JS 44 (Rev. 07/16)

CIVIL COVER SHEET

16-cv-6532

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
COOK PRODUCTIONS, LLC
844 Seward St.
Los Angeles CA 90038

(b) County of Residence of First Listed Plaintiff   Los Angeles, CA
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
LEE M. HERMAN ESQ.
426 E. Baltimore Ave.
Media PA 19063

DEFENDANTS
John Does 1 -5

County of Residence of First Listed Defendant   Unknown
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF
THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated or Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated and Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☒ 820 Copyrights
- ☐ 830 Patent
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation - Transfer
- ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing *(Do not cite jurisdictional statutes unless diversity)*:
17 USC 101 et. seq
Brief description of cause:
illegal distribution of copyrighted films

VII. REQUESTED IN COMPLAINT:
☐ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND $ Statutory damages

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY
(See instructions)
JUDGE _____   DOCKET NUMBER _____

DATE 12/20/16

SIGNATURE OF ATTORNEY OF RECORD

DEC 19 2016

FOR OFFICE USE ONLY

RECEIPT # _____   AMOUNT _____   APPLYING IFP _____   JUDGE _____   MAG. JUDGE _____

HB

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

CASE MANAGEMENT TRACK DESIGNATION FORM

Cook Productions, LLC   :   CIVIL ACTION
                                           :
                  v.   :
                                           :
John Does 1-5   :   NO.   16   6532

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

(a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255.   ( )

(b) Social Security – Cases requesting review of a decision of the Secretary of Health
    and Human Services denying plaintiff Social Security Benefits.   ( )

(c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2.   ( )

(d) Asbestos – Cases involving claims for personal injury or property damage from
    exposure to asbestos.   ( )

(e) Special Management – Cases that do not fall into tracks (a) through (d) that are
    commonly referred to as complex and that need special or intense management by
    the court. (See reverse side of this form for a detailed explanation of special
    management cases.)   ( )

(f) Standard Management – Cases that do not fall into any one of the other tracks.   (xx)

12-20-2016	Charles Thomas	Plaintiff
Date	**Attorney-at-law**	**Attorney for**
610-891-6500	215-689-1930	CThomas@LMHLaw.com
Telephone	**FAX Number**	**E-Mail Address**

(Civ. 660) 10/02

DEC 19 2016

UNITED STATES DISTRICT COURT

16   6532

FOR THE EASTERN DISTRICT OF PENNSYLVANIA — DESIGNATION FORM to be used by counsel to indicate the category of the case for the purpose of assignment to appropriate calendar.

Address of Plaintiff: Cook Productions, LLC 844 Seward St Los Angeles CA 90038

Address of Defendant: Unknown

Place of Accident, Incident or Transaction: Multiple locations within the Eastern District of PA

(Use Reverse Side For Additional Space)

Does this civil action involve a nongovernmental corporate party with any parent corporation and any publicly held corporation owning 10% or more of its stock?
(Attach two copies of the Disclosure Statement Form in accordance with Fed.R.Civ.P. 7.1(a))   Yes☐   No☑

Does this case involve multidistrict litigation possibilities?   Yes☐   No☑

RELATED CASE, IF ANY:
Case Number: _____ Judge _____ Date Terminated: _____

Civil cases are deemed related when yes is answered to any of the following questions:

1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court?   Yes☐   No☑

2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court?   Yes☐   No☑

3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action in this court?   Yes☐   No☑

4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual?   Yes☐   No☑

CIVIL: (Place ✔ in ONE CATEGORY ONLY)

A. *Federal Question Cases:*

1. ☐ Indemnity Contract, Marine Contract, and All Other Contracts
2. ☐ FELA
3. ☐ Jones Act-Personal Injury
4. ☐ Antitrust
5. ☐ Patent
6. ☐ Labor-Management Relations
7. ☐ Civil Rights
8. ☐ Habeas Corpus
9. ☐ Securities Act(s) Cases
10. ☐ Social Security Review Cases
11. ☑ All other Federal Question Cases
    (Please specify) Copyright

B. *Diversity Jurisdiction Cases:*

1. ☐ Insurance Contract and Other Contracts
2. ☐ Airplane Personal Injury
3. ☐ Assault, Defamation
4. ☐ Marine Personal Injury
5. ☐ Motor Vehicle Personal Injury
6. ☐ Other Personal Injury (Please specify)
7. ☐ Products Liability
8. ☐ Products Liability — Asbestos
9. ☐ All other Diversity Cases
    (Please specify) _____

ARBITRATION CERTIFICATION
(Check Appropriate Category)

I, Lee M. Herman , counsel of record do hereby certify:

☐ Pursuant to Local Civil Rule 53.2, Section 3(c)(2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of $150,000.00 exclusive of interest and costs;
☐ Relief other than monetary damages is sought.

DATE: 12-14-16 _____ 27570
                 Attorney-at-Law   Attorney I.D.#

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

I certify that, to my knowledge, the within case is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 12-14-16 _____ 27570
                 Attorney-at-Law   Attorney I.D.#

DEC 19 2016

CIV. 609 (5/2012)

#400

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

COOK PRODUCTIONS, INC.
Plaintiff

             v.

JOHN DOES 1-5,

             Defendants

Docket. No. **16 6532**

COMPLAINT

COPYRIGHT

JURY TRIAL DEMANDED

FILED
DEC 19 2016
LUCY V. CHIN Interim Clerk
By ___ Dep. Clerk

COMPLAINT

COOK PRODUCTIONS, INC. (hereinafter "CPI"), by and through counsel, hereby alleges the following:

1. This is a civil action for copyright infringement of federally registered copyrights in violation of the Copyright Act of 1976, 17 U.S.C. §§ 101 et seq. (the "Copyright Act"). Plaintiff seeks injunctive relief, statutory damages, attorney fees and costs, and such other relief as the Court deems proper.

2. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

3. Venue in this district is proper pursuant to 28 U.S.C. § 1391(b) and 28 U.S.C. § 1400(a) as the defendants are believed to reside in this district.

PLAINTIFF

4. Plaintiff CPI is a Nevada corporation with principal offices in Los Angeles, California and an affiliate of Nu Image / Millennium Films, production companies and distributors of a notable catalog of major motion pictures.

5. CPI is the registered holder of copyrights related to *Mr. Church*, a major motion picture theatrically released in the United States on Saturday, December 3, 2016.

6. *Mr. Church* is protected by the Copyright Act in registration PA 2-002-851. Exhibit A.

7. The motion picture contains wholly original material that is copyrightable subject matter under the laws of the United States.

8. The motion picture is currently offered for sale in commerce through multiple channels, including DVD release, On Demand streaming via cable providers, and available for rental through Amazon streaming video.

9. Defendant had notice of plaintiff's rights through general publication and advertising and more specifically as identified in the content of the motion picture, advertising associated with the motion picture and copies, each of which bore a proper copyright notice.

10. CPI seeks relief because its motion picture is currently available for lawful rental or purchase, yet is one of the most trafficked films in the BitTorrent network and is being illegally downloaded and distributed countless times worldwide with many confirmed instances of infringing activity traced to the Eastern District of Pennsylvania.

DEFENDANTS

11. The defendants are unknown persons, identified at this time by the IP addresses respectively assigned to each of them. Exhibit B

12. Using the BitTorrent peer-to-peer file sharing protocol, each defendant unlawfully transmitted some or all of the exact same illegal copy of *Mr. Church* to each other or common third parties.

13. Furthermore, each defendant uses Comcast for their Internet Service Provider (ISP); Comcast, on information and belief, sets their subscriber's equipment to be password protected by default.

14. Comcast provides notices and information to its customers about the importance of security, informing them that they are responsible for the activity associated with their account and cautioning subscribers against allowing third party or non-authorized access.

15. The records maintained by Comcast should be able to identify either the defendant, or the subscriber who contracted with Comcast for service who in turn is likely to have knowledge that will lead to the identity of the defendant.

16. Plaintiff intends to seek discovery, including issuing a subpoena for records from Comcast to ascertain the true identities of the defendants.

BITTORENT: THE TECHNOLOGY OF PIRACY

17. The heart of the matter before the Court is a 21st Century spin on an ages-old quest — how to get something for nothing.

18. BitTorrent is what is known as a peer-to-peer file sharing protocol; it allows a theoretically limitless number of users to share very large files across the Internet at a far higher speed than earlier file sharing methods.

19. BitTorrent is not, as some believe, software, but it requires software to implement; rather BitTorrent is a fire sharing protocol.

20. A protocol is a set of coded instructions that directs how software known as a BitTorrent client interacts with other users.

21. There are many different BitTorrent clients, each known by a different brand name — μTorrent, qBittorrent, and Transmission are but three — and users

may interact with anyone else on the network, even if using different BitTorrent clients.

22. No matter which BitTorrent client a person uses, using BitTorrent requires a number of volitional steps, the first of which is to install a BitTorrent client — plaintiff is unaware of any computer manufacturer shipping new computers with any BitTorrent client already installed.

23. Once installed, each BitTorrent user has access to hundreds of thousands of files, including major motion pictures, popular music, computer software, e-books, and entire seasons of hit television shows.

HOW IT WORKS

24. A user who wishes to share a new file via BitTorrent will find that it is very simple; every BitTorrent client has a function for creating new shared files, called Torrents.

25. The user identifies the file they wish to share, and the BitTorrent client takes that file and "breaks it up," into approximately 1000-2500 pieces; this means a very large file, like a high-definition motion picture, consists of relatively small puzzle pieces.

26. The BitTorrent client then assigns the new Torrent a unique hexadecimal string of characters called a Hash to the file; the Hash both identifies the file being shared and the order in which the discrete pieces must be reassembled to view the file once complete.

27. The initial user who first makes the file available for sharing is known as the Initial Seeder.

28. When a user (U1) first attempts to download the file, he or she searches through publicly available Torrents, either directly through their BitTorrent client, or through websites such as PirateBay.

29. When U1 finds the content he or she wishes to download, U1's BitTorrent client contacts the Seeder's BitTorrent client, and the Seeder begins to send U1 the file in 10KB pieces.

30. When a second user (U2) searching for the same file begins to download, U2 will receive pieces of the file from the Seeder; however, U2 will also receive what pieces U1 already has — in other words, U2 is now getting pieces from two users on the network.

31. A third user (U3) begins to download, and will receive pieces from the Seeder, and also U1 and U2.

32. The number of users continues to grow exponentially, as each new user collects pieces from all the users who already have pieces of the file, and in turn shares the pieces they have with subsequent users; the entirety of users sharing a particular file is known as a Swarm.

33. After a user has the entire file, they continue to participate in the Swarm, sharing the file in manageably sized pieces as long as their computer is connected to the Internet.

34. Participation in the Swarm is typically required — most BitTorrent clients do not permit users to download without uploading; as soon as a user has even a single piece, that piece will be shared with subsequent users.

35. However, custom built BitTorrent clients exist for purposes of investigation and detection of alleged infringements; plaintiff employs a consultant who uses one

such proprietary BitTorrent client that "mimics a user willing to act as a source of data, but no actual transfer takes place...." See Technical Report, attached as an Exhibit C hereto.

36. In other words, plaintiff's proprietary BitTorrent client only seems to act as an ordinary BitTorrent client — we are able to download pieces for investigatory purposes, but we do not further perpetuate the illegal file sharing by the Swarm.

37. That being said, the Swarm is what has made BitTorrent incredibly popular; since no single user is burdened with uploading an entire file to a single user, download speeds are much faster than earlier technologies where a single user shared to a single user.

38. Even despite the increased speed permitted by BitTorrent, downloading a very large file such as a feature length movie could take hours, or even days; it all depends on the number of users sharing the file, and whether their computers are connected.

THE INFRINGEMENTS AT ISSUE

39. Plaintiff CPI employs a consultant for the purpose of stopping internet piracy.

40. As part of the investigatory process, the consultant uses its proprietary download-only BitTorrent client to track BitTorrent traffic of the Plaintiff's works.

41. The consultant notes and records the IP addresses of all individuals from which infringing material is received.

42. Between 10/17/2016 and 12/3/2016, plaintiff's consultant did receive one or more pieces of a Torrent bearing the descriptive title *Mr.Church.2016.DVDRip.XViD-ETRG*, with assigned Hash value

FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A from each defendant's IP address.

43. On the date in question, the film *Mr. Church* had not yet been commercially released on DVD or Blu-Ray.

44. The illicit sharing of the film, therefore, directly interfered with Plaintiff's exclusive right to market, distribute, and profit from the display of this motion picture.

45. In other words, each defendant is a major pirate with no regard for the value of intellectual property.

46. Using geolocation technology, the consultant identified the city, county, and state of each infringer, as well as their ISP; based on that geolocation technology, plaintiff believes to a very high certainty that the IP addresses can be traced to physical locations within the Eastern District of Pennsylvania.

DIRECT COPYRIGHT INFRINGEMENT

47. Plaintiff herein reiterates paragraphs 1 through 46, and incorporates them by reference as if more fully set forth at length.

48. Each defendant did, and without the permission or consent of plaintiff, copied and distributed plaintiff's motion picture through a public BitTorrent network by transmitting the film in the BitTorrent file identified as Hash value *FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A*.

49. Defendants' actions infringed plaintiff's exclusive rights under the Copyright Act.

50. The conduct of the defendants has been willful, intentional, in disregard of and indifferent to plaintiff's rights with the intent to cause plaintiff harm.

REQUESTED RELIEF

51. As a direct and proximate result of the defendant's conduct, plaintiff's exclusive rights under 17 U.S.C. § 106 have been violated.

52. Plaintiff is entitled to an award of statutory damages pursuant to 17 U.S.C. § 504.

53. Plaintiff is entitled to an award of its costs, expenses and reasonable attorney fees pursuant to 17 U.S.C. § 505.

54. The conduct of the defendants is causing and, unless enjoined and restrained by this Court, will continue to cause plaintiff great and irreparable injury.

55. Pursuant to 17 U.S.C. §§ 502 and 503, plaintiff is entitled to injunctive relief prohibiting the defendant from further contributing to the infringement of plaintiff's copyrights, the economy of piracy, and ordering that the defendant destroy all copies of the motion picture made in violation of plaintiff's rights.

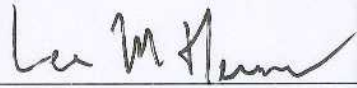**WHEREFORE**, plaintiff prays for judgment against each defendant as follows:

    A. For entry of permanent injunction enjoining each defendant from direct, indirect or contributory infringement of plaintiff's rights, including without limitation by using the internet to reproduce or copy plaintiff's motion picture, to distribute plaintiff's motion picture, or to make plaintiff's motion picture available for distribution to the public, except pursuant to a lawful license or with the express authority of plaintiff; further directing defendant to destroy all unauthorized copies of plaintiff's motion picture;

    B. For entry of permanent injunction enjoining each defendant from supporting the BitTorrent economy of piracy by enjoining the defendant from direct, indirect or contributory infringing file sharing in violation of U.S. copyright law;

C. For and award of statutory damages pursuant to 17 U.S.C. § 504;

D. For plaintiff's reasonable costs and attorney fees pursuant to 17 U.S.C.

§ 505; and

E. For such other and further relief as the Court deems proper.

DATED 12/15/16

CHARLES THOMAS, ESQUIRE
Atty. I.D. 89781
CThomas@lmhlaw.com

Attorneys for Plaintiff
426 E. Baltimore Ave.
Media, PA 19063
(t)610-891-6500   (f) (215) 689-1930

LEE M. HERMAN, ESQUIRE
Atty. I.D. 27570
lmh@lmhlaw.com

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, plaintiff demands a trial

by jury.

EXHIBIT A

Certificate of Registration

This Certificate issued under the seal of the Copyright Office in accordance with title 17, *United States Code*, attests that registration has been made for the work identified below. The information on this certificate has been made a part of the Copyright Office records.

Maria A. Pallante

United States Register of Copyrights and Director

Registration Number

PA 2-002-851

Effective Date of Registration:
August 29, 2016

Title

Title of Work: Mr. Church

Previous or Alternate Title: Cook

Henry Joseph Church

Completion/Publication

Year of Completion: 2015
Date of 1st Publication: September 16, 2016
Nation of 1st Publication: United States

Author

•   Author: Cook Productions, LLC
Author Created: entire motion picture
Work made for hire: Yes
Citizen of: United States
Domiciled in: United States

Copyright Claimant

Copyright Claimant: Cook Productions, LLC
844 Seward Street, First Floor, Los Angeles, CA 90038 United States

Limitation of copyright claim

Material excluded from this claim: script/screenplay

New material included in claim: all other cinematographic material, production as a motion picture

Rights and Permissions

Organization Name: Cook Productions, LLC
Address: 844 Seward St
First Floor
Los Angeles, CA 90038 United States

Certification

Name:	Mandy Blandford
Date:	August 22, 2016
Applicant's Tracking Number:	Mr. Church MP

Correspondence: Yes

EXHIBIT B

No	IP	Hit Date UTC	File Name	File Hash	City
1	96.93.53.22	2016-12-03 08:24:06	Mr.Church.2016.DVDRip.XViD-ETRG	SHA1: FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A	Philadelphia
2	69.253.230.6	2016-11-11 21:55:31	Mr.Church.2016.DVDRip.XViD-ETRG	SHA1: FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A	Media
3	174.54.63.179	2016-10-21 23:46:51	Mr.Church.2016.DVDRip.XViD-ETRG	SHA1: FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A	Lancaster
4	73.165.117.170	2016-10-19 03:35:01	Mr.Church.2016.DVDRip.XViD-ETRG	SHA1: FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A	Bensalem
5	69.249.39.63	2016-10-17 16:28:08	Mr.Church.2016.DVDRip.XViD-ETRG	SHA1: FB9EAB34A9CC31AABC73B4F560D4B6C49F3C856A	Philadelphia

EXHIBIT C

SACHVERSTÄNDIGEN-BÜRO FÜR COMPUTERWESEN
PROF. DR. PAUSCH & PARTNER

Büro Darmstadt: 64289 Darmstadt, Heinheimer Strasse 38
Tel: 06151/9712640 Fax: 06151/9712641
Büro Kassel: 34277 Fuldabrück, An der Röthe 10
Tel: 0561/95339100 Fax: 0561/95339101
Büro Grünstadt: 67310 Hettenleidelheim, Im Park 9
Tel: 06351/1359000 Fax: 06351/1359001
Büro Pegnitz: 91257 Pegnitz, Reisach 16
Tel: 09241/7359000 Fax: 09241/7359001
Büro Wiesbaden: 65197 Wiesbaden, Geschwister-Scholl-Str. 26
Tel/Fax: 0611/2046273
Office Sydney (G+R IT-Experts): Level 6, Spring Street, 2000 Sydney NSW
Phone: 02 82960492 Fax: 02 82960411

Report 140222/02

Evaluation of the System *MaverikMonitor*

On behalf of

Maverickeye UG (haftungsbeschränkt)
Herrn Yanick Gabriel
Heilbronner Straße 150
70191 Stuttgart

Expert witness

Dr. Simone Richter

von der Industrie-und Handelskammer Darmstadt
öffentlich bestellte und vereidigte Sachverständige
für das Sachgebiet Systeme und Anwendungen
der Informationsverarbeitung

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

1. Introduction

1.1   I was engaged as an expert by Maverickeye UG (haftungsbeschränkt) represented by Mr Yanik Gabriel, Heilbronner Straße 150, D-70191 Stuttgart, Germany.

1.2   I acknowledge that I have read, understood and complied with Practice Note CM7.

1.3   A copy of my CV may be found at appendix A of this report.

2. Instructions

2.1   My instructions were to provide answers to the questions set out below in relation to:

    (a)   the software program known as Maverik Monitor Version 1.47 (**Software**); and

    (b)   a system which monitors, detects and stores information in respect of data transfers of copyright material on the BitTorrent network of which the Software forms a part (**System**).

2.2   The questions which I was instructed to answer are:

    (a)   Is the Software capable of accurately detecting and recording copies of data being shared from a Subscriber's IP Address taking place on BitTorrent networks?

    (b)   How does the System function?

        (i)   Is there likelihood for erroneous information to be recorded by the Software?

        (ii)   Can the information recorded by the Software be manipulated by a user?

        (iii)   When the System engages in a BitTorrent transaction with a remote computer, is the System able to accurately record the IP address of the remote computer with the date and time?

        (iv)   What is the link between hash value and IP address, and does the System record this information accurately?

        (v)   What procedures are in place to ensure that the IP address recorded was allocated to the correct Subscriber at the time of the alleged copyright infringement?

        (vi)   What is the 'anti-leech mod' and how does it affect the System's reliability?

        (vii)   What are dynamic IP addresses and what effect (if any) do these have on the accuracy of the information recorded by the System?

        (viii)   What are hash collisions and how do they affect the accuracy of the information recorded by the System?

    (c)   Does the System download from a source computer the full file?

Page 2 of 27 Pages

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

3.   Source of Information and Scope of Work

3.1   In preparing this report, I have reviewed and relied upon:

(a)   user documentation for the Software (**User Documentation**);

(b)   the source code for the Software;

(c)   my visual inspection at one of the data centers where the System's information is gathered and stored; and

(d)   the test results from the physical test conducted between 16 and 20 January 2014, to test whether or not the System was capable of detecting distribution of a known data set being five different movie files using the BitTorrent protocol.

3.2   For the purpose of this report, I have accepted the information provided to me as accurate, unless otherwise stated.

3.3   I worked independently in my analysis of the Software and the System as laid out in the in deriving my opinion set out in this report.

3.4   My opinions are based wholly or substantially on the specialised knowledge set out in my CV at Annexure "A" to this report.

3.5   I do not express any opinion about the accuracy of the information provided to me upon which my findings are based. The conclusions in this report depend upon the accuracy of that information.

3.6   If any information I have relied upon is found to be inaccurate or incomplete, or further information is provided to me, I reserve the right to revisit my findings.

3.7   This report makes use of technical terminology, an explanation of which is set out at paragraph 6 of this report.

4.   Assumed Facts and Limitations

4.1   The NTP servers used by the System to calibrate its internal clock for the purpose of logging the date and time of alleged infringements are correct. The NTP servers are provided by local authorities and, as such, are trusted to distribute accurate time signals.

4.2   The hash value creation protocol for the copyrighted work and its sub-pieces is correct. As demonstrated with the five test files distributed over the BitTorrent Network.

5.   Summary of Findings

5.1   In my examination of the System, I found that:

(a)   it is capable of monitoring traffic on the BitTorrent network;

(b)   it identifies the IP addresses of users and records the time of the data transfer accurately. This information enables ISPs to identify the Subscriber whose internet connection was used to conduct the alleged copyright infringement;

(c)   The System implements mechanisms to ensure that no erroneous IP addresses are collected by the System.

(d)   The System establishes connections with remote computers and receives and stores pieces of data from those computers which make content available across the BitTorrent network.

(e)   The received pieces of data are compared to a control copy using hash value comparison. If the hash value of the piece of data downloaded from the source is the same as the control copy, then the received pieces of data and the control copy are considered to be identical.

(f)   Dynamic IP addresses have no influence on the accuracy of the System logging and recording IP addresses and associated time stamp of infringement.

(g)   If the source computer's IP address changes during capture of a data transfer, no data is saved by the System, and therefore not used by Maverickeye UG.

6.   Terminology

6.1   This report makes use of technical terminology. The technical terms used in this report are set out below.

BitTorrent

6.2   The BitTorrent network is a type of peer-to-peer network. Peer-to-peer networks are a conglomerate of computers that link together to share information, files or data with one another through the use of specialised software (**P2P Network**). The users or computers on a P2P Network can either receive or send information, files or data to other computers (or undertake both functions simultaneously).

6.3   On P2P Networks, a connection is established between the users of the network who are online at the time. Each participating computer can perform both the function of a "client" (i.e. the receiving or downloading computer) and that of a "server" (i.e. the sending or host computer). The computers can then both send data to, and receive it from, each other's computers. The data is exchanged directly between the participating computers and is never stored in a centralised place. The data distributed may have various origins, but data exchange takes place exclusively between two individual computer systems.

6.4   Users need to take active steps to set up and install software to enable participation in the P2P Network. These steps cannot be 'accidently' or inadvertently undertaken by a user. Any user wishing to participate in file sharing needs to install or actively start specialised software known as a BitTorrent client (**BitTorrent Client**). In order to do so, a user will need to download a

BitTorrent Client from a website that distributes BitTorrent clients. As part of the installation process, a user may configure the BitTorrent Client in accordance with his or her preferences, or adopt standard settings. A BitTorrent Client enables users to access a given P2P Network, such as eDonkey or BitTorrent. Some examples of BitTorrent Clients for the BitTorrent network include Azureus, BitComet and UT.

6.5   Once a user has installed the BitTorrent Client, the user may have an option to specify what is called the user's 'shared files' folder (**Shared Folder**) in which the user may place any files. Files placed in the Shared Folder are made available and may be distributed to other users requesting that file.

6.6   A user will then need to conduct a search of torrent files related to the data he or she wishes to acquire. Such data often includes copyrighted works such as films, television shows and music. Websites such as "The Pirate Bay" may be used to search for and obtain the relevant torrent files, as they offer torrent files and magnet links for download. The user then needs to download those torrent files and open them in their BitTorrent Client.

6.7   The BitTorrent network splits or separates a complete file, being for example, a movie or song (**Complete Data Set**) into pieces to enable efficient distribution to participants. Those pieces may be further broken down into sub pieces. When those pieces are reassembled, they constitute the Complete Data Set.

6.8   Once a user opens the torrent file in their BitTorrent Client, the BitTorrent Client queries the peers to which it is connected in order to ascertain which pieces of the Complete Data Set those peers have available to download. Some peers will have the Complete Data Set, and are known as "seeders" (**Seeders**). Other peers may have less that the whole file because they are still in the process of downloading it, but they will still be able to share the pieces that they have.

6.9   Over the time of downloading the Complete Data Set, pieces are requested and received by the BitTorrent Client from various other peers and are ultimately assembled together like a large jigsaw into the Complete Data Set. If, for example, the Complete Data Set is a film file, the film file will at this stage be in a state in which a user can view it.

IP address

6.10   An Internet Protocol (**IP**) address is an address which identifies a computer within an IP network. It is comparable to a postal address in the sense that it enables computers to exchange data with each other. The commonly used "IPv4" address consists of four numbers (values 0-255) separated by a dot. In computer terms it is a 32 bit large binary number.

6.11   There are more computers connected to the internet than available IPv4 addresses. To ensure that the information sent from another computer reaches the correct addressee, a dedicated technology is used called "Network Address Translation" (**NAT**).

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

6.12   Using NAT, an internet access point has at least one worldwide unique IP address. The internet access point is often a router or a a digital subscriber line (**DSL**) access point. This type of equipment is used to connect computers within an internal network. They are commonly found within households or businesses.

6.13   Each device connected to the internal network may have its own IP address assigned by a router. In circumstances where an internal network is present, the IP address logged by the Software will identify subscriber's internet access point only. That is, the IP address assigned to the router or DLS access point to which a number of computers can be identified.

6.14   It is not possible to determine if an internal network is present unless inquiries are made with the internet connection owner. There could very well be one computer connected to the router.

Dynamic IP address

6.15   An Internet Service Provider (**ISP**) has control of a large number of IP addresses. It assigns IP addresses to its account holders (**Subscribers**) in order to provide internet connections. An internet connection cannot function without an IP address.

6.16   The ISP may have more Subscribers than they control IP addresses. If this is the case, it may not assign fixed static IP addresses to its Subscribers.

6.17   An ISP may assign 'dynamic' IP addresses to its Subscribers. A dynamic IP address is only assigned for a limited time period. This period may vary from ISP to ISP. The time period could be up to six months or more and is dependent on each ISPs own internal policy.

6.18   Due to the nature of dynamic IP addresses, in order for ISPs to identify Subscribers from data logged by the System, two data points must be known: time of the data transfer and the associated IP address. Using this information, an ISP may cross-reference IP address, date and time with its Subscriber database.

Hash Values

6.19   An algorithm that correlates data of variable length to data of a fixed length is called a hash function. The value returned by the function is a hash value.

6.20   Two different sets of data may be compared using hash values. They are commonly referred to as digital fingerprints. They allow large quantities of data to be represented by a relatively small number of bytes. The determination of a hash value of a data set and the comparison of two hash values is more efficient than a byte-wise comparison of two files. The System uses hash value comparison to determine if two sets of data are identical.

6.21   For example, two different movies will have two different hash values. Furthermore, every piece of the movie will also have its own hash value.

6.22   There are various methods used to calculate hash values. The most commonly used hash value calculation method is called MD5. This method is known to have a mathematical "defect".

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

There is a possibility of creating the same hash value for two different sets of input data. If this occurs one calls this a hash collision. This method is <u>not</u> used by the System.

6.23   The second most applied method is called SHA-1. It is theoretically vulnerable to hash collisions, but so far there is no method known to create a hash collision. The method known to be collision free is called SHA-512 and the third most commonly used.

6.24   The P2P Network allocates a hash value to each file that is made available for sharing, so it can easily be identified by the P2P Network participants.

6.25   The System uses the SHA-1 and SHA-512 methods. The System uses SHA-1 as BitTorrent uses this to identify data. SHA-512 is used internally by the System to verify the downloaded sub-pieces against a control copy of data.

6.26   The Software uses hash value comparison to determine if two sets of data are identical. Accordingly, if two SHA-1 or SHA-512 hash values are the same, the data compared is said to be identical.

NTP Servers

6.27   A Network Time Protocol (**NTP**) server, or NTP Stratum-1 servers, is a networking protocol which synchronises all computers on an NTP server to within a few milliseconds by reference to Coordinated Universal Time (**UTC**), which is the primary time standard by which the world regulates clocks and times.

6.28   There are difference sources for UTC, such as the Global Positioning System and WWV, a radio station which continuously transmits official U.S. Government frequency and time signals. Both of these sources of UTC provide accurate time.

Module

6.29   A module is a part of a computer program which carries out a specific function and may be used along or in combination with other modules in the same program.

Data Structure

6.30   A data structure is the location where data is stored in a program. There are several different types of data structures which are capable of storing different types of data. If the data structure is not created for a particular type of data, then it will be unable to store that data.

Transport Control Protocol/Internet Protocol

6.31   The IP address attributes to a computer a unique reference number. By this number a computer is identified. The IP does not facilitate the transfer of data itself; therefore the Transport Control Protocol (**TCP**) was invented. It is a set of rules used along with the IP to send data in the form of message units between computers over the Internet.

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

7.   Method of Work

7.1   I examined and reviewed the User Documentation of the Software and the complete source code of the Software, line by line, and the scripts therein. In addition I set up files within the Bit Torrent network to be shared an downloaded by various users to determine if:

(a)   the System accurately monitors BitTorrent traffic;

(b)   the System's BitTorrent Client initiates a TCP connection with the source computers (as explained in paragraph 8.2 below);

(c)   the System accurately captures the IP address, together with time stamp and the port number used by the source computer when a data transfer between the Software and source computer is successful;

(d)   the System records the hash value of the data received from the source computer; and

(e)   the System accurately calculates the hash value of the sub-piece received from the source computer for the purposes of conducting a comparison with it and the reference file (a copy of the data set known to be a complete copy of the copyrighted work made available on BitTorrent networks).

7.2   I analyzed the source code of the Software line-by-line in order to ascertain:

(a)   the way in which data identified by the Software is processed;

(b)   the correctness of the various Data Structures containing the data identified; and

(c)   whether it correctly stores the data in the Data Structures and extracts the correct information from the data structures to ensure proper identification and comparison of hash values.

7.3   Finally, I examined the source code of the Software to evaluate the consequences of potential errors, including:

(a)   buffer overflows, which occur when data is being stored in the Software's module to capture amongst others the data set of IP-addresses, date, time and duration of the possible copyright infringements and the capacity to store the data is exceeded;

(b)   wrong variable handling, which can occur, for example, when the Software is expecting a variable (i.e. a location where temporary data is stored) to contain an integer number but instead it contains a string of text and is therefore unable to process the variable; and

(c)   logical errors resulting from bugs which cause the Software to operate incorrectly and produces an unintended or undesired output.

8.   **Live Tests performed in the BitTorrent Network to test the System**

8.1   I was asked by Maverickeye UG to test the System for accuracy by distributing Complete Data Sets using the BitTorrent Network. The purpose of this test was to conclude whether or not the System was capable of detecting distribution of a known Complete Data Set using the BitTorrent protocol.

8.2   This test was designed to be a real life test which allowed different users or peers to share data with the System.

8.3   I was given permission by the copyright owners of the Complete Data Sets distributed in the live scenario to use the Complete Data Sets in the tests described below.

9.   **Test implementation**

9.1   I informed Maverikeye UG of the time period that the tests would take place. I did so to ensure that Maverickeye's System was in operation during the time required to conduct the test. I also informed Maverickeye UG of the names of the files I was using as part of the test, so they would know which files to search for. I did not inform Maverickeye the precise point in time the downloading/uploading of the Complete Data Sets would occur. The test was performed between January 16th and 20th 2014 (**Test Period**).

9.2   In undertaking the test, I completed the following steps.

9.3   First, I uploaded four Complete Data Sets to my desktop computer. The Complete Data Sets used in the test were the following files:

    (a)   prepare-loopdevices.exe, being an executable file (i.e. software that causes a computer to perform tasks);

    (b)   AVI_0002.AVI, being a file containing both audio and video data;

    (c)   AVI_0004.AVI, being a file containing both audio and video data; and

    (d)   Vorlesungen.zip, being a compressed file containing multiple pdf files.

    (together **Test Data Sets**)

9.4   Second, I created a torrent file in respect of each of the files in the Test Data Sets using the following BitTorrent clients:

    (a) μTorrent version 3.3.2;

    (b)   KTorrent version 4.2.0 and 4.3.1; and

    (c)   Transmission version 2.82.

9.5 When creating the torrent files, I had to include a tracker address. The tracker address is what announces that the file is being made available and can be accessed by those using the BitTorrent network.

9.6 The trackers used for each of torrent files are set out below:

udp://tracker.openbittorrent.com:80/announce

udp://tracker.publicbt.com:80/announce

9.7 Third, during the Test Period, I used two mobile devices, named Samsung Mobile Device 1 and Samsung Mobile Device 2, to download the torrent files for each of the files in the Test Data Sets. Both of these devices are Samsung Tablets and each have internet connections provided by different ISPs and each have different IP addresses.

9.8 At the time of each download on each of the Samsung Tablets, I noted down the following information:

(a) the device being used, that is Samsung Mobile Device 1 or Samsung Mobile Device 2;

(b) the particular file being downloaded, e.g. prepare-loopdevices.exe;

(c) the IP Address of the device being used to download the file;

(d) the date on which the download commenced; and

(e) the time at which the download commenced.

A copy of the information that I have noted down in respect of the data transfers is set out in Schedule 2 to this Report.

9.9 I ascertained the date and time of the commencement of the download by monitoring my BitTorrent Client and noting the time at which the download appeared to commence on the BitTorrent Client.

9.10 I ascertained the IP address of each device by going into the settings of each device, where the IP address of the device is stated.

9.11 I was aware of each of the ISP providing the internet connection for each of the Samsung tablets, because I contracted with each ISP in relation to each device. In any event, using the IP address, it is possible to perform an internet search to obtain the ISP which owns the IP address.

9.12 After the termination of the test, Maverickeye UG provided me with an extract from their database, which had detected and stored information in respect of the data transfers which occurred during the Test Period.

9.13 I then compared the information I had noted down about the data transfers, with the information extracted from Maverickeye UG's databases.

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

9.14 An example extract of the System's database provided to me by Maverickeye UG is set out below. This extract is the information obtained by Maverickeye UG in relation one download by a user of the prepare-loopdevices.exe file. Each second line gives a short explanation of the meaning of the database entries.

ExportId	4771520570
	Unique number assigned automatically by the System
ExportTs	2014-01-16 16:44:22
	Timestamp of the export into the System's database
ClientinformationId	11313558141
	Unique number assigned to the user
Date	2014-01-16
	Date of the data transfer
Time	15:32:32
	Time of the data transfer
ClientProto	Bt
	Name of the protocol used in the data transfer. Bt means BitTorrent Protocol.
ClientIp	109.85.95.91
	IP Address of the user downloading the file
ClientPort	55980
	Port number used for the data transfer
ClientDhtPort	6881
	Special Port number used within the data transfer
ClientUserName	
	The username of the particular user with their ISP (unknown by Maverickeye UG)
ClientUserHash	2D4241333330302D9676CEC37D543F1A69838FD6
	Hash value
ClientVersion	-BA3300-
	Version of the Bit Torrent Client used
FileName	prepare-loopdevices.exe
	Name of the downloaded file
TrackName	prepare-loopdevices.exe
	Name of the part of the downloaded file
FileHash	8AAE50E22398E28AC4F20E5460A312B95E693F3A
	Hash value identifying the file
FileSize	16683
	Size of the file in bytes
BtBitField	0
	Value indicating the piece to download
GeoIpIsp	Vodafone D2 GmbH
	Name of the Internet Service Provider (ISP)

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

GeoIpOrg	
	Information about the ISP
GeoIpCity	Andernach
	City where the ISP is located
GeoIpZip	
	Post code of the city where the ISP is located
GeoIpCountry	DE
	Country where the ISP is located. DE means Germany.
GeoIpRegion	Rheinland-Pfalz
	Further information about the location of the ISP
GeoIpLon	7.4
	Geographical coordinates of the ISP location
GeoIpLat	50.4333
	Geographical coordinates of the ISP location
SessionStart	16/01/2014 3:31:58 PM
	Date and Time of the start of the detection of the download (UTC)
SessionEnd	16/01/2014 3:33:34 PM
	Date and Time of the end of the detection of the download (UTC)
TransferStart	16/01/2014 3:32:31 PM
	Date and Time of the end of the transfer (UTC)
TransferEnd	16/01/2014 3:32:32 PM
	Date and Time of the end of the transfer (UTC)
SessionDuration	96
	Duration of the session in seconds
LoggerId	clientng13
	Unique number of the logging process
LoggerIp	787014805
	IP number of the logging computer
LoggerCountry	DE
	Country where the logging computer is located
LoggerLon	8,4287
	Geographical coordinates of the logger's location
LoggerLat	49,0019
	Geographical coordinates of the logger's location
TotalPeers	0
	Number of additional peers
UniqTs	2014011615
	Another time stamp indicating the beginning of activity within the program. e.g. 16 Jan 2014 at 3pm (being 1500 hours).
RelatedTitleId	6467
	Internal unique number identifying the file
OwnerId	3668
	Internal unique number identifying the owner of the file

Dr. Simone Richter   64289 Darmstadt   Heinheimer Straße 38
Report 140222/02 from 2 April 2014 for Maverikeye UG

VerifyPartOk	YES
	Indicates whether the comparison of the data against a control copy was fine
ExporterVersion	2.5
	Version number of the Module forming part of the System used to export the data into the secure database
ExporterBinCRC32	c0dcf654
	The value assigned by a cyclic redundancy check[1] to the data transferred to the database. Upon retrieval of the data from the database, the cyclic redundancy check is repeated and if the two values match, then it can be assumed that the data is correct and has not been corrupted.

9.15   The System database extracts provided to me by Maverickeye UG are set out at Schedule 3 to this Report. These extracts set out all of the downloads of the Test Data Sets during the Test Period.

9.16   The data shown in the table above is extracted from row 5 of the file "6467 – Prepare-loopdevices.xls" of Schedule 3. This data correlates with the data I noted down in Schedule 2 at the tab titled "Prepare-loopdevices", that is, the ISP name, IP address, data and times of distribution correctly matched.

9.17   I can verify that the information that I noted down in Schedule 2 correlates with the data provided to me by Maverickeye UG.

9.18   It is my conclusion that the System is able to accurately detect data transfers on the BitTorrent network when deployed to do so.

10.   Inspection of the data center

10.1   I visited the data center where the System was running.

10.2   The purpose of my visit was to check that data was stored securely and could not be tampered with. From my inspection, I am confident that the safety measures put in place provide sufficient security to ensure that the data collected by the System is secure.

10.3   I also confirm that write once read many (WORM) tape drives are used to store data collected by the System in a secure manner. WORM technology provides non-editable data storage such that any data stored by the System cannot be altered, overwritten or corrupted.

11.   Answers to the Questions

11.1   The opinions set out below are based wholly or substantially on the specialised knowledge referred to in appendix A.

---

[1] Mathematical method developed by W. Wesley Peterson, 1961.