

Honorable Thomas S. Zilly

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

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON AT SEATTLE

VENICE PI, LLC,
Plaintiff,
v.
SEAN O’LEARY JR., et al.
Defendants.

Civil Action No. 17-cv-988TSZ

VENICE PI, LLC,
Plaintiff,
v.
JONATHAN DUTCZAK, et al.
Defendants.

Civil Action No. 17-cv-990TSZ

VENICE PI, LLC,
Plaintiff,
v.
MARTIN RAWLS, et al.
Defendants.

Civil Action No. 17-cv-991TSZ

VENICE PI, LLC,
Plaintiff,
v.
INA SICOTORSCHI, et al.
Defendants.

Civil Action No. 17-cv-1074TSZ

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

VENICE PI, LLC,
Plaintiff,
v.
GREGORY SCOTT, et al.
Defendants.

Civil Action No. 17-cv-1075TSZ

VENICE PI, LLC,
Plaintiff,
v.
YELENA TKACHENKO, et al.
Defendants.

Civil Action No. 17-cv-1076TSZ

VENICE PI, LLC,
Plaintiff,
v.
CELINA POTTER, et al.
Defendants.

Civil Action No. 17-cv-1160TSZ

VENICE PI, LLC,
Plaintiff,
v.
TONJA LAIBLE, et al.
Defendants.

Civil Action No. 17-cv-1163TSZ

VENICE PI, LLC,
Plaintiff,
v.
VICTOR TADURAN, et al.
Defendants.

Civil Action No. 17-cv-1164TSZ

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

VENICE PI, LLC,
Plaintiff,
v.
JESSE COOPER, et al.
Defendants.

Civil Action No. 17-cv-1211TSZ

VENICE PI, LLC,
Plaintiff,
v.
JASMINE PATTERSON, et al.
Defendants.

Civil Action No. 17-cv-1219TSZ

VENICE PI, LLC,
Plaintiff,
v.
DAVID MEINERT, et al.
Defendants.

Civil Action No. 17-cv-1403TSZ



DECLARATION OF BENJAMIN PERINO

I, Benjamin Perino, declare as follows:

1. My name is Benjamin Perino.
2. I am over the age of 18 and am otherwise competent to make this declaration. This declaration is based on my personal knowledge and, if called upon to do so, I will testify that the facts stated herein are true and accurate.
3. I am willing to travel to the State of Washington, and appear before Your Honor to answer any questions and to discuss the statements in this declaration and in my prior declaration.

My Skills, Knowledge, Experiences, and Qualifications

4. I understand that my expertise and knowledge regarding peer-2-peer and the BitTorrent network has come into question. As such, I wanted to clarify some of my prior work experience and provide the Court with more details.
5. Much of my knowledge about Information Technology and network traffic monitoring was obtained during my ten years of employment at Siemens.
6. After attending technical high school, I was hired by Siemens to undergo vocational training as a Developer with a specialization in Information Technology systems integration. This was an apprenticeship which lasted three years.
7. Siemens AG, my prior employer, is a “global powerhouse focusing on the areas of electrification, automation and digitalization. One of the world’s largest producers of energy-efficient, resource-saving technologies, Siemens is a leading supplier of systems for power generation and transmission as well as medical diagnosis. In infrastructure and industry solutions the company plays a pioneering role.”¹ In sum, Siemens AG provides, “state-of-the-art solutions in fields including IT, industry, finance and energy.”² As of September 30, 2017, Siemens had

¹ <https://www.siemens.com/global/en/home/company/about.html> (Last Accessed on January 23, 2018)

² *Id.*

around 372,000 employees in more than 200 countries/regions.”³ “In fiscal 2017, which ended on September 30, 2017, Siemens generated revenue of €83.0 billion and net income of €6.2 billion.”⁴

8. As stated in my earlier declaration, I began at Siemens as a Developer and IT Specialist in Research and Development. Eventually, I obtained the title of Senior Developer. And around 2007, I worked at a Siemens department where I was responsible for the quality assurance for the automation development process of SIMATIC PCS 7 PDM. The key part of this job was to pass new features developed for Siemens’ proprietary monitoring software.

9. In paragraph 9 of my earlier declaration, I explained that while working at Siemens as a Senior Developer, I helped develop the Industrial Ethernet Bus Analysis Software titled BANY.NET / PNIO (“BANY”) which records ethernet network traffic. This educated me on *how* to monitor network traffic. I also learned how to record large amount of network traffic into a database. This is because BANY itself monitored network traffic at a higher level than even Wireshark. Specifically, BANY enabled reaction-free real-time analysis of data traffic at rates of up to 1 Gbps per second. One Gbps per second (Gbps) equals 1000 Mbps.⁵

10. Wireshark was first developed in 1998. My team at Siemens was able to create a software similar to Wireshark which was usable for industrial communication and with higher standards. Although created in 1998, to date Wireshark is one of the most popular and widely used packet analyzers on the market. And, Law Enforcement still uses it to analyze network traffic.⁶ My work at Siemens which clearly made advancements in network traffic monitoring, is what provided me with my experience, knowledge, and expertise in ethernet and network traffic monitoring—independent from the content monitored. I used this basis to specialize in monitoring Bittorrent content when I started GuardaLey.

³ <https://www.siemens.com/global/en/home/company/about.html#Siemensworldwide> (Last Accessed on January 23, 2018)

⁴ <https://www.siemens.com/global/en/home/company/about.html> (Last Accessed on January 23, 2018)

⁵ <https://www.lifewire.com/bits-per-second-kbps-mbps-gbps-818122> (Last Accessed on January 23, 2018)

⁶ <https://gcn.com/articles/2017/05/25/cybercrime-investigations.aspx> (Last Accessed on January 23, 2018); https://sharkfestus.wireshark.org/sharkfest.12/presentations/MB-7_Network_Forensics_Analysis-A_Hands-on_Look.pdf (Last Accessed on January 23, 2018)

11. As I stated in my earlier report, I have been subpoenaed to testify either at deposition, trial, or by written statement for the cases listed on Exhibit A of my prior declaration.⁷ More specifically, I have testified by deposition, trial, or by written statement about my experience and knowledge in BitTorrent technology and the infringement detection system in each of the cases listed below.

- a. Amtsgericht München Splendid Film GmbH Cichon, J. 224 C
16522/15 2017-02-02
- b. Bochum - I-5 114-16 WVG vs Hill - 2017-04-28
- c. Karlsruhe - 101 AR 32/15 KSM vs Demangeot 2015-09-30
- d. Nürtingen - 17 C 1148/14 MIG vs Harder - 2014-09-15

Background of Infringement Detection Systems and Various Witnesses and Companies

12. I understand that there is concern regarding the many different infringement detection services, companies, employees, and their relations to one another. I have been involved in this industry for ten (10) years, and I therefore can provide some information on the evolution of these companies as I understand it.

13. As I previously stated, I am the sole owner of GuardaLey which I created in 2008. GuardaLey was created to provide clients and their respective attorneys with the ability to monitor the illegal downloading and distribution of their copyrighted works so that they may protect their content if necessary.

14. In order to provide these kinds of services, I needed to study peer-to-peer networks. This was easy since I already had network traffic monitoring experience. And so, between 2007 and 2008, I began studying Gnutella and BitTorrent. I learned how they each worked. Since most clients for these protocols were open source, I used existing platforms as a basis for creating new clients to monitor peer-to-peer networks.

15. As I learned, I began to develop an infringement detection system—a system which could use .torrent files associated with a specific work to join the swarms, connect with IP

⁷ As I stated in my prior report, I did not have to appear in all cases since some of them were canceled/settled before I had to appear. I cannot reproduce exactly which ones were cancelled.

addresses, and download the relevant work from these IP addresses without distributing the work. By 2008, I had created such a system.

16. GuardaLey licenses its monitoring interface to companies like Maverickeye UG, which were retained to track illegal content for their clients. In 2011, I decided that GuardaLey would outsource parts of the infringement detection and data collection tasks to a company called Excipio. As such, we retained and instructed Excipio to develop and maintain a system and obtained a license for it. And, from 2012 to 2015 GuardaLey used Excipio's system. During this time, Michael Patzer worked as independent contractor for Excipio.

17. GuardaLey's licensees (such as MaverickEye) employ software consultants that are charged with the task of reviewing and organizing data log files created by the GuardaLey's system. They were also charged with verifying hashes, meaning they had to ensure that the work being distributed within particular swarms were actual visual copies of the copyrighted work. This would require them to review the infringing files and compare them to the control copy of the work. The completion of these tasks was time consuming and has nothing to do with the actual data collection.

18. To be clear, GuardaLey is solely a software and service provider to these licensee companies that use the data captured by GuardaLey for their own purposes.

19. By 2015, I had redesigned and created GuardaLey's new infringement detection system, which was ready to collect infringement data. At that point, GuardaLey terminated its licensing agreement with Excipio, and cease consulting with Michael Patzer.

20. GuardaLey has employed, among others, the following individuals: Daniel Arheidt, and Tobias Fieser. Each of these individuals performed their duties in Germany. They never performed any of their duties for GuardaLey in the State of Washington. I also personally met each of them.

21. GuardaLey is a German company, and it is not a company organized, existing, located or operating in Washington State. GuardaLey has no employees or agents in Washington. It does not conduct any business in Washington. It does not pay taxes in Washington. Its servers

do not detect or record evidence of infringement in Washington State. Indeed, its servers and all employees or consultants are located in Germany and thus the detection and recording are completed in Germany.

22. To the best of my knowledge, in addition to working for GuardaLey, Tobias Fieser currently works for IPP International UG⁸ and MaverickEye on a part-time basis. I personally met Mr. Fieser and I see him on a daily basis. Daniel Macek used to work for both MaverickEye and IPP. I personally met Mr. Macek. To the best of my knowledge, he no longer works for either company. Daniel Arheidt currently works for GuardaLey. To the best of my knowledge, in addition to working for GuardaLey, Mr. Arheidt currently works for IPP and MaverickEye. I personally met Mr. Arheidt. Each of these individuals have provided data log examination and hash verification services.

23. GuardaLey's infringement detection system has been examined and tested repeatedly by a number of experts including, Mathias Gärtner, Dr. Simone Richter, Patrick Paige of Computer Forensics, LLC, and Robert Young. In addition, it was most recently tested this past week by Stephen Bunting of Bunting Digital Forensics, LLC. Each expert has found GuardaLey's system to be reliable and accurate.

False Positives

24. With respect to my opinion in my prior declaration regarding "false positives," I maintain that the infringement detection system cannot yield a false positive. However, I would like to provide some clarification on what I mean by this statement. The infringement detection cannot yield a false positive in that it cannot possibly record a TCP/IP connection and transaction that did not occur at the specific time date and time. I did not opine that the subscriber of the IP address is the infringer. Indeed, it is possible that the infringer is another person within the household who had access to and used the IP address. I only stated that a recording of a false positive with respect to the connection and transmission of data via the BitTorrent network cannot

⁸ IPP is another licensee of GuardaLey's system.

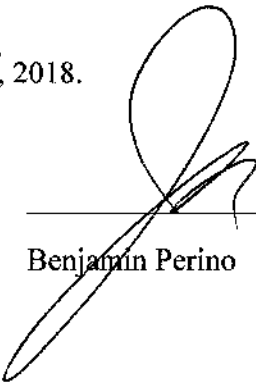
happen. The best analogy I can use to explain this is a video camera. The monitoring system acts similarly to a video camera recording events, but instead it records events occurring via the BitTorrent network. The PCAP is like a video tape recording an action in real time on a tape the records of which cannot be altered. This PCAP or video tape establishes that the particular event recorded actually occurred. However, the PCAP or video tape only provides us with some information. Here, the PCAP has the date and time of each infringing transaction, the IP address engaged in the transaction, the BitField Value, and the BitTorrent client used. And, the PCAP is recorded on an inalterable tape. The only question is the identity of the individual that used a device to engage in that transaction. This is an issue that the parties and their attorneys attempt to resolve in the case. GuardaLey only ensures the integrity of the data, and supplies the data to MaverickEye, who in turn supplies it to the Plaintiff's attorneys. The interpretation of that data is left to the parties and the Court. And evidence in a case can narrow down who, in proximity and with access to the internet connection, is the infringer.

25. The Court's order notes a Washington private investigator statute. I am not an attorney and so I cannot interpret that statute. I will, however, confirm that GuardaLey, GuardaLey's employees, and all equipment (servers, infringement detection system, etc.) which GuardaLey uses (as well as licensees such as MaverickEye) are *not* located in Washington State. Rather, all the equipment and all employees are located in Germany. And the data center that stores the electronic evidence is located in an ISO 27001 certified Datacenter in Karlsruhe, Germany.

26. Additionally, all of the information the infringement detection system collects and records is public information available to those who join the swarm. Indeed, anyone can see which IP addresses are in a swarm and can eliminate any false positives/spoofing issue by establishing a TCP/IP connection with the IP addresses in a swarm. I am willing to travel to the State of Washington, and appear before Your Honor to provide any additional explanation on how this works.

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

EXECUTED the 5th day of FEBRUARY, 2018.



Benjamin Perino

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

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served to all counsel or parties of record who are deemed to have consented to electronic service via the Court’s CM/ECF system, and to all Defendants at their last known address via U.S. mail.

s/ David A. Lowe