**UNITED STATES DISTRICT COURT**
**SOUTHERN DISTRICT OF FLORIDA**
**FORT LAUDERDALE DIVISION**

| | | |
|---|---|---|
| MALIBU MEDIA, LLC, | ) | |
| | ) | |
| Plaintiff, | ) | |
| v. | ) | Civil Action No. |
| | ) | 0:14-cv-61957-JIC |
| ROBERT DARE, | ) | |
| | ) | |
| Defendant. | ) | |
| _____ | ) | |

**DEFENDANT'S STATEMENT OF MATERIAL FACTS**

COMES NOW Defendant, ROBERT DARE, by and through his undersigned counsel, pursuant to Local Rule 56.1, and hereby submits the Statement of Material Facts to support his Motion for Summary Judgment.

1. Plaintiff is a publisher of pornographic videos.

2. Comcast is the Internet Service Provider that issued IP address 98.249.146.169.

3. Through a subpoena, Plaintiff asked Comcast for the name and address of the Comcast customer who subscribed to IP address 98.249.146.169 on only one date and time: June 8, 2014, at the exact time of 00:13:41 UTC. (MSJ Exh. 1)

4. Comcast responded with a letter identifying Defendant, Robert Dare, as the individual who subscribed to IP address 98.249.146.169 on only one date and time: June 8, 2014, at 00:13:41 GMT. (MSJ Exh. 2)

5. Even though Plaintiff accuses Defendant of downloading 17 videos, Plaintiff has only tied Defendant to being the accountholder of the IP address in question for one

of the 17 alleged "hit" date and times: June 8, 2014, at 00:13:41 GMT.

6. "IP addresses can change frequently due to their dynamic nature." *Bubble Gum Prod., LLC v. Does 1-80*, 2012 Copr. L. Dec. P 30292, 2012 WL 2953309 (S.D. Fla. 2012).

7. Comcast assigns dynamic IP addresses. *U.S. v. Vosburgh*, 602 F.3d 512, 523 (3d Cir. 2010).

8. Comcast purges its information after 180 days. *Id.*

9. Without Comcast's testimony, Plaintiff cannot establish that IP address 98.249.146.169 was assigned to Defendant. Doc. 69 at 2.

10. Plaintiff has no evidence that Defendant downloaded any of its videos.[1]

11. Plaintiff has not obtained any admission from Defendant about downloading or distributing Plaintiff's videos. Doc. 54-2 at 22-23 (Rog 15); MSJ Exh. 4.

12. No witness has admitted to having observed Plaintiff downloading or distributing Plaintiff's videos.

13. In an attempt to obtain whether Plaintiff's videos had been downloaded onto his computer devices, Defendantbrought his iPhones and iPads to computer technicians at NextDoorGeeks, LLC, who searched for the titles of Plaintiff's works as listed in Exhibit B to the Amended Complaint as well as terms "X-Art," "Malibu Media," or "torrent." The search revealed no documents. Exh. "4" at ¶¶ 5-7.

[1] *See* Exh. "3" at 5 # 1, Defendant's requests for admissions to Plaintiff, asking, "You have no evidence to tie Defendant directly to the alleged downloads." Plaintiff failed to respond or object to this request for admission; accordingly, it is deemed admitted. Fed. R. Civ. P. 36(a)(3).

14. The only other computer Defendant had used at his home within the subject download period was a work-issued computer that Defendant had returned to his former employer, OpenPeak, in August 2014. (Doc. 54-2 at 9.)

15. This computer was been disposed of due to damage and was therefore unavailable. MSJ Exh. 5.

16. Plaintiff has no evidence that any of its alleged videos were downloaded onto any of Defendant's computer devices.

17. Defendant was running an open guest network that was accessible by neighbors and was not password protected.

18. Because Defendant's Internet was accessible by neighbors via an unprotected wifi, if Plaintiff's videos were downloaded from Defendant's Internet account, the downloader could have been — and probably was — a neighbor.

19. During the alleged download period of Plaintiff's videos (March-June 2014), Defendant had (and still has) a Netgear N600 wireless router that he installed himself. Doc. 54-2 at 11 (Rog 5).

20. In or about February 2014, after an extended family trip out of the country, Defendant removed the password for the 2.4 Ghz band to make it an open guest network. Doc. 54-2 at 11 (Rog 5).

21. Once Defendant received notice from Comcast regarding this lawsuit, he replaced the password, changed the SSID, and disabled SSID broadcast. Doc. 54-2 at 11 (Rog 5).

22. Multiple people had access to the router within the alleged download period, including Defendant, his wife, at least four specific guests plus unknown persons within the range of the routers. (Doc. 54-2 at 13-14 (Rog 7).)

23. Throughout and since the alleged download period (March through June 2014), Defendant has resided in a multi-family condominium structure with six units to his building. Within the building, Defendant's unit is No. 3, and both left and right sides of Defendant's unit share a wall with Units 2 and 4. MSJ Exh. 4.

24. The condominium is built with all six units in a row, all facing the street, as such:

| **Unit 1** | **Unit 2** | **Unit 3** Defendant, his wife, and two infant children | **Unit 4** | **Unit 5** | **Unit 6** |
|---|---|---|---|---|---|
| *EAST ARAGON BOULEVARD* | | | | | |

25. During the time of the alleged downloads, Defendant's immediate next-door neighbors were the residents of Units 2 and 4. The couple who resided in Unit 2 in 2014 moved out in early 2015, and Defendant did not maintain contact with them. The gentleman was a mechanic, and he sometimes worked on cars in the garage, while his girlfriend would sit with her laptop in the garage. (Exh. 4.)

26. Various other people reside in the other units. In Unit 4, for instance, so many people have come and gone that Defendant is unsure as to who exactly resides there. In Unit 1, a family resides; Unit 5 had, during 2014, a young couple who no longer live there; and, in Unit 6, a man and his wife have resided. (Exh. 4.)

27. Because Defendant lives in such close proximity to other neighbors, wifi signals pass through the walls. (Exh. 4.)

28. Defendant made observations to detect whether other wifi signals could be detected from within his own unit. While he was in his kitchen and living room, and upstairs (and not next to a window or open door), Defendant viewed the network preferences of his computer and noticed that at least 12 wifi signals other than his own were visible. These signals had not been generated from within Defendant's unit and came from neighbors. Therefore, the walls of Defendant's condominium structure are such that wifi signals can pass through them. (Exh. 4.)

29. In an effort to determine whether the signal from his router could be detected from outside the walls of his condominium unit, Defendant carried his laptop computer outside and took it to various access points in front of, beside, and behind his unit, and at each point examined his computer's network preferences. Defendant observed that his his signal was accessible from various access points at all sides of his home, which indicates that the signal would also be accessible within the units directly adjacent to Defendant's home, with the very units with which Defendant shares walls. (Exh. 4.)

30. Defendant even went as far as to download an application called NetSpot, which is used to test WiFi signal strengths. He then input the appropriate measurements into the application to detect the strength of his wifi from various access points. The wifi is measured in decibel-milliwatts, abbreviated "dBm." He made a screenshot of his

unit as well as various access points, where he had walked around outside, and attached the screenshot to his declaration (Exh. "4.")

31. Next, none of the Plaintiff's evidence can connect the alleged downloads to Defendant anymore than it can connect them to any other person who had access to IP address 98.249.146.169.

32. Defendant pays for the Internet at his location. "[T]he assumption that [Defendant,] the person who pays for Internet access . . . is the same individual who allegedly downloaded . . . [Plaintiff's] sexually explicit film[s] is tenuous." *Bubble Gum Prods.*, 2012 Copr. L. Dec. P 30292 (quoting *In re BitTorrent Adult Film Copyright Infringement Cases*, 2012 WL 1570765, at *3 (E.D.N.Y. May 1, 2012).

33. An IP represents nothing more than a router or gateway through which other devices connect. These devices may have their own MAC or private IP addresses that are not visible to outside Internet users. *Malibu Media, LLC v. Doe*, 0:14-CV-60259-UU, 2014 WL 2615351, at *2, n. 2 (S.D. Fla. 2014). The router used by Defendant has a "Network Address Translation Firewall, which conceals behind it the devices that would be connected to the router. Therefore, none of Plaintiff's evidence presented shows which computer, if any, downloaded the videos in question." Exh. "7" at 9 ¶ H.

34. Plaintiff's only evidence links the *IP address*, not Defendant, to the alleged downloads of Plaintiff's videos, and the IP address does not identify a particular computer or individual.

35. Plaintiff "produce[d] all documents it intends to use at trial which it will rely upon to conclude Defendant was

the individual who infringed Plaintiff's works." MSJ Exh. 6 at 14.

36. The data files that Plaintiff produced that are related to Plaintiff's videos — the PCAPs and spreadsheets and reports based on them — identify only an IP address, 98.249.146.169, as allegedly downloading Plaintiff's films. They have no information or data that can identify a specific computer or individual. *See, e.g.*, MSJ Exh. 7 at 8 ("none of Plaintiff's evidence presented shows which computer, if any, downloaded the videos in question").

37. Here, Plaintiff's investigators did not detect any specific computer device. MSJ Exh. 7 at 9 ¶ H.

38. Even if Plaintiff could prove that the downloads were caused from IP address 98.249.146.169, Plaintiff still would not be able to prove that Defendant was the individual who downloaded that video.

39. Plaintiff produced a document it refers to as the "Additional Evidence." It is a list of alleged downloads from IP address 98.249.146.169 that have nothing to do with Plaintiff's videos, and which appear to have been downloaded at various times and dates different from times and dates. *See* Doc. 8, ¶¶ 24-27.

40. The "additional evidence" is only a list. It had "no accompanying PCAP data, no torrent file, no copy of the video, nor any other accompanying data." MSJ Exh. 7 at 9.

41. One of the items on the "Additional Evidence" appears to be a Beethoven's 5th Symphony, which is the most well-known piece of classical music of all time.

42. Defendant may "like" Beethoven classical music; however, he did not download any Beethoven works via BitTorrent, and Plaintiff has no evidence that he did.

43. Even, *arguendo*, if Defendant did download a Beethoven symphony via BitTorrent (which he did not), doing so would have nothing to do with Plaintiff's pornographic videos.

44. Plaintiff's videos do not incorporate Beethoven's classical music, and Beethoven has nothing to do whatsoever with Plaintiff's pornography.

45. The items on the "Additional Evidence" list could have been downloaded by any possible combination of individuals or computers accessing the router.

46. "The additional evidence is not specific to one computer on IP address 98.249.146.169." MSJ Exh. 3 at 8 RFA 30.

47. "The alleged downloads and/or the 'additional evidence' could have been downloaded from more than one computer connected to IP address 98.249.146.169." MSJ Exh. 3 at 7, RFA 22.

48. "The additional evidence was downloaded from more than one computer connected to IP address 98.249.146.169." MSJ Exh. 3 at 8 RFA 31.

49. Plaintiff has no evidence beyond speculation that Defendant is the individual who downloaded the additional evidence files. Therefore, even if, *arguendo*, Plaintiff could prove that Defendant downloaded all the videos on the list of additional evidence (which he did not), such proof would not prove that Defendant downloaded Plaintiff's completely unrelated and separate pornographic films on completely separate occasions.

50. Plaintiff's evidence does not even show that an entire video was downloaded. At best, Plaintiff only has evidence that an unusable *piece* of movie was copied by a computer connected to IP address 98.249.146.169.

51. Plaintiff's data — in the form of a "PCAP" or "pocket capture" for each video — is "not representative of an entire video and does not contain sufficient data to show that an entire video was transferred." MSJ Exh. 7 at 4.

52. For *Hot Orgasm*, file hash the associated PCAP files produced by Plaintiff demonstrate that Plaintiff only detected Defendant's public IP address allegedly transferring *one piece* of a file, as opposed to an entire movie. the total size equaling 67KB. MSJ Exh. 7 at 4.

53. The copy of *Hot Orgasm* produced by Plaintiff has a total file size of 441.2MB. Comparatively speaking, Plaintiff's PCAP, which is Plaintiff's only evidence of recording any downloading of *Hot Orgasm* from IP address 98.249.146.169, is only 0.015% the size of the actual film. Thus, Plaintiff only has evidence that a fragment of its video was downloaded from IP address 98.249.146.169. MSJ Exh. 7 at 4.

54. Because the PCAP only includes data for one piece, it does not include enough data to correspond to an entire video file. For a torrent file to be viewable, it needs all of the torrent pieces. *See, e.g.*, Doc. 8, ¶ 13 ("After the infringer receives all of the bits of a digital media file, the infringer's BitTorrent client software reassembles the bits so that the file may be opened and utilized.")

55. Copying a single piece of a torrent is not the same thing as copying an entire video file. MSJ Exh. "7" at 5. For a movie to be watchable, it needs all the pieces.