Internet-Infrastruktur. Wir sind der perfekte Partner für ganzheitlichen Schutz digitaler Inhalte jeglicher Art. Durch die Kombination verschiedener Methoden und Techniken erreichen wir eine nie dagewesene Abdeckung und ganzheitlichen Schutz von Software, Filmen, Musik, Bildern und Texten. Von Downloads bis hin zu illegalen Verkäufen - unsere Ermittlungen decken jeden Bereich ab. Die Effektivität, mit der wir unsere Produkte betreiben und kombinieren, ermöglicht unsere Dienstleistungen besonders kosteneffizient anzubieten. Unser Angebot: Einen zukunftssicheren Arbeitsplatz in einem hochmotivierten Team und ein interessantes Aufgabenfeld. Ihre Aufgabe: Serveradministration und Skriptprogrammierung Mysql Datenbank und VMware ESX Server Ihr Profil Sie verfügen über umfangreiche Kenntnisse folgenden Bereich: ¿ Umgang mit Linux-Betriebssystemen ¿ Administration von MySQL Datenbanken ¿ SQL ¿ PC- und Netzwerktechnik ¿ Skriptprogrammierung (wenn möglich Pearl) Optionale Kenntnisse: ¿ Webprogrammierung (PHP, HTML.) ¿ Windows Programmiersprachen (C++, VB) - Geforderte Anlagen: Lebenslauf, Zeugnisse; Kenntnisse und Fertigkeiten: Betriebssystem LINUX; Datenbank MySQL; Datenbank SQL; PC-Technik

Veröffentlicht am
2011-10-12

E-Mail
jobs@guardaley.com

Telefon
+49 721 66800093

Adresse
Am Hubengut 8, D-76149 Karlsruhe, Baden, Deutschland

Weitere Informationen
Jennifer Cindori

Wie bewirbt man sich
per Email

Bitte beachten Sie, dass die Bewerbungsfrist abgelaufen ist.

Meistgesuchte Jobs

- Verkäufer/in im BASE Shop ...
- Tischler/in Arbeitsort: S ...
- Fachlagerist/in Arbeitsor ...
- Filialleiter/in im BASE S ...
- Teamassistenz/ Büroassist ...
- Amtsvormund/Amtspfleger (...
- Stop! Weiterlesen ! Hier ...
- Elektroniker/in Arbeitsor ...
- Examinierte Pflegefachkra ...
- Automaten-Techniker für W ...
- Sportlehrer/in Arbeitsort ...
- Podologin gesucht Arbeits ...
- Architekt/in Arbeitsort: ...
- TOP>> Mehrere Service-Tec ...
- Ergotherapeut/in im mobil ...

Beliebte Tags

- Klebetechnik
- Hydraulikmonteure
- Mehlingen
- Interaktiv
- Primonda

Neue Arbeitgeber

- Xchange Language Services ...
- Skare fleisch
- Dr. Bilir, Martinovic, St ...
- BVU GmbH
- Klaus Hinz Taxiunternehmen
- Gasthaus Almbachklamm Ber ...
- Schornsteinfeger
- Werksarztzentrum Deutschl ...
- Opticost GmbH
- PolygonVATRO GmbH

Links

Kontaktieren Sie uns
Stellennummer: 6753360

EXHIBIT U

Hauptmenü

Home
Imprint
Services

Imprint

IPP International Unternehmensgesellschaft (haftungsbeschränkt)

Überseering 25
22297 Hamburg
Deutschland

Fon: + 49 (0) 40 600 385 3230
Fax: +49 (0) 40 600 385 3237
E-Mail: info@ippint.de
Internet: www.ippint.de

CEO: Uwe Hennrich

Registergericht: Amtsgericht Hamburg
Registernummer: HRB 115546

Disclaimer:

1. Online-contents
The author reserves the right not to be responsible for the topicality, correctness, completeness or quality of the information provided. Liability claims regarding damage caused by the use of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected. All offers are not-binding and without obligation. Parts of the pages or the complete publication including all offers and information might be extended, changed or partly or completely deleted by the author without separate announcement.

2. Referrals and links
The Author is not responsible for any contents linked or referred to from his pages - unless he has full knowledge of illegal contents and would be able to prevent the visitors of his site from viewing those pages. If any damage occurs by the use of information presented there, only the author of the respective pages might be liable, not the one who has linked to these pages. Furthermore the author is not liable for any postings or messages published by users of discussion boards, guestbooks or mailinglists provided on his page.

3. Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic or printed publications is not permitted without the author's agreement.

4. Legal force of this disclaimer
This disclaimer is to be regarded as part of the internet publication which you were referred from. If sections or individual formulations of this text are not legal or correct, the content or validity of the other parts remain uninfluenced by this fact.

Hauptmenü

- Home
- Imprint
- Services

Imprint

IPP International Unternehmensgesellschaft (haftungsbeschränkt)

Hermannstraße 9
20095 Hamburg
Deutschland

Fon: + 49 (0) 40 600 385 3230
Fax: +49 (0) 40 600 385 3237
E-Mail: info@ippint.de
Internet: www.ippint.de

CEO: Uwe Hennrich

Registergericht: Amtsgericht Hamburg
Registernummer: HRB 115546

UST-ID Nr.: DE 279686524

Disclaimer:

1. Online-contents
The author reserves the right not to be responsible for the topicality, correctness, completeness or quality of the information provided. Liability claims regarding damage caused by the use of any information provided, including any kind of information which is incomplete or incorrect, will therefore be rejected. All offers are not-binding and without obligation. Parts of the pages or the complete publication including all offers and information might be extended, changed or partly or completely deleted by the author without separate announcement.

2. Referrals and links
The Author is not responsible for any contents linked or referred to from his pages - unless he has full knowledge of illegal contents and would be able to prevent the visitors of his site from viewing those pages. If any damage occurs by the use of information presented there, only the author of the respective pages might be liable, not the one who has linked to these pages. Furthermore the author is not liable for any postings or messages published by users of discussion boards, guestbooks or mailinglists provided on his page.

3. Copyright
The author intended not to use any copyrighted material for the publication or, if not possible, to indicate the copyright of the respective object. The copyright for any material created by the author is reserved. Any duplication or use of such diagrams, sounds or texts in other electronic or printed publications is not permitted without the author's agreement.

4. Legal force of this disclaimer
This disclaimer is to be regarded as part of the internet publication which you were referred from. If sections or individual formulations of this text are not legal or correct, the content or validity of the other parts remain uninfluenced by this fact.

EXHIBIT V

Imprint

BSAG Bueroservice24 AG
Überseering 25
22297 Hamburg

Free advice: 0800-8885885

E-mail: info (at) bueroservice24.de
URL: www.bueroservice24.de

Chairman Marcus Polke
Board of Directors: Christian Weber, Kim Barthel
Commercial Register: Amtsgericht Hamburg HRB 112 851
VAT Reg. DE270104172

Tel: 040-600385-0
Fax: 040-600385-130

Geschäftsadresse Hamburg einfach und zuverlässig, fähig, preiswert! | Bueroservice24 AG

http://www.bueroservice24.de/geschaeftsadresse-hamburg-einfach-und-zuver

RUN powered by ADP Trademark E...tem (TEAS) Apple Yahoo! Google Maps YouTube Wikipedia News (4183) Popular

Bueroservice24.de

Persönliches Telefon-Sekretariat

Gleich anrufen und informieren: 040/600385 - 4990

Jetzt 2 Wochen
kostenlos testen!

31

Eine Geschäftsadresse in Hamburg inklusive eigener Telefonnummer?

Sie sind auf der Suche nach einem Anbieter, der Ihnen eine deutschen Postadresse inklusive deutscher Telefon- und Faxnummer generiert und betreut? Wir helfen Ihnen!

Wir verlegen Ihre Geschäftsadresse an Hamburgs exklusivste Adresse - in die Hermannstraße 9! Das heißt, wir generieren eine Postadresse für Ihr Unternehmen (mit eigenem Namensschild am Eingang) an die Kunden und Geschäftspartner Ihre Post und Pakete senden können. Wir nehmen diese entgegen und senden Sie an Sie weiter. Die Hamburger Adresse schafft Seriosität und Vertrauen bei Ihren Kunden. Gerne bieten wir Ihnen zusätzlich eine Hamburger Telefon- und Faxnummer an, unter der wir Ihre Anrufe unter Ihrem Unternehmensnamen annehmen, sobald Sie bei Ihrem Telefon die Rufumleitung aktivieren.

Ihre neue Geschäftsadresse in der Hamburger Hermannstraße 9, in 20095 können Sie für 84,90 Euro nutzen. Auch hier besteht die Möglichkeit, diese in Verbindung mit einem Telefonservice-Paket zu buchen. So sparen Sie sich eine teure Büromiete und Möblierung und haben eine professionelle Bürovertretung für Ihr Unternehmen! Die **Geschäftsadresse Hamburg einfach und zuverlässig** nutzen zu können, schätzen unsere Partner: Viele Unternehmen berichten uns stetig die positiven Rückmeldungen Ihrer Kunden auf unseren Telefonservice. Das Gute daran ist, dass diese nicht gemerkt haben, dass sie mit einem externen Telefonsekretariat verbunden wurden.

Wenn sich weitere Fragen ergeben haben oder Sie sich über zusätzliche Leistungen wie den Büroservice oder Bonitätsauskünfte informieren sollen, so melden Sie Bedarf an unter unserer Firmennummer:

040/ 600385 - 4990

O Herr O Frau

Ihr Name:*

Telefonnummer:*

E-Mail:*

* Pflichtfelder

Jetzt Rückruf anfordern!

Folgende Seiten könnten Sie auch interessieren

Büroservice Aachen
Büroservice Berlin
Büroservice Düsseldorf
Büroservice Frankfurt (Main)
Büroservice Hamburg
Büroservice Heidelberg
Büroservice Karlsruhe
Büroservice Kiel
Büroservice Köln

Google Translate

http://translate.google.com/translate?sl=de&tl=en&js=n&prev=_t&hl=en&ie=

RUN powered by ADP Trademark E...tem (TEAS) Apple Yahoo! Google Maps YouTube Wikipedia News (4183) Popular

Try a new browser with automatic translation. Download Google Chrome Dismiss

Google http://www.bueroservice24.de/geschaeftsadresse-hamburg-einfach-und- +morgan Share

Translated in Safe Mode. This may cause problems with some websites, especially those that use plugins like Flash. Click here to disable Safe Mode

Translate From: German To: English View: Translation Original

Bueroservice24.de

Persönliches Telefon-Sekretariat

Call immediately and inform: 040 / 600385-4990

Now two weeks
Free Trial Now!

31

A business address in Hamburg, including its own phone number?

You are looking for a provider that you generated a German postal address including German telephone and fax number and cared for? We can help!

We publish your business address on Hamburg's most exclusive address - in the Hermann Street 9! That is, we generate a mailing address for your business (with its own name sign at the entrance) to the customers and business partners can send your mail and packages. We accept this and send it on to you. The address in Hamburg creates integrity and trust with your customers. We are happy to offer you a hamburger telephone and fax number in addition, under which we accept your calls to your company name as soon as you activate the diversion on your telephone.

Your new business address in Hamburg Hermann Strasse 9, 20095 in, you can use for 84,90 Euro. Again, there is the possibility this in conjunction with a telephone service to book package. To save yourself an expensive office rent and furniture and have a professional office representation for your business! To use the **business address Hamburg simple and reliable,** value our partners: Many companies tell us constantly the positive feedback of your customers to our Phone Service. The good thing is that they have not realized that they were connected to an external telephone Secretariat.

O Mr. O Woman

Your Name: *

Telephonenumber: *

E-Mail: *

* Mandatory fields

Request a Call Now!

The following pages, you might also consider

Secretarial services Aachen

https://maps.google.com/maps?client=safari&oe=UTF-8&q=Hermannstraße+9+20095+Hamburg+Deutschland&ie=UTF-8&hq=&hn

Hermannstraße 9 20095 Hamburg Deutschland

RUN powered by ADP | Trademark E...tem (TEAS) | Apple | Yahoo! | Google Maps | YouTube | Wikipedia | News (4167) | Popular

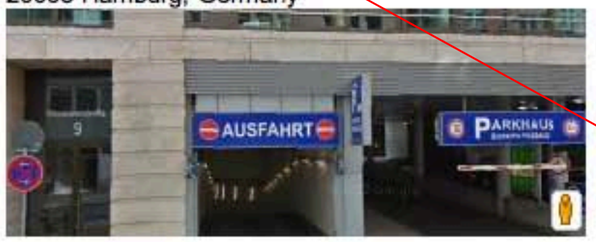
Google

Hermannstraße 9 20095 Hamburg Deutschland

+morgan | Share

Get directions | My places

Hermannstraße 9
20095 Hamburg, Germany



Directions | Search nearby | Save to map | more

Maps Labs - Help

Satellite | Traffic

Aktiengesellschaft
Hogan Lovells International LLP
Dr. Götze Land + Karte
Alstertor
Dr. Götze Flug & Reise
MM Warburg & Co
Credit Suisse (Deutschland)
Schuhhaus Horsch Sondergrößen
Barbier
UBS Deutschland
hessnatur Hamburg
Street Super Shoes
Unisono
Prüssmann & Sohn e. K. Andre Reinhardt
Backeria GmbH & Co. KG Bäckerei
highQ Computerlösungen GmbH - Büro Hamburg
Werkhaus
Raboisen
Butlers
Bueroservice24.de
Playa Games
Rechtsanwalt Löffler Klaus P
HSH Real Estate Treuhand
Action Direct Werbeagentur
City Back
Allyve GmbH & Co.
World Coffee
Shoes
Grüne Erde
Tom Tailor in der Europapassage
Erdgeschoss E1
Eingang / Ausgang
Bianco Footwear Europa-Passage
Jochen Schweizer Shop Europa Passage
Hilfiger Denim store
EDC PS Store Hamburg
Street One
Tally Weijl
BoseÂ® Experience Center
Cecil Store
Jeff Green
50 ft
20 m

Map data ©2014 GeoBasis-DE/BKG (©2009), Google - Edit in Google Map Maker | Report a problem

Telephone counseling for FREE 0800 8 885 885

Now two weeks

free test!

Immediately test

Convince yourself personally and quickly in just two minutes from the quality of our services and the professionalism of our technical secretaries and secretaries! The immediate test is completely free and without obligation.

Now start the test immediately

Personal quote

In the future, always be reached by phone at attractive rates: Get our no-obligation quote for your personal phone Bueroservice24.de Secretariat.

Get a Quote Now

Industry Solutions

Real estate agents, online shops - Exposé shipping, order taking, appointment - every industry has its specific requirements of our professional Telephone-secretariat. Learn more here!

Choose an Industry

The advantages of a professional secretariat by telephone Bueroservice24.de for you:

100 percent accessibility: Optimize your business performance and grow your business through a permanent telephone availability. No call you will get lost!

Real-time conversation Note: Whether you are in a meeting or on vacation. Immediately after the phone call you receive an e-mail, SMS or a fax and can act and react accordingly.

Corporate Benefits: Through our professional answering service will show potential customers and other key audiences professionalism and integrity - and thereby have more time for your business success.

Professional answering: Our professional staff understands your needs and industry characteristics, and knows how to communicate with your callers professionally and success-oriented - in your company name.

Flexible rates, we know that entrepreneurs different demands on a phone have a medium as a company secretary. Therefore we offer to businesses of any size and any industry the right tariff.

High German and English guarantees: As a Hamburg company, we offer you and your callers a perfect High German and English - guaranteed.

Telephone-secretariat
Benefits
Immediately test
Offer Calculator
And Price List
Entry-level package
Standard Package
Professional Package
Weekend Package

Services
Business address
Credit Report
Industry Solutions

Social Media
The SME blog
Facebook
Google +
Twitter
Xing

Business
Home
Contact
Cooperation
Affiliate
Press
Jobs

Support
Terms and Conditions
FAQ
Privacy Policy
Imprint
Lexicon
Sitemap

TUV tested

Germany's largest office survey showed that poor telephone accessibility has a negative effect on customer relationships.

We are here for you - if you are not there - and beyond!
Our professional and nationwide phone service is the core competence of our company. In addition, we offer additional services, secretarial services - even in multiple languages - for business customers. We guarantee our customers a reliable business and personal secretarial services. With modern communication technology and trained professionals, we enable your company secretaries constantly available to your customers and business partners for your support as well as vacation and sick leave. With an inexpensive and attractive pricing model, we help you reduce your fixed costs. In addition to an affordable fee, you pay only for services actually provided and verifiable.

Bueroservice24.de also offers you an exclusive business address in Hamburg. Find out about our Hamburg business addresses .

Take advantage of our service Services for your business or yourself and contact us today so that we are there for your customers if it can not be themselves.

If you have further questions about the telephone office, the credit information or other products? Perhaps you can find in our FAQs that answer.

We thank the many customers who are already our telephone service or office service.

EXHIBIT W

Morgan Pietz <morganpietz@gmail.com>

Defendant Deposition Availability, 8:13-cv-3024, MD109

Jon Hoppe <JHoppe@mhhhlawfirm.com> Sat, Mar 1, 2014 at 5:23 PM
To: "Morgan E. Pietz" <mpietz@pietzlawfirm.com>
Cc: "John C. Lowe" <johnlowe@johnlowepc.com>

Dear Messrs. Pietz and Lowe:

I am interested in taking the deposition of your client in this case as soon as possible. Would you please contact me as soon as possible to set up an appropriate date for doing so? If I do not hear from you shortly, I may have no other recourse than to act unilaterally on this issue. Thank you for your prompt attention to this matter.

Very truly yours,

Jon A. Hoppe, Esquire
Maddox, Hoppe, Hoofnagle & Hafey, L.L.C.
1401 Mercantile Lane #105
Largo, Maryland 20774
(301) 341-2580 (ph.)
(301) 341-5727 (fax)

EXHIBIT X

Morgan Pietz <morganpietz@gmail.com>

Malibu Media - D. Md. - 13-3024 - Deposition and Discovery re IPP "Oral Contingency Agreement"

3 messages

Morgan E. Pietz <mpietz@pietzlawfirm.com> Mon, Mar 3, 2014 at 2:02 PM
To: "Jon A. Hoppe" <jhoppe@mhhhlawfirm.com>
Cc: "John C. Lowe" <johnlowe@johnlowepc.com>

Jon,

Per our conversation -- to confirm:

(1) I will get back to you regarding tentative date availability for a deposition of my client in this case, on Monday 3/31 or Tuesday 4/1. If necessary, I will stipulate to extend the discovery deadline.

(2) Attached, please find a recent motion to exclude the testimony of IPP, on the ground that it comes from an expert (or fact) witness being impermissibly compensated on a contingent fee basis, filed in a Malibu case in Colorado, which will serve as a jumping off point for my further inquiry on this issue. The verified discovery responses I mentioned from MM are attached as exhibits thereto.

As I explained, I would like a firm answer, under penalty of perjury, as to whether IPP was being compensated pursuant to an "oral contingency agreement" at the time it conducted the observations at issue in this case, and at the time it made its declaration which you used in support of your motion for early discovery. I'd like to know what were the terms of the so-called "oral contingency agreement", when it stopped, and what are the current terms of the deal with IPP.

You made it very clear that you thought any attempt to investigate this issue would be bad faith on my part, and you would make a Rule 11 motion if I file any motion of any kind since your view is my client lacks standing to do anything other than have his deposition taken. You further noted that you would not spend even one "split second" considering anything I sent you on this issue, and you threatened to make any cases we have together from here on out as unpleasant and as expensive as possible.

Respectfully, I disagree that this is bad faith or personally motivated on my part, and feel it is my duty to my client to investigate this issue, as the entire case against my client is apparently built upon compromised expert witness testimony that may very well be excluded. You can review the attached motion for the law on that issue, at least as applicable in Colorado.

Since you are correct that my client is not yet a party to this suit, what I propose is making a motion to intervene and to propound limited early written discovery inquiring into the compensation structure for IPP. I had offered that you could investigate and get back to me with something under oath saying this is all a big mistake, explaining why. You refused, and said you would vigorously contest any attempt to make any inquiry into how IPP is compensated, as you think it is irrelevant, even though I noted that inquiries and impeachment as to how experts are compensated is essentially routine, par for the course trial practice.

If you change your mind, and want to try and explain, with something under oath, why the verified discovery responses previously served by your client about the "oral contingency agreement" are incorrect, there is indeed still a chance we can resolve this short of motion practice. Note though, a declaration which says

'well, we don't do it anymore' which is how I read what your client tried to say before, is not going to be sufficient in my view.

Thus, absent a satisfactory explanation, I contemplate making a motion to be heard on this issue on an expedited time frame. It occurs to me that if IPP's potential testimony is excluded, and its contribution to the complaint is stricken, then you have no basis to take my client's deposition. As I mentioned, I am nevertheless willing to proceed with the deposition as scheduled, but in exchange I want some answers on this "oral contingency" issue to be similarly prioritized here for the first phase of pre-service discovery. If your position is that you will refuse to engage on the IPP compensation issue, I may make a motion to stay my client's deposition pending resolution of the IPP issue. Or, we can both get a round of limited discovery; you, the one hour deposition of my client; me, some answers to some limited written discovery on IPP's compensation structure. Your choice; but discovery should not be a one-way street.

I hope that after you have had a chance to calm down, and the shock of this apparent revelation subsides, that we can manage to continue to work together in a professional manner. Until today, I never had any cause to complain on that account as to our prior dealings. And despite your insistence that 'everything is personal,' I hope you can see that, at least as far as I am concerned, this really is not.

Best regards,
Morgan

--

Morgan E. Pietz
THE PIETZ LAW FIRM
3770 Highland Ave., Ste. 206
Manhattan Beach, CA 90266
mpietz@pietzlawfirm.com
Ph: (310) 424-5557
Fx: (310) 546-5301
www.pietzlawfirm.com

---

8 attachments

Exhibit A.pdf
379K

Exhibit B.pdf
366K

Exhibit C.pdf
144K

Exhibit D.pdf
161K

Exhibit E.pdf
114K

Exhibit F.pdf
39K

Kerr's Motion (Non-Comformed).pdf
1296K

Motion to Exclude FINAL.pdf
92K

Jon Hoppe <JHoppe@mhhhlawfirm.com> Mon, Mar 3, 2014 at 5:13 PM
To: "Morgan E. Pietz" <mpietz@pietzlawfirm.com>

Morgan:

Thank you for agreeing to set up a depostion of your client and get back to me about the date and tome of the same.

As to the entirely separate "issue" of the compensation of IPP, I will have a comprehensive response for you shortly. I am heatened somewhat by your suggestions that this "issue" might be resolved short of the waste of both our time and our clients' money on frivolous motions practice. I am initally disinclined to open the door to two-way preliminary discovery (particularly on the record in any case at bar) for reasons which I can briefly explain.

The preliminary discovery which my client has been granted in these matters is designed to resolve one issue only: whether the internet subscriber is the most likely actual infringer of my client's copyrighted material (and, if not, whom else might be the same). The preliminary discovery process is not designed to pre-litigate the sufficiency of the Complaint or the strength of any potential trial presentation of the same. Such "issues' are entirely premature until a John Doe defendant may be revealed, named and served. Your assertion that such discovery is "kind of unfair" could not be further from the truth. To the contrary, the preliminary discovery process set out by the Maryland Court is designed entirely to protect the identity and reputation of the internet subscriber involved and to guard against any untoward or coercive negotiation of the dispute.

Your criticism of my point of view on the nature and purpose of your raising this "issue" at this juncture of these matters is also entirely unfounded. Up until now, we have engaged in a number of matters in fruitful and professional discussion and negotiation of the real issues of whether the subscriber at issue is the actual infringer and if so, what is a fair compensation under which to settle. Your attempt now to suddenly use the prelimanary discovery process already designed to protect your client to pre-litigate the case in chief clearly poison's the well of goodwill between us. Clearly, theft of copyrighted material is going on against my client's legally compensable interest on a grand scale. Your attempt to prevent that rightful compensation through clever argument and procedural manipulation is both professionally and morally reprehensible.

As to the response you expect to receive on the "issue" you have clearly prematurely raised, and as to your view of the sufficiency thereof, I think you are once again professionally off the mark. To the contrary, I should think that even in the absence of any statement under oath, you should be professionally willing to consider reference to clear statement of legal precedent that your attack on the sufficiency or admissibility of our evidence is either entirely premature or procedurally wrongheaded. Assuming my presentation of such precedent to you, the same would be the basis of any Rule 11 Motion I might contemplate.

On the other hand, my client and/or his investigator may have or be willing to prepare an affidavit as to the nature of compensation between them and an explanation of how the same is either consistent or not with the discovery responses to which you refer. You provide no evidence of any response stating "well, we don't do that any more", so I wont respond directly to such a suggestion, except to note its disrespectfully perjorative tone. But in the event that such a document can and will be produced to you, the same would have to be presented with the strict understanding that we do not in any way concede your procedural right to the same

or any other information at this juncture of this or any other suit by my client regarding these matters. Our position remains - and must continue to be in all of these matters - that the role and function of internet subscribers and their counsel prior to the amendment of a Complaint and service of the same along with a Summons is to present themselves for deposition to determine whether such amendment and service will involve them. Under no circumstances will we consider the idea of making preliminary discovery in these cases a two-way street. It was not designed that way by the Court and for good reason.

Finally, your unsolicited and off-hand remarks regarding my state of mind are entirely out of line and unprofessional. You flatter yourself, sir, if you think you can inflict shock upon me or in any way disturb my calmness or peace of mind. And you falsely and disingenuously flatter me by asserting that I can change the objective nature of human relations by not "taking" something personally. Your final sentence raises your self-flattery to superhuman levels, asserting that your "concern" can somehow change an objective fact of human relations. Perhaps if you can somehow obtain the mystical power to change one or the other of us into something not defined as a "person" you can render interactions between us not "personal".

In conclusion, I can concur with the sentiment expressed in the next to last sentence of your e-mail. Until now, I had no cause to complain about our ability to work together in a professional manner. That was, of course, before you elected to poison the well of goodwill between us with frivolous, too-clever-by-half, procedural manipulations and attempts to prematurely begin the general litigation of this matter. I hope that such tactics on your part will cease and we will be able to return to the professional and procedurally proper resolution of these matters.

Very truly yours,

Jon A. Hoppe, Esquire
Maddox, Hoppe, Hoofnagle & Hafey, L.L.C.
1401 Mercantile Lane #105
Largo, Maryland 20774
(301) 341-2580 (ph.)
(301) 341-5727 (fax)

From: morganpietz@gmail.com on behalf of Morgan E. Pietz
Sent: Mon 3/3/2014 5:02 PM
To: Jon Hoppe
Cc: John C. Lowe
Subject: Malibu Media - D. Md. - 13-3024 - Deposition and Discovery re IPP "Oral Contingency Agreement"

[Quoted text hidden]

Morgan E. Pietz <mpietz@pietzlawfirm.com> Mon, Mar 3, 2014 at 6:16 PM
To: Jon Hoppe <JHoppe@mhhhlawfirm.com>
Cc: "John C. Lowe" <johnlowe@johnlowepc.com>

Thanks, Jon.

Please send me something under oath, which details the full history of IPP and Fieser's compensation arrangements, and explains the "oral contingency agreement" discovery response, and I will consider holding off on a motion. In terms of the kind of substantive answer which I consider insufficient, see Mr. Kotzker's email attached as Exhibit C to the motion I sent you.

Best regards,
Morgan
[Quoted text hidden]

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 1:13-cv-02394-WYD-MEH

MALIBU MEDIA, LLC,

Plaintiff,

v.

JEREMIAH BENSON,

Defendant.

DEFENDANT'S MOTION TO EXCLUDE TESTIMONY AND EVIDENCE FROM IPP INTERNATIONAL UG AND TOBIAS FEISER

Defendant, Jeremiah Benson, through undersigned counsel, hereby moves for an order excluding all testimony and evidence from IPP International UG and Tobias Feiser (collectively "IPP"). Plaintiff also respectfully requests that, Plaintiff Malibu Media disclose all past and present fee agreements between Plaintiff, its counsel and IPP. In support of the requests, Defendant states as follows:

BRIEF IN SUPPORT

Plaintiff, Malibu Media ("Malibu") is a prolific copyright litigant. In the last three years alone, Malibu has filed approximately 1773 copyright lawsuits nationwide, with 308 of those suits being filed in this Court alone. In every instance, these lawsuits are supported by evidence provided by the German firm IPP. (*See e.g.* Amended Complaint ¶¶ 16-17, 19-20; Exhibits A-B; Docket. No. 16; *see also* Affidavit of Tobias Feiser in support of Motion for Leave to Take Early Discovery; Dck. No. 7 Exhibit D.) However, what has not disclosed to this, or any other Court is that IPP is a financially interested party. Specifically, in each of the above referenced cases IPP supplied evidence to Malibu pursuant to an "oral contingency agreement" with its national counsel

Keith Lipscomb, of the Miami based law firm Lipscomb, Eisenberg & Baker, P.L. IPP's actions as a contingent-fee witness are contrary to common law principles, public policy, the ABA Model and Colorado Rules of Professional Conduct as well as the Federal Anti-Gratuity Statute. For these reasons, IPP should not be allowed to offer evidence or testimony in this case. In addition, Malibu should be ordered to disclose to the Defendant, this Court, and any other court in which it has filed a lawsuit using evidence provided by IPP, all past and present fee agreements between Plaintiffs, its counsel and IPP for review and other appropriate judicial action.

FACTUAL BACKGROUND

IPP is a German based company that provides services that involve the "track[ing] and monitor[ing of] illegal propagators within [BitTorrent] networks."[1] Malibu's lawsuits are supported by evidence provided by IPP, and in particular IPP employee Tobias Feiser. (*See e.g.* Amended Complaint ¶¶ 16-17, 19-20; Exhibits A-B; *see also* Affidavit of Tobias Feiser in support of Motion for Leave to Take Early Discovery; Dck. No. 7 Exhibit D.) In an identical copyright infringement case in a separate jurisdiction Malibu, certified under penalty of perjury that IPP is paid only based on a contingent of settlement proceeds. Specifically, Malibu admitted the following:

> **Interrogatory No. 1**: Please identify all . . . business entities that have an interest, financially, or otherwise, in this litigation, including, . . . forensic consultants, and/or witnesses, . .. and specifically and in detail describe the nature of the interest.
>
> **Response to Interrogatory No. 1**: . . . IPP International UG, is a fact witness who will testify that its technology detected that a person using Defendant's IP address was downloading and distributing Plaintiff's copyrighted works. **Pursuant to an oral contingency fee agreement, IPP International UG is entitled to a small portion of the proceeds from the resolution of this case in consideration for the services it provides.**

[1] *See* www.ippint.de/index.php?option=com_content&view=article&id=3&Itemid=3 (accessed Jan. 29, 2014).

(*See* Exhibit A – Verified Response No. 1). In response to an Interrogatory in another identical federal lawsuit, Malibu admitted that "[it] and IPP International UG have an oral agreement that was formed approximately 2.5 years ago "negotiated the terms of [Malibu]'s agreement with IPP." (Exhibit B – Verified Response No's. 4-5). Again, Malibu admitted that that its national counsel M. Keith Lipscomb, of the Miami based law firm Lipscomb, Eisenberg & Baker, P.L "negotiated the terms of Plaintiff's agreement with IPP International UG" and that IPP is "entitled to a small portion of the proceeds from the resolution of this case in consideration for the services it provided." *Id*. Finally, Malibu has repeatedly identified in court filings that IPP is "a fact witness who will testify that its technology detected that a person using Defendant's IP address was downloading and distributing Plaintiff's copyrighted works."[2] (*See* Exhibit A – Verified Response No. 1).

In response to this information, Defendant's counsel sought clarification from Malibu's local counsel as to the Malibu's fee agreement with IPP. (Exhibit C) Malibu's response however was completely contrary to the above referenced statements provided under penalty of perjury by Malibu's representative Colette Field, and submitted by its counsel pursuant to F.R.C.P. 11. *Id*. Defendant's counsel sought additional assurances, such as a simple declaration from Mrs. Field for example, or even Mr. Lipscomb. *Id*. Malibu never responded to this request. More telling perhaps is the fact that despite being ordered by the Honorable Geraldine S. Brown of the U.S. District Court for the Northern District of Illinois to disclose the nature and terms of this "oral

[2] The reference to IPP's "technology" would indicate that it is not as much a fact witness as an expert witness. However, it is likely that such designation was applied to IPP so as to avoid the need for drafting an expert report under Fed. R. Civ. P. 26.

contingency agreement," Malibu has steadfastly refused and now stands under the threat of a motion for show cause why it should not be held in contempt. (See Exhibit D).

LEGAL ARGUMENT

I. ALL EVIDENCE FROM IPP SHOULD BE EXCLUDED

a. CONTINGENCY BASED COMPENSATION OF WITNESSES IS CONTRARY TO COMMON LAW PRINCIPLES, PUBLIC POLICY AND SUBJECT TO EXCLUSION

Relying on the common law and the court's authority to forestall violations of ethical principles, many jurisdictions have held that testimony of witnesses whose compensation is contingent upon the outcome of the case must be excluded. See, e.g., *United States v. Singleton*, 144 F.3d 1343, 1347 (10th Cir. 1998) (contracts to pay fact witnesses are void as violative of public policy), vacated on other grounds, 165 F.3d 1297 (10th Cir.), cert. denied, 119 S. Ct. 2371 (1999); *see also, Hamilton v. General Motors Corp.*, 490 F.2d 223, 228-229 (7th Cir. 1973) (holding that paying fact witnesses for testimony is against public policy and refusing to allow payment for testimony); *Followwill v. Merit Energy Co*., 2005 WL 5988695, at *1 (D. Wyo. Apr. 11, 2005) (granting defendants' motion to exclude plaintiffs' expert witness and strike his expert report because the witness was paid on a contingency basis).[3]

[3] *See also Straughter v. Raymond*, 2011 U.S. Dist. LEXIS 53195, at *9-10 (C.D. Cal. May 9, 2011) (excluding expert witness compensated pursuant to a contingency fee); *see also e.g. Caldwell v. Cablevision Sys. Corp*., 984 N.E.2d 909, 912, 960 N.Y.S.2d 711 (N.Y. 2013) ("What is not permitted and, in fact, is against public policy, is any agreement to pay a fact witness in exchange for favorable testimony, where such payment is contingent upon the success of a party to the litigation."); *Westin Tucson Hotel Co. v. State*, 936 P.2d 183, 190 (Ariz. App. 1997)("…a contract providing for compensation of a witness contingent on the success of the litigation is subversive of public justice for the reason that his evidence may be improperly influenced. Public policy considerations brand such a contract illegal."), *In re Schapiro*, 128 N.Y.S. 852, 858 (N.Y. App. Div. 1911) ("A witness who . . . receives compensation or a promise of compensation for giving his testimony is necessarily a discredited witness."); *Reffett v. C. I. R*., 39 T.C. 869, 878 (1963) ("[I]t seems to be a rather generally accepted rule that all agreements to pay witnesses extra compensation contingent on the success of the lawsuit are against public policy whether the agreement is with an ordinary witness, an expert witness, or a witness who cannot be compelled to testify, because such agreements constitute a direct temptation to commit perjury."). *Ouimet v. USAA Casualty Ins. Co*., 2004 U.S. Dist. LEXIS 31199, 2004 WL 5865274, at *2 (C.D. Cal. Jul. 14, 2004) (excluding expert's testimony, in part, because it "would run directly afoul of [Rule 5-310 of the California Rules of Professional Conduct], as her compensation under the contingency fee agreement depends upon the outcome of the case."); *Farmer v. Ramsay*, 159 F. Supp. 2d 873, 883 (D. Md. 2001) (granting motion to strike reports of expert retained under contingency fee arrangement), aff'd on other grounds, 43 Fed. App'x 547 (4th Cir. 2002); *Cosgrove v. Sears Roebuck & Co*., 1987 U.S. Dist. LEXIS 11696, 1987 WL 33595,

On the face of its discovery responses, Malibu admits under penalty of perjury that IPP is being paid on a contingent basis. (*See* Ex's A and B). IPP will make money only if this case is resolved positively for Malibu. Further, the amount of money IPP will make is contingent on the proceeds received in settlement or collected in judgment. Such an arrangement is contrary to public policy and common law principles that hold such agreements void on their face and an affront to the integrity of the judicial system by turning third parties into both a witness and a "de facto" financially interested Plaintiff. *See e.g*. *Commonwealth v. Miranda*, 458 Mass. 100, 934 N.E.2d 222, 229 n.15 (Mass. 2010) ("[c]ompensation to fact witnesses is said to violate the integrity of the judicial system, to undermine the proper administration of justice, and to be contrary to a witness's solemn and fundamental duty to tell the truth."). While the common law torts of maintenance no longer exist in Colorado, *Fastenau v. Engel*, 125 Colo. 119, 122 (Colo. 1952), such quasi barratrous and/or champertous financial arrangement should not be endorsed by this Court and evidence from IPP should be stricken from the record and excluded going forward.

b. CONTINGENCY BASED COMPENSATION OF WITNESSES VIOLATES THE RULES OF PROFESSIONAL CONDUCT

While an issue of apparent first impression in this District, some trial courts have precluded improperly paid witnesses because their payment violates ethical rules. See, e.g., G*olden Door Jewelry Creations, Inc. v. Lloyds Underwriters Non-Marine Ass'n*, 865 F. Supp. 1516, 1526 (S.D. Fla. 1994) (excluding fact witness as a sanction where lawyer "violated the very heart of the integrity of the justice system"). Moreover, model and state based ethical rules have long

at *1-2 (S.D.N.Y. Dec. 21, 1987) (precluding testimony of expert witness paid on contingency fee basis, but allowing party sixty days to designate new expert witness); *In re SMTC Mfg*., 421 B.R. 251, 264 n.2 (W.D. Tex. Bankr. 2009) (noting prior dismissal of expert witness retained under contingency fee arrangement); *cf. Accrued Fin. Servs., Inc. v. Prime Retail, Inc*., 298 F.3d 291, 300 (4th Cir. 2002) (holding that to the extent that employees of financial auditing company planned to testify as experts, company was improperly offering expert testimony for contingent fee in violation of public policy).

EXHIBIT Y

Morgan Pietz <morganpietz@gmail.com>

Malibu Media v. Doe 8:13-cv-3024; MD109

Jon Hoppe <JHoppe@mhhhlawfirm.com> Thu, Mar 6, 2014 at 8:28 PM
To: morganpietz@gmail.com

Morgan,

Our investigation on this case has revealed that your client may be living with roommates who could be responsible for the infringement. This is why we intended to schedule the deposition. The same might very well have led to the need to move for leave to depose one or more of your client's roommates. Unfortunately, looking at the calendar for this case, our client is up against its second Rule 4(m) deadline to serve the Summons and Complaint. From my experience, Maryland judges have not always been amenable to multiple extensions of the Rule 4(m) deadline. And in this case, I can't see us agreeing on a protective order for my client (who will not hand over confidential information about its contracts without one), providing you declarations, contracts, and other information, and getting through the depositions in any sort of timely fashion that would allow us to proceed and serve reasonably quickly.

For that reason, instead of continuing on and accruing more attorney's fees on this case only for it to be dismissed for failure to serve in time, my client has dismissed the case. Please be aware that in the future, my client plans on resolving these issues with you and your clients in a timely fashion and will proceed. Unfortunately in this case the timing was against us.

Very truly yours,

Jon A. Hoppe, Esquire
Maddox, Hoppe, Hoofnagle & Hafey, L.L.C.
1401 Mercantile Lane #105
Largo, Maryland 20774
(301) 341-2580 (ph.)
(301) 341-5727 (fax)

EXHIBIT Z

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. 1:13-cv-02394-WYD-MEH

MALIBU MEDIA, LLC,

Plaintiff,

v.

JEREMIAH BENSON,

Defendant.
_____/

PLAINTIFF'S MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO EXCLUDE TESTIMONY AND EVIDENCE FROM IPP INTERNATIONAL UG AND TOBIAS FEISER [CM/ECF23]

I. INTRODUCTION

Defendant's Motion to Exclude Testimony and Evidence from IPP international UG and Tobias Fieser (CM/ECF 27) ("the Motion") correctly asserts that Malibu Media, LLC ("Malibu") paid IPP International UG ("IPP"), for its data collection services. From these facts, Defendant erroneously argues that the physical evidence obtained by IPP is inadmissible and that IPP's employee should be precluded from testifying. While not titled as such, it is a Motion *in Limine* seeking to exclude relevant evidence and testimony. Paying a service provider to record a computer is not a basis under the Federal Rules of Evidence to exclude relevant evidence and testimony.

II. FACTUAL BACKGROUND

A. The Data Evidencing The Infringement Is *Not* Capable of Being Manipulated By Humans

Defendant's entire argument is premised on the possibility of witness bias based upon Malibu's payment for IPP's services. As explained below, the evidence that Malibu uses for purposes of proving infringement occurred is *recorded* in such way that it is *not* capable of being manipulated or altered. Humans play no part in the creation or storage of the evidence. Significantly, the evidence can be independently verified by anyone – including Defendant. Indeed, in preparation of this response, Plaintiff independently verified that the evidence is correct. Consequently, there is no possibility of biased testimony. The fact section explains why this paragraph is true.

1. A Very Short Explanation of How BitTorrent Works

To understand the evidence upon which Plaintiff relies, there are two important things to address about the way BitTorrent works: (a) peers in a BitTorrent swarm connect to each other's computers in order to transmit "pieces" of a computer file (here, the computer files transmitted

contain copies of Plaintiff's works); and (b) every "piece" of the computer file – and the entire computer file – being transmitted via BitTorrent has its own *unique* hash value. Hash values are digital fingerprints for pieces of data.[1] Hash values are more reliable than DNA evidence. *See* FN1. A hash value is calculated. Regardless of who calculates the hash value of any certain piece of data, the hash value for that certain piece of data will always be the same.[2]

2. A 10,000 Foot Overview of the Data Collection System Used By IPP

The data collection system used by IPP has numerous components. It contains, *inter alia*: (1) a proprietary BitTorrent Client[3]; (2) servers running a MySQL database which log verified infringing transactions; (3) packet analyzers, also known as packet sniffers, which create and analyze PCAPs; (4) servers that run the proprietary BitTorrent Client and record PCAPs; (5) WORM ("Write Once Read Many") tape drives for storing the PCAPs and MySQL server data; (6) a program to synchronize the servers' clocks with both a GPS clock and an atom clock[4]; (7) a proprietary program for checking the MySQL log files against the contents of the PCAPs; and (8) a proprietary program which checks the information contained in an Excel Spreadsheet

[1] See Exhibit A, citing numerous district and appellate court decisions describing hash values and finding that they are reliable unique identifiers for data akin to digital fingerprints.
[2] *See* Composite Exhibit B, which is an article explaining that hash values can be calculated and websites advertising commercially available free hash calculators.
[3] In other words, a software program that enables the BitTorrent protocol to work. The BitTorrent Client used by Excipio is not commercially available and its code is a trade secret. Patzer, at ¶ 6. It was written to overcome the unique challenges of entering into a massive number of BitTorrent transactions with a massive number of people without distributing data. *Id.*, at ¶ 7.
[4] If the servers are not synchronized with both the GPS clock and atom clock to within one hundredth of a second the infringing transaction is not logged but instead disregarded. Patzer, at ¶ 8.
[5] *See* Exhibit D, Wikipedia Article on "Internet Protocol," at paragraph 2.
[6] *See* Exhibit E, Wikipedia Article on "PCAP."
[7] *See* Exhibit F, Wikipedia Article on "Packet Analyzer."

In other words, a software program that enables the BitTorrent protocol to work. The BitTorrent Client used by Excipio is not commercially available and its code is a trade secret. Patzer, at ¶ 6. It was written to overcome the unique challenges of entering into a massive number of BitTorrent transactions with a massive number of people without distributing data. *Id.*, at ¶ 7.
If the servers are not synchronized with both the GPS clock and atom clock to within one hundredth of a second the infringing transaction is not logged but instead disregarded. Patzer, at ¶ 8.

against what is in the PCAPs and server's log files. *See* Patzer Declaration, at ¶ 5, Exhibit K; and Exhibit C, Mr. Fieser's testimony during the Bellwether Trial transcript at p. 100.

3. The Evidence Produced By the Data Collection System Is Independently Verifiable

The *evidence* that the data collection system produces is comprised of PCAP computer files and MySQL server log files. Each entry on the MySQL log file correlates to a specific PCAP file. Patzer, at ¶ 9.

a. PCAP Computer Files Are Independently Variable

Data sent through the internet is delivered in the form of "packets" of information.[5] PCAP stands for "Packet Capture." A PCAP is a computer file containing captured or recorded data being transmitted between two computers.[6] A "Packet Analyzer" records packets of data being transmitted between two computers over a network, such as the internet, and saves it in a computer file called a PCAP.[7] Packet analyzers also enable users to read and analyze PCAPs. IPP's data collection system uses a proprietary packet analyzer *and* TCPDump to record the *entire* infringing transaction. TCPDump is an open source free packet analyzer.[8]

(i) Anyone Who Downloads TCPDump – For Free – Can Review and Verify the Infringing Transaction

Anyone who downloads TCPDump – for free – can review and verify the entire transmission of a piece of Malibu's copyrighted work from Defendant's IP address. The proof of infringement is a PCAP *recording* of Defendant's IP Address *sending* a piece of the copyrighted work to the MySQL server. The PCAP recording speaks for itself. Testimony

[5] *See* Exhibit D, Wikipedia Article on "Internet Protocol," at paragraph 2.
[6] *See* Exhibit E, Wikipedia Article on "PCAP."
[7] *See* Exhibit F, Wikipedia Article on "Packet Analyzer."
[8] http://www.tcpdump.org/#

about what is contained in the PCAP can be elicited at trial by either IPP's employee, Mr. Fieser, Malibu's computer forensic expert Mr. Patrick Paige, Excipio's independent contractor, Mr. Michael Patzer, or via a demonstration during trial by any other witness. The demonstration would merely require the witness to install TCPDump so that he or she could read and analyze the PCAP. Here, in preparation of its response to this motion, Plaintiff's attorneys asked Michael Patzer, an individual who does not work for IPP, to examine the evidence, without compensation. Mr. Patzer independently reviewed the PCAPs in this case and confirmed that the PCAPS recorded Defendant's IP address infringing Plaintiff's copyrighted works at the exact Hit Dates and UTC times listed on Exhibit A to Plaintiff's Complaint. Patzer, at ¶ 13.

b. Every Entry Onto the MySQL Server Log File Correlates To a PCAP

Defendant sent the investigative server numerous "pieces" of each one of the computer files that contain a copy of Malibu's works. Accordingly, TCPDump recorded numerous BitTorrent transactions for each infringing computer file. *See* Exhibit G. Each one of these transactions was logged in a MySQL log file *and* fully recorded as a PCAP. Significantly, every entry on the MySQL server log file correlates to a specific PCAP. Patzer, at ¶ 9. Both the MySQL log file and the PCAP are computer records.

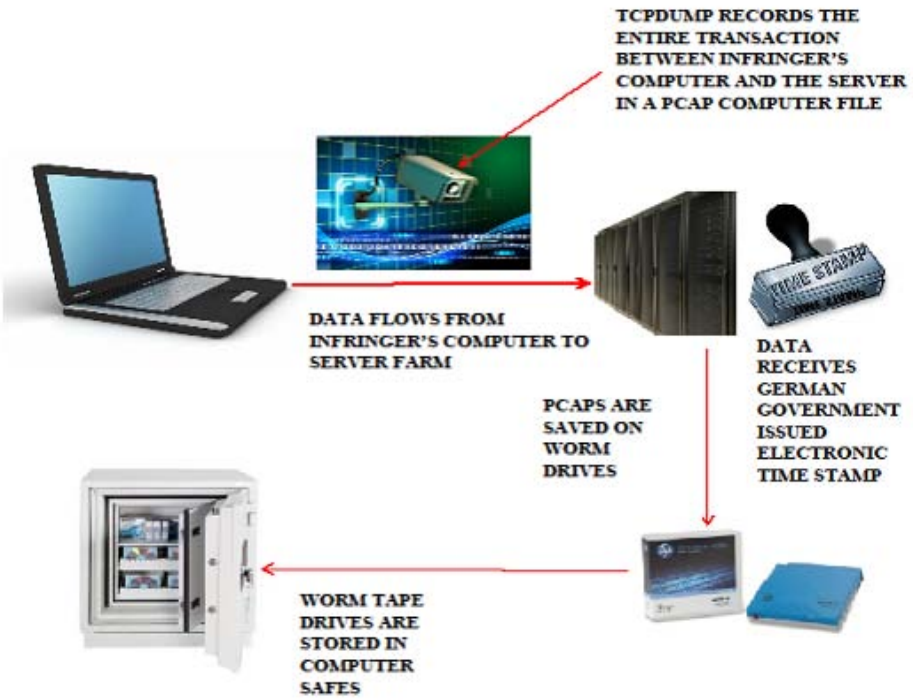
4. The PCAP and Log Files Are Saved on an Uneditable WORM ("Write Once Read Many") Tape Drive

"Write once read many (WORM) describes a data storage device in which information, once written, cannot be modified. This write protection affords the assurance that the data cannot be tampered with once it is written to the device."[9] Both the PCAPs and log files are saved onto WORM tape drives. Patzer, at ¶ 10. There is no possibility that the information on these WORM drives can be edited. *Id.,* at ¶ 11. Further, each of the WORM tape drives is

[9] *See* Exhibit H, Wikipedia article entitled "Write once read many."

electronically stamped with a German government issued time stamp at least every twenty four hours. *Id.,* at ¶ 12.

PCAP CREATION AND STORAGE FLOW-CHART



B. A Short Summary of Mr. Fieser's Possible Testimony

Mr. Fieser is the only employee of IPP who *may* testify. His testimony is unnecessary. Therefore, Malibu will *not* likely call Mr. Fieser. What follows is a short summary of what Mr. Fieser would say if Malibu calls him.

Tobias Fieser is a salaried employee of IPP. Fieser Declaration, at ¶ 4, Exhibit L. He does not have an ownership interest in IPP nor any other entity involved in or affiliated with IPP's data collection system. *Id.*, at ¶ 6. Mr. Fieser is not being paid for his testimony and does not have the right to receive any portion of a settlement or judgment in Plaintiff's favor.[10] *Id.,* at ¶ 7.

Mr. Fieser has three primary functions at IPP: (1) verify that the BitTorrent computer files as evidenced by their unique hash values are copies of the original works; (2) extract the MySQL server data and make it available to IPP's clients, here Malibu's counsel; and (3) upload a declaration prepared by IPP's clients' counsel (in this case Malibu's attorney) into a computer program and sign a declaration if a green light appears.[11] *See* Exhibit C, Mr. Fieser's testimony during the Bellwether Trial transcript at pp. 92, 100. The computer program verifies the attested to infringement data is contained in the servers' MySQL log files. This ensures it has not been altered by counsel during the suit formation process. *Id.*

1. Mr. Fieser Does Not Need to Testify That the Computer Files Transmitted Via BitTorrent Are Copies Because Anyone Can Do That

[10] Malibu would reimburse IPP for Mr. Fieser's travel and lodging costs and pay IPP a reasonable flat daily rate fee for Mr. Fieser's time away from work.

[11] Each month approximately 80,000 U.S. citizens infringe Malibu's copyrighted works. Malibu's counsel culls through this infringement data received by IPP and sues 100-150 of the worst-of-the-worst infringers. To identify potential defendants, Malibu's counsel analyzes various things such as length of infringement, number of infringed works, and evidence of third party infringements the content of which can be used to identify a specific person. After using IPP's infringement data counsel sends it back as formatted declarations.

Mr. Fieser does not need to testify that the computer files transmitted via BitTorrent are copies of Malibu's movies. To explain, the computer files have *unique* cryptographic hash values and are playable movie files. Accordingly, anyone can watch the BitTorrent computer file copy and compare it to the original for purposes of ascertaining whether it is a copy. For this reason, in all other recent matters around the country which have approached trial, opposing counsel has stipulated that the computer files contain copies. If opposing counsel will not so stipulate then Malibu will ask this Court to take judicial notice. Judicial notice is appropriate under rule Fed. R. Evid. 201(b) because it is "a fact that is not subject to reasonable dispute [and] . . . can be accurately and readily determined from sources whose accuracy cannot reasonably be questioned." A stipulation or judicial notice is particularly appropriate because the movies contain adult content. Consequently, it may be uncomfortable or distracting for jurors to watch them. Nevertheless, in the absence of a stipulation or judicial notice, Malibu could have Patrick Paige, its expert witness, Plaintiff's principle, or Mr. Patzer calculate the hash values of the subject computer files at or before trial and play the copy and original in a split screen. This proves A is a copy of B.

2. Mr. Fieser is Not the Witness Malibu Will Call to Authenticate the Infringement Data at Trial or to Lay the Foundation For its Introduction

At trial, Malibu will call Mr. Patzer to testify that the PCAPs and MySQL log files contain evidence that proves that an infringement was committed by a person using Defendant's IP Address. Malibu will not use Mr. Fieser for this purpose because he will not be able to establish the chain of custody to the PCAP. To explain, Mr. Patzer, not Mr. Fieser, restores the PCAPs saved onto the WORM tape drives and makes forensically sound copies of them for use at trial. Thus, only Mr. Patzer can testify to the chain of custody.

C. A Very Short Explanation of Michael Patzer's Anticipated Testimony

Michael Patzer works as an independent contractor predominantly for Excipio GmbH, a German company. Patzer, at ¶ 2. Excipio contracts with IPP to provide IPP with the data collection system that IPP uses to detect infringement of Malibu's works.[12] *Id.*, at ¶ 4. Mr. Patzer designed, implemented, maintains and monitors the data collection system that Excipio both owns and uses to identify the IP addresses used by people to commit copyright infringement via the BitTorrent protocol. *Id.*, at ¶ 3. *See also* Exhibit I, Mr. Patzer's testimony during the Bellwether Trial transcript at p. 54. No one at Excipio has an ownership in IPP or vice versa. *Id.*, at ¶ 14. Mr. Patzer does not have an ownership interest in Excipio. *Id.,* at ¶ 15. He is not paid for his testimony and is not entitled to any portion of any money received from a settlement or judgment in Malibu's favor.[13] *Id.,* at ¶ 16. Malibu has never paid Excipio or Mr. Patzer anything. *Id.,* at ¶ 16.

Mr. Patzer will answer all of the questions necessary to lay the foundation for the introduction into evidence of the PCAP and MySQL log files as business records within the meaning of Fed. R. Evid. 803(6). Further, he will answer all of the questions necessary to authenticate the PCAP and MySQL log files pursuant to Fed. R. Evid. 901(a). Finally, Mr. Patzer will testify that the PCAPs are recordings of computer transactions during which a person using IP Address 76.25.62.43 sent pieces of the infringing computer files to the servers that he personally maintains and monitors.

[12] IPP used to maintain and operate and use its own system. At some time unknown to Malibu, but well in advance of any of the infringement that was logged in this case, IPP entered into a license agreement with Excipio to use its system. The two companies now both compete with each other and are licensor-licensee. Under this arrangement, IPP licenses the use of Excipio's system and servers. Patzer, at ¶ 3. IPP adds value and distinguishes itself by, *inter alia*, customer specific analysis tools and its client service.

[13] Malibu does intend to reimburse Excipio for Mr. Patzer's travel and lodging cost and pay a reasonable flat daily rate fee for Mr. Patzer's time away from work.

D. Patrick Paige Tested the Data Collection System

Malibu's computer forensic expert, Patrick Paige, tested the data collection system. His report is attached as Exhibit J. His test involved seeding public domain movies, i.e. movies that are not protected by copyright. *See* Exhibit J. He gave IPP the titles of the works. *Id.* IPP, using Excipio's system, found the works and entered into BitTorrent transactions with Mr. Paige's test servers. *Id.* Mr. Paige used a packet analyzer on his test servers to record all of the transactions in PCAPs. *Id.* He compared the PCAPs he recorded during the transactions with the PCAPs that were recorded by IPP using Excipio's system. *Id.* They matched perfectly. *Id.* This could not happen unless Excipio's system accurately created PCAPs of transactions. *Id.*

E. Judge Baylson Found the Data Collection System Was Valid

Judge Baylson presided over the Bellwether trial wherein Malibu was the first ever Plaintiff to try a BitTorrent copyright infringement case. At the trial, Judge Baylson had an independent court appointed computer expert in attendance. After the trial, Judge Baylson found that IPP's data collection system "is valid." *See Malibu Media, LLC v. John Does 1, 6, 13, 14*, 950 F. Supp. 2d 779, 782 (E.D. Pa. 2013) ("Malibu [] expended considerable effort and expense to determine the IP addresses of the infringing parties, and the technology employed by its consultants . . . was valid.")

F. Defendant Can Retain An Expert to Test the Data Collection System

Defendant has the right to hire an expert to test the data collection system. Defendant has chosen instead to attack the data collection system based upon unfounded speculation about the potential for biased testimony. Defendant's attack does not specify how the system may be flawed or how testimony that merely reads computer records can be biased. This is no surprise because there is no possibility for biased testimony.

G. Malibu and IPP Have a Written Fixed Fee Agreement

Malibu and IPP have a written fixed fee agreement pursuant to which Malibu pays IPP for providing the service of collecting data about infringements. Field, at ¶ 8. IPP has not been paid anything for this case. Fieser, at ¶ 10. Malibu's prior oral agreement with IPP to pay IPP a small portion of the amount received from a settlement or judgment from Malibu's litigation does not apply to this case. Field, at ¶ 7. Malibu has never paid *any* fact witness to testify in this case or any other case. *Id.*, at ¶ 9.[14]

III. ARGUMENT

A. Malibu is Permitted to Pay For Data Collection Services

Malibu has not paid nor offered to pay any individual for testimony. The fee Malibu pays IPP is for data collection services. Paying IPP for data collection services is neither unethical nor prohibited by law. "[P]arties are free to pay individuals, including fact witnesses, for providing information and assisting with litigation, so long as the payment is not for their testimony." *Armenian Assembly of Am., Inc. v. Cafesjian*, 924 F. Supp. 2d 183, 194 (D.D.C. 2013). "[T]his Court is unaware of any authority that interprets Rule 4-3.4(b) as barring counsel from compensating someone for their efforts in collecting evidence." *Platypus Wear, Inc. v. Horizonte Fabricacao Distribuicao Importacao Exportacao Ltda*, 2010 WL 625356 (S.D. Fla. 2010). "[T]he court concludes that [defendant] and its counsel paid [the witness] only for time spent in connection with the litigation process." *Centennial Mgmt. Servs., Inc. v. Axa Re Vie*, 193 F.R.D. 671, 679 (D. Kan. 2000). "Anyone has a right, when threatened with litigation, or desiring himself to sue, to employ assistance with a view of ascertaining facts as they exist, and to hunt up and procure the presence of witnesses who know of facts and will testify to them." *Hare v. McGue*, 178 Cal. 740, 742, 174 P. 663, 664 (1918). At significant expense, IPP provides

[14] Malibu pays Mr. Paige, an expert, an hourly rate to prepare for and appear at legal proceedings.

Malibu with labor and a data collection service. Malibu Media is permitted to pay IPP for its service.

B. No Witness Has Ever Been Paid For Testimony Much Less on a Contingent Basis

Defendant erroneously conflates Malibu's proper payment to IPP for its data collection services with the false allegation that Malibu paid Tobias Fieser for testimony. Mr. Fieser is a salaried non-equity owning employee of IPP. Fieser, at ¶¶ 4, 7. Malibu has never paid nor offered to pay Mr. Fieser anything. *Id.*, at ¶ 11. When, as here, "[i]t is clear that the [individual] himself, as a witness, is not eligible to receive compensation for his testimony . . . [the] case does not even involve the payment of a fee to a witness." *People v. McNeill*, 316 Ill. App. 3d 304, 306, 736 N.E.2d 703, 705 (Ill. App. Ct. 2000). In *McNeil,* the witness's employer's compensation was contingent on the outcome of the case. Like here, however, the witness was not paid for his testimony. The *McNeil* Court refused to exclude the witness and opined that the defendant could always attempt to impeach the witness's credibility on the basis that his employer had a contingent interest in the case.

C. Even if Malibu Had Paid a Witness on a Contingency That Witness's Testimony Should Not be Excluded

"The *per se* exclusion of whole categories of evidence is disfavored by the Federal Rules of Evidence. It is a fundamental tenet of those rules that, with few exceptions, 'all relevant evidence is admissible,' Fed. R. Evid. 402, and 'every person is competent to be a witness,' Fed. R. Evid. 601." *U.S. v. Cervantes-Pacheco*, 826 F.2d 310, 315 (5th Cir. 1987) (refusing to prevent the federal government's confidential informant from testifying even though the federal government had offered the confidential informant *contingent* compensation for his testimony.) Notably absent from Fed. R. Evid. 402 and 601 is that a witness be disinterested or uncompensated in order to be permitted to testify.

Consistent with the foregoing, "the 'assumption that interested witnesses necessarily lie or that disqualification is the best way to deal with the threat of perjury' has been rejected." *Just In Case Bus. Lighthouse, LLC v. Murray*, 2013 COA 112, (Colo. App. 2013) citing 27 Charles A. Wright & Victor J. Gold, *Federal Practice & Procedure* § 6005, at 69 (2007). The court in *Just in Case Bus. Lighthouse* also noted that "under CRE 601, per se exclusion of testimony is disfavored", "the potentially corrupting effect of contingent compensation implicates credibility, but does not involve competency" and "questions relating to the credibility of a witness and the weight to be accorded the testimony of a witness are matters to be resolved solely by the jury". *Id*. at *4-*5.

Here, there has been no bad faith by Plaintiff or Plaintiff's counsel. Defendant's motion relies on incidents that happened outside this case. Further, Plaintiff's counsel has informed undersigned that all of the discovery regarding this issue was provided to opposing counsel in the case in the Northern District of Illinois before the Honorable Judge Brown. *See* CM/EF 23 at *3. Finally, even if Plaintiff's agreement with IPP was improper, *which it is not*, it does not violate Colorado Rule of Professional Conduct 3.4(b) because undersigned did not negotiate the agreement and IPP has not been paid anything for this case.

D. Malibu Did Not Violate the Federal Anti-Gratuity Statute But Even if it Had That Would Not Be a Basis For Excluding Evidence or Testimony

Defendant's assertion that Malibu violated 18 U.S.C. § 201(c)(2) – which prohibits knowingly paying a person to testify – is baseless. First, Plaintiff has an agreement to pay IPP for its data collection efforts. It does not pay Mr. Fieser nor does it pay IPP for Mr. Fieser's testimony. *Centennial Mgmt. Servs., Inc. v. Axa Re Vie*, 193 F.R.D. 671, 681 (D. Kan. 2000) ("the court has concluded, based on the evidence before it, that neither [defendant] nor its counsel paid money to [witness] 'for' or 'because of' his testimony. Accordingly, the court must

conclude that no violation of section 201(c)(2) occurred." Second, Mr. Fieser's testimony is truthful. Therefore, 18 U.S.C. § 201(c)(2) does not apply. *Golden Door Jewelry Creations, Inc. v. Lloyds Underwriters Non-Marine Ass'n*, 865 F. Supp. 1516, 1524 (S.D. Fla. 1994) ("Because there is no evidence in the record that the testimony elicited through [Defendant's] monetary inducements was false testimony, the Court concludes that the evidence does not support a violation of § 201(c)(2).")

Third, and most significantly here, 18 U.S.C. § 201 is a criminal statute *not* an evidentiary rule of exclusion. Indeed, even if testimony is proffered which violates 18 U.S.C. § 201(c)(2) the testimony should not be excluded under Fed. R. Evid. 403 or any other rule because "exclusion confers windfalls on the guilty," and "a jury should be competent to discount appropriately testimony given under a powerful inducement to lie." *United States v. Dawson*, 425 F.3d 389, 394 (7th Cir. 2005).

E. Malibu's Motion for Leave Did Not Violate Colorado Rule of Professional Conduct 3.3(d)

Defendant erroneously argues that undersigned violated the Colorado Rules of Professional Conduct because "Malibu plainly knew that its fee arrangement with IPP could subject the evidence to exclusion, or at a minimum increased scrutiny into its credibility." CM/ECF 23, at p. 11. Defendant further states that "Malibu failed to disclose that IPP was and is being illegally and/or unethically compensated. Even if such testimony were not excluded out of hand, this Court should have at least had the opportunity to judge the credibility and weight of the evidence prior to its grant of early discovery." *Id.*

"The object of an ex parte proceeding is [] to yield a substantially just result." Colo RPC 3.3 (2012), at Comment 14. This is accomplished by an attorney's duty to "make disclosures of material facts known to the lawyer and that the lawyer reasonably believes are necessary to an

informed decision." *Id.* Here, the Court's only decision with regard to Plaintiff's ex parte motion, was limited to whether or not Plaintiff had demonstrated that "good cause" existed for it to serve early discovery on Defendant's ISP to uncover Defendant's identity. The good cause standard examines: (1) whether the plaintiff made a prima facie showing of a claim of copyright infringement, (2) whether the plaintiff submitted a specific discovery request, (3) whether there is an absence of alternative means to obtain the subpoenaed information, (4) whether there is a central need for the subpoenaed information, and (5) the defendant's expectation of privacy. *See* CM/ECF 7-1, at p. 4. Significantly, this Court found that Plaintiff satisfied the above factors. *See* CM/ECF 10, at p. 2 ("After review of the motion, the Court finds that Plaintiff establishes good cause for limited expedited discovery.") The weight and credibility of the evidence that Plaintiff may use to prove its case is not relevant to the good cause standard. To the contrary, this Court and numerous others have previously examined many similar motions by this Plaintiff and none has ever found it necessary or appropriate to examine the evidence or its credibility prior to allowing early discovery.[15] Regardless, as explained herein, Plaintiff's evidence is sound and immune to bias because of the numerous steps and safeguards involved.

No unjust result came about from Plaintiff's ex parte motion. Defendant has not argued to the contrary. The only result was that Plaintiff was allowed to serve its subpoena on Defendant's ISP. Defendant's interests were adequately protected by his ability to move to

[15] In a similar BitTorrent copyright infringement case brought by this Plaintiff in the Western District of Michigan a defendant attempted to assert a similar argument under Michigan Rule of Professional Conduct 3.3(d), which is identical to the Colorado Rule. There the defendant included three pages of "disclosures" which he believed Plaintiff should have disclosed to the court in its ex parte motion for early discovery. Similar to here, many of the "disclosures" related to Plaintiff's evidence and ability to prove its case. Rejecting the defendant's argument, the court held that it was "unconvinced that omission of those statements violated Rule 3.3(d). The Court has previously scrutinized Plaintiff's subpoena request and determined that Plaintiff has established 'good cause' . . . with 'good cause' shown, such a process is necessary for a copyright holder to protect its copyright when BitTorrent protocol is the alleged method of infringement." *Malibu Media, LLC v. Doe*, 1:13-cv-00893-RJJ, CM/ECF 15, at p. 2 (W.D. Mich. October 28, 2013).

DECLARATION OF PATRICK PAIGE

I, PATRICK PAIGE, DO HEREBY DECLARE:

1. I am over the age of eighteen (18) and otherwise competent to make this declaration. The facts stated in this declaration are based upon my personal knowledge.

2. I was a police officer from 1989 until 2011 for the Palm Beach County Sherriff's Department. And, from 2000-2011, I was a detective in the computer crimes unit.

3. As a detective in the computer crimes unit, I investigated internet child pornography and computer crime cases.

4. I have conducted forensic computer examinations for:

   (a) Broward County Sheriff's Office (BSO);

   (b) Federal Bureau of Investigation (FBI);

   (c) U.S. Customs and Border Protection (CBP);

   (d) Florida Department of Law Enforcement (FDLE);

   (e) U.S. Secret Service;

   (f) Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); and

   (g) Various municipalities in the jurisdiction of Palm Beach County.

5. I was also previously assigned to a police unit working in conjunction with TLO Corp., which is a private company.

6. When I worked with TLO Corp., I supervised the other detectives assigned to the unit, which was consisted of six online investigators and two computer forensic examiners.

7. I am familiar with software programs used to investigate computers, including EnCase and Access Data.

13. I have been called to testify as a fact and expert witness on numerous occasions in the field of computer forensics in both trial-level and appellate proceedings before state, federal, and military courts in Florida, California, New Jersey, and New York.

14. No court has ever refused to accept my testimony on the basis that I was not an expert in computer forensics. My skill set and my reputation are my most important assets in my current position with Computer Forensics, LLC.

15. With regard to my experience investigating child pornography cases, I supervised police officers whose responsibility it was to establish a successful TCP/IP connection with persons who were sending pornographic images of children or other illegal content over the Internet.

16. The offenders' IP addresses, as well as the dates and times of the illegal transmission were recorded.

17. An officer would then request that the assistant state attorney subpoena the corresponding ISPs for the purpose of identifying the subscribers that were transmitting the illegal content.

18. In these cases, the subscribers were not notified by the ISPs that their identity was being subpoenaed because they could have deleted the images and destroyed the data.

19. After receiving the subscribers' identities, we would prepare a search warrant that would authorize us to enter the subscribers' dwelling and seize all of their computer devices.

20. I was directly involved in approximately 200 search warrants either by way of managing the process or performing it personally.

21. I can recall only one instance in all the times that we executed a search warrant and seized computers where we did not find the illegal content at the dwelling identified in the search warrant.

22. In that one instance, the Wi-Fi connection was not password protected, and the offender was a neighbor behind the residence.

23. I never came across a Wi-Fi hacker situation.

24. In my opinion, a child pornographer has a greater incentive to hack someone's Wi-Fi connection than a BitTorrent user because transmission of child pornography is a very serious crime with heavy criminal penalties, and many offenders can face life sentences if convicted.

25. I tested IPP International U.G.'s ("IPP") IP detection process.

26. To do so, I downloaded four public domain movies from the national archive.

27. I then encoded text into the videos, so that I would know whether someone that downloaded that particular movie downloaded the version of the movie that I created.

28. I then rented four virtual servers, each of which was connected to the Internet and used a unique IP addresses.

29. I then configured the servers so that all of them were running Windows 2008 server edition, and I put a different BitTorrent client onto each server.

30. A BitTorrent "client" is software that enables the BitTorrent protocol to work.

31. After installing the BitTorrent clients, I also installed Wireshark onto each server. "Wireshark" is a program that captures network traffic and creates PCAPs, just as TCP Dump, which IPP uses, does. A PCAP is like a video recording of all the incoming and outgoing transactions of a computer.

32. After installing Wireshark onto each of the servers, I transferred the movies from my local computer to the servers.

33. I then used the BitTorrent clients on each of the servers to make .torrent files. I uploaded these .torrent files onto various torrent websites.

34. I then informed IPP of the movie names. Thereafter, IPP sent me screen captures of the movies I had seeded.

35. The screen captures sent by IPP had my codes on them; thus, I knew that IPP had caught the movies I had seeded.

36. IPP also sent me additional data identifying the IP Address used by each of the four servers, and sent me PCAPs.

37. I reviewed IPP's PCAPs vis-à-vis the PCAP log files created by each of my test servers, and determined that IPP's PCAPs match my PCAPs. This could not have happened unless IPP's server was connected to the test server because the transactions would not match.

38. From this test, I concluded that IPP's software worked, and had a subpoena been issued for my IP addresses, it would have revealed my identity.

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury that the foregoing is true and correct.

Executed on this 11th day of November, 2013.

By:_____
PATRICK PAIGE

FURTHER DECLARANT SAYETH NAUGHT.

DECLARATION

PURSUANT TO 28 U.S.C. § 1746, I hereby declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on this 19th day of March, 2014.

By: _____
TOBIAS FIESER