

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1 Heather L. Rosing, Bar No. 183986
David M. Majchrzak, Bar No. 220860
2 KLINEDINST PC
501 West Broadway, Suite 600
3 San Diego, California 92101
(619) 239-8131/FAX (619) 238-8707
4 hrosing@klinedinstlaw.com
dmajchrzak@klinedinstlaw.com

5 Attorneys for
6 PAUL DUFFY, ANGELA VAN DEN
HEMEL, and PRENDA LAW, INC.
7

8 UNITED STATES DISTRICT COURT
9 CENTRAL DISTRICT OF CALIFORNIA

10
11 INGENUITY 13 LLC,

12 Plaintiff,

13 v.

14 JOHN DOE,

15 Defendant.
16
17

Case No. 2:12-cv-8333-ODW(JCx)

**DECLARATION OF JOSHUA CHIN IN
SUPPORT OF RESPONSE TO ORDER
TO SHOW CAUSE**

Judge: Hon. Otis D. Wright, II
Magistrate Judge: Hon. Jacqueline Chooljian
Courtroom: 11
Date: April 2, 2013
Time: 10:00 A.M.

Complaint Filed: September 27, 2012
Trial Date: None set

18
19 I, Joshua Chin, declare as follows:

20 1. I am over the age of 18 years and the Executive Director of Net Force,
21 an internet and information systems security and forensics investigation company,
22 based in the City of Industry, California.

23 2. I have personal knowledge of the following facts and expert opinions
24 and, if called upon as a witness, could competently testify thereto, except as to
25 those matters which are explicitly set forth as based upon my information and
26 belief and, as to such matters, I am informed and believe that they are true and
27 correct.
28

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

3. I hold the following relevant certifications for my profession:
 - a. NSA NSTISSI 4011 – National Training Standard for Information System Security Systems Professional.
 - b. NSA CNSSI 4012 – National Information Assurance Training Standard for Senior Systems Managers.

4. I am a member of the following Professional Associations:
 - a. High Tech Crimes Investigator Association (HTCIA)
 - b. Information Systems Audit and Control Association (ISACA)
 - c. Open Web Application Security Project, Los Angeles (OWASP-LA)
 - d. FBI Infragard, Los Angeles
 - e. United States Secret Service, Los Angeles Electronic Crimes Task Force

5. I have competed for and received the following awards relevant to my industry:
 - a. 2nd place in Computer Forensics – 2010 Information Technology Competition
 - b. 2nd place finalist – 2012 Symantec Cyber Readiness Challenge, Irvine, California.
 - c. 3rd place finalist – 2013 Symantec Cyber Readiness Challenge, Mountain View, California.

6. I have engaged in research and delivered numerous presentations to companies, universities, and trade associations engaged in electronic security measures and computer forensics throughout the country. Examples include Cal-Poly Pomona, the High Tech Crimes Investigation Association International Conference, and the Information Systems Audit and Control Association.

7. I graduated from California State Polytechnic University, in Pomona, California, with a Bachelor of Science in Business Administration and major in

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1 Computer Information Systems.

2 8. I was requested by counsel for Prenda Law, Paul Duffy, and Angela
3 Van Den Hemel to research and provide an objective analysis on the following
4 topics:

- 5 a. Whether the IP address tracking protocol described by Peter
6 Hansmeier in his declaration filed in the matter entitled *Ingenuity*
7 *13, LLC v. John Doe*, assigned case number 1:12-cv-04238 by the
8 United States District Court for the Northern District of Illinois,
9 Eastern Division, was reasonable for purposes of identifying IP
10 addresses whose users were found to be engaged in the
11 unauthorized down- and uploading of copyrighted work; and
- 12 b. The best and most reasonable means by which to identify the user
13 of the IP address responsible for the unauthorized down- and
14 uploading of copyrighted works.

15 **Information Reviewed and Research Conducted**

16 9. I reviewed the following documents as part of my research into the
17 topics on which I was to provide my analysis and opinions:

- 18 a. The Declaration of Peter Hansmeier filed in the matter entitled
19 *Ingenuity 13, LLC v. John Doe*, assigned case number 1:12-cv-
20 04238 by the United States District Court for the Northern District
21 of Illinois, Eastern Division;
- 22 b. This Court’s February 7, 2013, Order to Show Cause re Sanctions
23 for Rule 11 and Local Rule 83-3 Violations;
- 24 c. Pleadings, declarations, and exhibits filed on behalf of Brett Gibbs
25 and in response to the Court’s February 7, 2013, Order to Show
26 Cause re Sanctions for Rule 11 and Local Rule 83-3 Violations;
- 27 d. Pleadings, declarations, and exhibits filed on behalf of the putative
28 John Doe by Morgan Pietz, said documents filed in response to the

1 Court’s February 7, 2013, Order to Show Cause re Sanctions for
2 Rule 11 and Local Rule 83-3 Violations; and

3 e. Various peer-reviewed research papers, abstracts, law journal
4 articles, and newspaper articles regarding the economic impact of
5 internet piracy and statistics pertaining to the pervasiveness of
6 internet piracy.

7 10. In addition, I consulted with industry experts and employees
8 concerning the subject matters for which I was asked to opine.

9 **Expert Conclusions and Opinions**

10 11. The protocol described by Peter Hansmeier in his declaration and a
11 similar protocol described in Brett Gibbs’s Response to the Court’s February 7,
12 2013, OSC, at page 13, to identify IP addresses that were engaged in the unlawful
13 down- and uploading of copyrighted material in a Bit Torrent swarm are a
14 reasonable means by which to identify the IP addresses.

15 12. My experience with Internet Service Providers (“ISPs”) is that they
16 will not voluntarily provide an investigator with the name or contact information of
17 a subscriber whose IP address was identified as unlawfully down- and uploading
18 copyrighted materials. Based on this experience, and in order to assist my client in
19 defending against unlawful infringement of its works, I would recommend that the
20 client retain an attorney and seek discovery via the courts.

21 13. I have reviewed the procedures described in the Declaration of Brett
22 L. Gibbs in Support of Response to February 7, 2013, OSC, at paragraphs 26-42
23 regarding his attempts to identify the actual infringers associated with the IP
24 addresses identified by Peter Hansmeier. I believe Mr. Gibbs engaged in
25 reasonable efforts to identify the infringers and simply ran into the inevitable
26 investigative limitations arising from conduct that more times than not is
27 conducted in secrecy and in the privacy of one’s home. I have recited further
28 limitations in paragraph 16 below.

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1 14. If I have reservations concerning any part of Mr. Gibbs's declaration
2 regarding his attempts to identify infringers, it would pertain to his conclusions
3 regarding the accessibility of the subscribers' wireless signals (paragraphs 31 and
4 38). My concerns are that certain routers have more range than others and the
5 position of the routers within the homes would impact the range that the routers'
6 signals could reach outside of the structures. Therefore, Mr. Gibbs might or might
7 not be correct in his conclusions that the wireless networks were inaccessible to
8 others outside the home. But, as discussed in paragraph 16 below, the fact that
9 there is one or more wireless signals present in any given area provides little useful
10 information, as one would have to illegally log onto the wireless networks to
11 determine the identity of the network's owner, and even then, the pervasive use of
12 dynamic IP addresses means that one who unlawfully logs onto a network to obtain
13 identifying information likely will not find the same IP address as previously
14 assigned to the subscriber. Given these facts, I do not consider Mr. Gibbs's
15 somewhat lay comprehension of wireless routers to be material to the issue of the
16 reasonability of his identification efforts.

17 15. I have also reviewed the letters Mr. Gibbs sent to Defendants David
18 Wagar and Marvin Denton (Exhibits 2-5 to the Gibbs's Declaration) and find that
19 the investigatory procedures outlined by Mr. Gibbs, in the event that Mssrs. Wagar
20 and Denton were not forthcoming with information concerning potential infringers
21 using their networks, were reasonable. If the subscribers are not forthcoming
22 about whether they have secured wireless networks, whether they or anyone with
23 access to their networks had unlawfully downloaded the client's copyrighted work,
24 or whether they or anyone with access to the networks were online at the time of
25 the infringement, a forensic inspection of the subscribers' computers is appropriate
26 to determine these questions. As noted by Mr. Gibbs, he had dismissed lawsuits in
27 which subscribers informally provided sufficient information to quell any concerns
28 that they had engaged in piracy.

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

16. Having reviewed the Court’s February 7, 2013, Order to Show Cause re Sanctions for Rule 11 and Local Rule 83-3 Violations, I have concluded that the Court’s recommendation of an “old-fashioned stakeout” is based on erroneous data and protocols that inevitably will not lead to the type of information sought by the Court. In addition, the Court’s suggested protocol may lead to criminal sanctions. For example:

- a. In a Bit Torrent swarm, only one electronic file is being distributed, and upon joining the swarm, the participant by default becomes immediately both a receiver and distributor of the file being traded.
- b. Any participant in a Bit Torrent swarm can observe the size of the electronic file currently in possession of any other swarm participant.
- c. Incomplete files possessed by anyone in the swarm can be viewed with free, online media players such as the VLC Player (<http://www.videolan.org/>). This player is so effective, local law enforcement, including but not limited to the Los Angeles District Attorneys’ High Tech Crimes Division and Riverside County’s District Attorneys’ Office, use the player in their efforts to prosecute criminal infringers. Use of the VLC Player has produced up to five seconds or more of images from a video file that had been the subject of no more than thirty seconds of downloading.
- d. Students with access to university computer networks and a Bit Torrent swarm have downloaded full length, 2-hour Hollywood feature films in as little as 30 minutes.
- e. Wireless networks, whether protected or unprotected, do not identify their assigned IP addresses or owners’ information unless

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- a user logs onto the network. Unauthorized entry onto a wireless network, whether protected or unprotected, to my understanding is a violation of the Computer Fraud and Abuse Act. As such, I would not attempt to identify a network’s IP address by unlawfully logging onto the network.
- f. Due to the pervasive use of dynamic IP addresses by ISPs, it is highly likely that the IP address associated with an allegedly downloading subscriber will have changed by the time an investigator reaches the subscriber’s home or place of business for a stakeout.
 - g. In the last 2-3 years, ISPs that furnish wireless hardware with their internet service and other wireless hardware manufacturers have provided default protection modes for the networks created by their wireless hardware. Thus, on the first day that a user plugs in his new wireless router, the network that is created is protected. Although some of this hardware requires its owner to provide passwords to further protect the networks, the growing awareness of wireless security options, combined with the default security protections, have significantly reduced the number of unprotected residential wireless networks in the State of California and likely across the nation. In my experience, a large majority of residential networks in California are now protected.
 - h. Impediments such as building walls, foliage, and other structures, both natural and man-made, can significantly weaken a wireless signal, thereby reducing its effective range by as much as 50%.
 - i. Even if it was ascertained that the infringer’s network was protected, absent the unlikely scenario that an infringer downloads and watches his pornography in the open or said infringer discloses

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

his activities to a complete stranger (the investigator), there is still no legal method by which an investigator could with absolute certainty conclude that the identified subscriber was the only person in a residence or commercial building engaged in the downloading of copyrighted materials at any one time.

17. In addition, the time necessary for a traditional investigation greatly prejudices any copyright owner’s efforts to protect its legal rights in its copyrights. My research has disclosed that 500,000 movies are illegally distributed around the world each day.¹ The economic detriment to the movie industry alone is estimated to cost \$447 million a year.² Pursuing lawsuits against individuals on the basis of time-intensive stakeouts, in lieu of available electronic means that provide sufficiently similar, if not identical, information about multiple infringers, is unreasonable in my expert opinion and not in the best interests of a copyright owner who is attempting to stem the tide of pervasive piracy.

18. By way of example, CNN reported on April 2, 2013, that the recent season premiere of the award-winning “Game of Thrones” was downloaded by more than 1 million viewers on the first day after it had aired. The article goes on to state the following: “At one point, more than 163,000 people were simultaneously sharing a single torrent – a new record.” The 2012 season finale of “Game of Thrones,” a one-hour action-adventure show on the pay channel, HBO, was downloaded by 4.3 million people, and the series in general “was the most pirated show in 2012.”

(<http://money.cnn.com/2013/04/02/technology/game-of-thrones-piracy/>)

19. Whereas it would be virtually impossible to deploy 163,000 investigators simultaneously to eavesdrop through windows to identify

¹ “Uniting to Fight Content Theft,” Ortman, Chris, Boxoffice 148:11 (November 2012).
² “Piracy or promotion? The impact of broadband internet penetration on DVD sales,” Smith, Michael D. and Telang, Rahul, School of Information Systems and Management, Carnegie Mellon University, April 2, 2010.

KLINEDINST PC
501 WEST BROADWAY, SUITE 600
SAN DIEGO, CALIFORNIA 92101

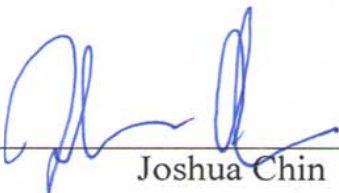
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

contemporaneously with the swarm who each of the infringers were during the few minutes it would take to complete a download, it would be possible and more practical to identify the infringers through electronic means and subsequent court-sanctioned discovery. For the same reason, electronic investigation of AF Holdings's and Ingenuity 13's infringers is likewise, not only within the computer forensic community's standard of care, but the overwhelmingly most common means of infringer identification.

20. By way of a second example, FOX Studios estimated for Variety Magazine in May 2009 that its then-new release, "X-Men Origins: Wolverine," which had been unlawfully leaked prior to its premiere, was illegally downloaded 4.5 million times in a month. BBC News estimated on April 1, 2009, that 75,000 copies of the movie had been unlawfully downloaded in a 24 hour period after the leak. FOX estimated its losses due to this piracy approached \$20 million.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed the 8th day of April 2013 at County of Los Angeles, California.



Joshua Chin

15508970v1