United States District Court,
W.D. Pennsylvania.
UNITED STATES of America,
v.
Richard STANLEY, Defendant.

Nov. 14, 2012.

2012 WL 5512987

MEMORANDUM OPINION AND ORDER

CONTI, District Judge.

***1** Pending before the court is a motion to suppress evidence seized during a search of the home and computer of Richard Stanley ("Stanley" or "defendant") on January 19, 2011, and statements made by Stanley subsequent to that search. (ECF No. 24.) On November 9, 2011, a federal grand jury in the Western District of Pennsylvania returned a one-count indictment charging Stanley with possession of child pornography in violation of 18 U.S.C. § 2252(a) (4)(B). (ECF No. 1.) On December 1, 2011, he pleaded not guilty to count one of the indictment. (ECF No. 17.) On April 13, 2012, Stanley filed a motion to suppress evidence and statements made by him. (ECF No. 24.) The government filed a response to defendant's motion to suppress on April 27, 2012. (ECF No. 26.) Defendant filed a reply brief to the government's response to defendant's motion to suppress on May 11, 2012. (ECF No. 27.) Defendant filed a supplemental brief with respect to the motion to suppress on May 23, 2012. (ECF No. 28.)

On May 24, 2012, the court held a hearing with respect to defendant's motion to suppress. (ECF No. 29.) The court heard testimony from Cpl. Robert Erdely (retired) of the Pennsylvania State Police ("Erdely") and exhibits were entered into evidence. The court ordered the parties to file proposed findings of fact and conclusions of law. The proposed findings of fact and conclusions of law were filed on August 6, 2012. (ECF Nos. 36 and 37.) Defendant filed a reply to the government's proposed findings of fact and conclusions of law on August 8, 2012. (ECF No. 38.) The government filed a response to defendant's proposed findings of fact on August 14, 2012. (ECF No. 39.) Defendant filed a reply brief on August 28, 2012. (ECF No. 41.)

After reviewing the parties' submissions and considering the evidence presented at the suppression hearing on May 24, 2012, the court determined additional evidence was required to decide the issues presented by defendant's motion to suppress. On August 24, 2012, the court reopened the record and continued the suppression hearing for the parties to present additional evidence with respect to the issues contained in the court's order, dated August 24, 2012. (ECF No. 40.) At the continued suppression hearing on October 15, 2012, the court heard testimony from Erdely and exhibits were entered into evidence. After considering the parties' submissions and the evidence and testimony presented at the suppression hearings, the court makes the following findings of fact and conclusions of law:

I. *Findings of Fact*

Erdely's Use of the Moocherhunter™

1. On November 11, 2010, Erdely, the head of the computer crime unit of the Pennsylvania State Police ("PSP"), was investigating the distribution of child pornography files over peer-to-peer file-sharing networks on the internet. (5/24/2012 Tr. at 6–7.)

2. As the head of the computer crime unit, Erdely ran the statewide computer crime task force and was responsible for a twenty-six member unit. Erdely also handled his own caseload investigating internet crimes involving the sexual exploitation of children. Erdely served as an instructor in online investigations for the Internet Crimes Against Children Task Force, and his training included various computer crime conferences and numerous Microsoft, Cisco, and computer forensics certifications. (*Id.* at 5–6; Gov't's Ex. 8, ¶ 2.)

***2** 3. During Erdely's online investigation on November 11, 2010, he discovered a computer sharing seventy-seven files (the "subject computer") on the Gnutella network, which runs various file-sharing programs and allows users to share files between their computers. (5/24/2012 Tr. at 6.)

4. Erdely suspected at least twenty-two of the seventy-seven files were child pornography based on the files' titles. Erdely was able to confirm with certainty that several of the seventy-seven files contained child pornography. (*Id.* at 8, 11; Gov't's Ex. 8, ¶ 19.)

5. Law enforcement officials maintain an electronic database of files containing child pornography recovered from criminal investigations. The files maintained in the database have unique identifiers called hash values. Erdely found that the hash values of several of the files on the subject computer were identical to the hash values of the files

in the law enforcement child pornography database. Based on this information, Erdely concluded that the subject computer was sharing child pornography on the Gnutella network. (5/24/2012 Tr. at 8, 11; Gov't's Ex. 8, ¶ 20.)

6. Each computer which accesses a file-sharing program on the Gnutella network is assigned a globally unique identification ("GUTD") that stays with the computer even after a particular file-sharing session is completed. Erdely identified the GUTD of the user sharing the seventy-seven files as "8754E6525772BA0134C4C6CACF12E300" ("300 GUID"). (5/24/2012 Tr. at 9; Gov't's Ex. 8, ¶ 17.)

7. Erdely identified that the subject computer was using an internet protocol address ("IP address"), of "98.236.6.174" (the "174 IP address"). An IP address is a number assigned to a modem when it connects to the internet. Every modem that connects to the internet has a unique IP address. When users share an internet connection through the use of a wireless router, the wireless devices, such as a computer, which are connected to the internet through the wireless router, are assigned private IP addresses, which are not disclosed to the public. All users connected to the internet via the wireless router use the public IP address of the modem the wireless router is connected to in order to communicate on the internet.[FN1] (5/24/2012 Tr. at 8–9; Gov't's Ex. 8, ¶ 17.) The only persons that can view the private IP addresses are those persons that are able to access the wireless router's configuration, i.e. those whose devices are connected to the wireless router. (*See* ¶ 13 *infra.*) Unlike GUIDs, IP addresses can be reassigned and do not always stay the same for a particular modem. (5/24/2012 Tr. at 8–9; Gov't's Ex. 8, ¶ 17.)

FN1. When a person whose device, such as a computer, is connected to the internet via a wireless router visits a webpage, the public IP address of the modem the wireless router is connected to would be visible via that webpage's server. The private IP address assigned to that person's device by the wireless router would not be visible via the webpage's server. Erdely testified: "Private IP addresses can be seen by other private IP addresses behind the router, and public IP addresses can typically be seen from anywhere in the world, because they are globally routed." (10/15/12 Tr. at 28–29.)

8. Erdely searched publically available records and determined the 174 IP address assigned to the subject computer through which the Gnutella network was accessed was subscribed to through Comcast

Cable (“Comcast”). On November 11, 2010, Erdely obtained a court order directing Comcast to identify the subscriber of the 174 IP address. (5/24/2012 Tr. at 6, 8–9, 11–12; Gov't's Ex. 8 ¶ 21.)

***3** 9. Comcast identified that on November 11, 2010, the 174 IP address was assigned to William Kozikowski (“Kozikowski”) in Allegheny County. Comcast provided Erdely with Kozikowski's home address in Allegheny County. (5/24/2012 Tr. at 12; Gov't's Ex. 8 ¶ 21.)

10. Based on the information provided by Comcast, Erdely obtained and executed a search warrant for Kozikowski's home. Erdely found two computers in the home, but concluded that neither was the subject computer because neither computer contained internet file-sharing software with the 300 GUID. (5/24/2012 Tr. at 12–13.)

11. Erdely learned that Kozikowski used a wireless router in his home to connect his computers to the internet. (*Id.*at 13, 30.)

12. Comcast provides internet service through a coaxial cable that is run into the subscriber's home. The coaxial cable is physically connected to a modem inside the subscriber's home. A wireless router is connected to a modem via a cable. The wireless router is located within a small box and allows multiple devices, e.g. computers, to connect to the internet. Through the modem, the multiple devices share one public IP address, and may or may not have a physical connection to the wireless router. Once the wireless router is connected to the modem, computers equipped with wireless technology can detect the wireless router and send signals to and receive signals from that router in order to connect to the internet. A computer can also connect to the wireless router via a cable. (10/15/12 Tr. at 3–5.)

13. In Kozikowski's house, one computer was connected to the wireless router via a cable, while another computer was connected to the wireless router via a signal. (10/15/12 Tr. at 3–5, 10–11.)

14. The wireless router may be secured, meaning a password is required to access the wireless router, or may be unsecured, meaning a password is not required to access the wireless router to connect to the internet. (*Id.*) Erdely found Kozikowski's internet connection was unsecured; thus, it did not require users to enter a username and password before connecting to the internet via Kozikowski's internet connection. Kozikowski informed Erdely that he had not given anyone

outside his home permission to use his internet connection. (5/24/2012 Tr. at 13, 30.)

15. A password is required, however, for a person to view the wireless router's settings or to examine the information stored on the wireless router. This information included, among other things, the router's settings, detailed information about the devices connected to the wireless router, and the private IP addresses it assigned to those devices. This information is stored on the wireless router and even if the wireless router is powered down, the information remains stored on the wireless router. (10/15/12 Tr. at 7, 9.) To view the wireless router's settings or to examine the information stored on the router, a user must open a web page on his or her computer and type the wireless router's IP address into the address bar. The user must then enter a password. Once a user correctly enters the password, the wireless router's settings and other information stored on the wireless router are displayed on the web page. (10/15/12 Tr. at 8.)

***4** 16. Computers [FN2] are generally equipped with wireless technology, sometimes referred to as a "wireless card," which enables them to connect to a wireless router. A computer user can view information about his computer's wireless technology by clicking an icon located on his computer screen. [FN3] This wireless technology is assigned a unique serial number called a MAC address. When computers are powered on, and assuming the wireless technology is not turned off, the wireless technology sends out a signal to search for wireless routers within a certain range of the computer. Each wireless router has a name, and when the user clicks on the wireless technology icon on his computer screen, the names of available wireless routers within the computer's range appear in a list on the computer screen. To connect to one of those wireless routers, the user clicks on that wireless router's name and is prompted to connect to that wireless router. (10/15/12 Tr. at 13–14 .) If the wireless router is secured, the user will have to enter a password to connect to that wireless router. If the wireless router is not secure, the user can connect to the wireless router without entering a password. (*Id.* at 21.)

FN2. This description refers specifically to Windows and Apple based operating systems. (10/15/12 Tr. at 12.) Stanley was using an Apple based operating system. (*Id* at 62.)

FN3. For Windows based operating systems, the wireless connection icon is at the bottom of the screen. For Apple based operating systems, the wireless connection icon is at the top of the screen. (10/15/12 Tr. at 14.)

17. A person must take those affirmative steps to connect his or her computer to a wireless router. (10/15/12 Tr. at 14, 27, 62.) Stanley had to follow that process to connect his computer to Kozikowski's wireless router. (10/15/12 Tr. at 62.)

18. Once a computer is connected to the wireless router, it is assigned a private IP address. The private IP address is used to identify the devices connected to the internet via that wireless router. Each device connected to the wireless router has a different private IP address. Private IP addresses are only used by the wireless router and are not revealed to third parties on the internet. All devices connected to the modem share the modem's public IP address. The public IP address is disclosed to third parties to facilitate the user's interactions on the internet. (5/24/2012 Tr. at 8–9; 10/15/12 Tr. at 15–16.)

19. Following Erdely's initial investigation of Kozikowski's home and computers, Kozikowski left his wireless router unsecured and allowed Erdely to place a computer in his home and connect it to his wireless router. Erdely had access through that computer to the wireless router's settings, which provided, among other things, the public IP address the wireless router was using, the private IP addresses the wireless router assigned to any devices connected to that wireless router, and the MAC address of any of those devices connected to the wireless router. This set-up allowed Erdely to continue his investigation of the person using Kozikowski's wireless router to share and view child pornography. (*Id* at 13–14.)

20. Law enforcement officials have a computer system that allows investigators to record the results of their investigations of child pornography crimes to share with law enforcement officials in other states. (10/15/12 Tr. at 41, 80.)

***5** 21. On January 19, 2011, Erdely was using this computer system while in Harrisburg, Pennsylvania to view the search results of other law enforcement officials' investigations of child pornography crimes. These search results updated every thirty minutes to include the results of the most recent investigations. (*Id.*) Erdely learned two other computer crime investigators, Jessica Eger ("Eger"), an employee of the Pennsylvania Attorney General's Office and Paula Hoffa ("Hoffa"), an investigator with the Hartland Police Department, each identified a computer sharing child pornography that had the same 300 GUTD as the subject computer identified by Erdely. (5/24/2012 Tr. at 17–18; Gov't's Ex. 8 ¶ 21 .)

22. Eger's investigation that identified the 300 GUTD sharing child pornography took place at 9:50 a.m. on January 19, 2011. (5/24/2012 Tr. at 23, 24, 66; Gov't's Ex. 8 ¶ 21.)

23. Hoffa's investigation that identified the 300 GUTD sharing child pornography took place at 3:19 p.m. on January 19, 2011. (Gov't's Ex. 8 ¶ 21.)

24. Hoffa reported the public IP address of the user sharing child pornography was "98.239.133.215" (the "215 IP address"). (Id,)

25. After Erdely learned about Eger's and Hoffa's investigations, he logged into the computer located at Kozikowski's residence from his computer in Harrisburg, Pennsylvania and examined the configuration of Kozikowski's wireless router. (5/24/2012 Tr. at 22; 10/15/12 Tr. at 46–47; Gov't's Ex. 8 ¶ 21.)

26. Erdely learned that the 215 IP address was assigned to Kozikowski's wireless router. Erdely examined the logs on Kozikowski's wireless router, which revealed there was a computer connected to that router with a private IP address of "192.168.2.114" (the "114 IP address") and the computer's MAC address was "mac=00–lC–B3–B4–48–95" (the "95 MAC address"). (5/24/2012 Tr. at 22–24; Gov't's Ex. 8 ¶ 21.)

27. An online search of the prefix "mac" of the 95 MAC address identified that the wireless networking card was an Apple wireless device, which led Erdely to believe the computer using the private 114 IP address was an Apple computer. Neither computer in Kozikowski's home was an Apple computer. (5/24/2012 Tr. at 20, 24; Gov't's Ex. 8 ¶ 21.)

28. Erdely learned from his review of the Kozikowski's wireless router's configuration that the computer assigned the private 114 IP address was using port 6346 to interact with other devices assigned IP addresses. (5/24/2012 Tr. at 23–24; 10/15/12 Tr. at 63–64; Gov't's Ex. 8 ¶ 21.)

29. Ports are channels of communication on the internet. There are 65,536 available ports. The first 1,023 of these ports are well-known ports and are set aside for particular internet traffic, such as viewing a webpage (port 80), sending email (port 25), or receiving email (port 110). (10/15/12 Tr. at 31.) There are other ports, starting with port 1,024, that are registered ports. The Internet Assignment Number Authority (the "IANA") is responsible for, among other things, registering ports. The Gnutella network registered port 6346 with the IANA, and it is one of the most common ports used to access the Gnutella network. (*Id.*) Even though a port is registered, it can still be used for internet activity not associated with its registering network, meaning that a computer could use port 6346 without accessing the Gnutella network. (*Id* at 31–33, 70.)

***6** 30. In Erdely's experience investigating child pornography crimes, he saw port 6346 being consistently used by persons via their computers to view and share child pornography by accessing the Gnutella network. (*Id.*)

31. At some point after Erdely learned about Eger's and Hoffa's investigations, looked at the configuration of Kozikowski's wireless router, and called Eger and Hoffa to confirm their search results, he drove from Harrisburg, Pennsylvania to Kozikowski's residence in Allegheny County, Pennsylvania. (5/24/2012 Tr. at 25–26; 10/15/12 Tr. at 47–48.)

32. Erdely called Craig Haller, an Assistant United States Attorney ("Haller"), to determine whether it was appropriate to use a program called Moocherhunter™ to locate geographically the computer assigned the 114 IP address. (5/24/2012 Tr. at 25–26.) After Erdely called Haller, he decided to use Moocherhunter™ to locate the subject computer. (*Id.*)

33. Erdely had previously received a few minutes of training on the use of Moocherhunter™ by Cpl. Jon Nelson of the PSP.[FN4] (*Id,* at 32, 70.)

FN4. Cpl. Jon Nelson retired from the PSP prior to January 19, 2011. Cpl. Jon Nelson was not retired when he trained Erdely on the use of Moocherhunter™. (5/24/2012 Tr. at 32.)

34. Erdely used a free version of Moocherhunter™, which is available on the manufacturer's website. (5/24/2012 Tr. at 32–34, 83; Gov't's Ex. 1.)

35. According to the manufacturer's website:

> Moocherhunter™ is a free mobile tracking software tool for the real-time on-the-fly geo-location of wireless moochers, hackers and users of wireless networks for objectionable purposes (e .g. paedophile activity, illegal file downloading, illegal music/video sharing, etc.)”
>
> ...
>
> Moocherhunter™identifies the location of an 802.11–based wireless moocher or hacker by the traffic they send across the network. If they want to mooch from you or use your wireless network for illegal purposes (e.g. warez downloading or illegal filesharing), then they have no choice but to reveal themselves by sending traffic across in order to accomplish their objectives. Moocherhunter™ enables the owner of the wireless network to detect traffic from this unauthorized wireless client (using either Moocherhunter™'s Passive or Active mode) and enables the owner, armed with a laptop and directional antenna to isolate and track down the source.

(5/24/2012 Tr. at 33; Gov't's Ex. 1.) [FN5]

[FN5] FN5. The manufacture of Moocherhunter™ also manufactures a law enforcement edition of the software, which is available for purchase. Erdely did not use the law enforcement edition of the software. (5/24/2012 Tr. at 32–34, 83; Gov't's Ex. 1.)

36. Moocherhunter™ has an active mode and a passive mode. At all times during his investigation, Erdely used Moocherhunter™ in the passive mode. In the passive mode, the user of Moocherhunter™ enters the MAC address of a wireless router that is connected to a wireless device and traces the signal of that wireless device from the wireless router back to its source. In active mode, the user of Moocherhunter™ searches for wireless routers to determine whether the wireless device being searched for is connected to that wireless router. Once the Moocherhunter™ connects to a wireless router, it can trace the signal of any wireless devices, e.g. computers, connected to that wireless router. In either mode, the wireless device, e.g. a computer, must be connected to a wireless router for Moocherhunter™

to be able to trace the signal of the wireless device. (10/15/12 Tr. at 23, 25–26.)

***7** 37. The ability of Moocherhunter™ to trace a signal of a wireless device, such as a computer, back to the wireless device is dependent upon a connection between the wireless device and the wireless router. Moocherhunter™ cannot cause a computer to send a signal that it is not otherwise already emitting. If the person accessing Kozikowski's wireless router with the 95 MAC address had terminated his connection with the wireless router, Moocherhunter™ could not have located the origin of that signal. (*Id* at 24.)

38. Erdely arrived at the Kozikowski residence during the evening of January 19, 2011. (5/24/2012 Tr. at 30.)

39. To use Moocherhunter™, Erdely downloaded the Moocherhunter™ software to his laptop, connected a directional antenna to his laptop, and used a USB wireless card to connect to Kozikowski's wireless router. (5/24/2012 Tr. at 81; Gov't's Ex. 1.)

40. Erdely knew the MAC address of Kozikowski's wireless router's MAC address. This information enabled him to identify Kozikowski's wireless router with Moocherhunter™ and trace the 95 MAC address that was connected to Kozikowski's router to its origin—Stanley's computer. (10/15/12 Tr. at 23.)

41. To track the signal, Erdely pointed the directional antenna at Kozikowski's wireless router in Kozikowski's home and found the signal of the 95 MAC address. Erdely began to follow the signal from Kozikowski's wireless router to the source of the signal, i.e. the computer assigned the 114 IP address. (5/24/2012 Tr. at 62–63, 88–89.)

42. The Moocherhunter™ provides a reading that indicates how close the user of the software is to the source of a signal, with 100 being the highest possible reading. Erdely followed the signal from Kozikowski's wireless router and pointed the antenna across the street from Kozikowski's residence.

43. Kozikowski's residence is directly across the street from Stanley's residence. There are sidewalks and trolley tracks between the two buildings in which their residences are located. Stanley's residence is one unit in an apartment complex comprised of six units. There are four ground units and two upper level units in the apartment

building. Stanley's apartment was a ground unit. There are two ground units to the left of Stanley's apartment and one ground unit to the right of Stanley's apartment. The two ground units to the left of Stanley's residence are set farther back from the trolley tracks and Kozikowski's home than Stanley's unit and the fourth ground unit. There is a door between Stanley's unit and the fourth ground unit. That door led to the two units located on the upper level. (5/24/2012 Tr. at 55–57; 89–92; Gov't's Exs. 5, 6, 7; Def's Exs. A, B, C.)

44. When Erdely pointed the antenna across the street toward the apartment building in which Stanley resided, the meter reading was 67. Erdely continued to follow the signal, left the Kozikowski residence, and walked across the street to the sidewalk in front of the apartment building in which Stanley's unit was located. (5/24/2012 Tr. at 28–29; Gov't's Ex. 8, ¶ 21.)

***8** 45. Erdely saw the apartment building had a door to the left, which turned out to be Stanley's residence, and two doors to the right. The door closest to Stanley's door led to stairs to two second floor apartments. The other door led to another ground floor unit. When Erdely pointed the antenna to the second floor apartments, the meter reading on his laptop weakened. (5/24/2012 Tr. at 28–29.)

46. When Erdely stood on the sidewalk in front of Stanley's residence and pointed the antenna toward the front door of that residence, the meter reading was 100. When Erdely pointed the antenna to the left or right of Stanley's residence, the meter reading weakened. Based on the Moocherhunter™'s readings, Erdely determined the signal from the computer assigned the 95 MAC address to connect to Kozikowski's wireless router was emanating from Stanley's residence. (5/24/2012 Tr. at 28–29, 68, 81; Gov't's Ex. 8, ¶ 21.)

47. After the meter reading reached 100, Erdely stopped using Moocherhunter™, authored an affidavit of probable cause, and obtained a search warrant for Stanley's residence (the "Stanley search warrant"). (5/24/2012 Tr. at 29.)

The Stanley Search Warrant

48. The Stanley search warrant is part of a twelve-page document, which included a two-page application for search warrant and authorization. (Gov't's Ex. 8.)

49. The affidavit of probable cause executed by Erdely (the “affidavit”), which was attached to the application for search warrant and authorization, provided, among other things, that Erdely was assigned to the Bureau of Criminal Investigation, Computer Crime Division. (Gov't's Ex. 8, ¶ 2.) The affidavit contained a list of seventeen training courses Erdely attended and seventeen of his computer-based training certifications. In the affidavit, Erdely stated:

> As part of my duties I investigate violations of state law, including the online exploitation of children, particularly in relation to violations of Title 18, Section 6312 which criminalize, among other things, the possession, receipt and transmission of child pornography. I have gained expertise in the conduct of such investigations through training in seminars, classes, and everyday work related to conducting these types of investigations. I have attended numerous computer crime conferences over the past nine years. I have also been trained in the investigation of persons using the Gnutella network, more specifically, “LimeWire/4.18.8 (Cabos/0.8.2)”. Also, I have participated in the execution of more than one hundred search warrants related to computer crimes, the majority of which have involved child exploitation and/or child pornography offenses. I have testified in both State and Federal Court as an expert in Online Investigations.

(Gov't's Ex. 8, ¶ 2.)

50. In the affidavit, Erdely noted that Cpl. Jon Nelson trained him in the use of Moocherhunter™. The affidavit does not contain a reference to such training lasting a few minutes. (Gov't's Ex. 8, ¶ 21.)

***9** 51. The affidavit cause does not contain a statement that this was the first time Erdely used Moocherhunter™ in an investigation.

52. The affidavit contained a detailed description of the Gnutella network and how persons interested in obtaining child pornographic images use the Gnutella network, specifically LimeWire, to share and view child pornography. (Gov't's Ex. 8, ¶ 11–16.)

53. The affidavit described Erdely's initial online investigation, which took place on November 11, 2010, and how he learned the 300 GUID was sharing seventy-seven files of child pornography via LimeWire. He described LimeWire as follows:

> A growing phenomenon on the Internet is peer to peer file sharing (P2P). P2P file sharing is a method of communication available to

> Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up file(s) on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, and conducting a search for files that are of interest and currently being shared on the network. LimeWire, one type of P2P software, sets up its searches by keywords. The results of a keyword search are displayed to the user. The user then selects files(s) from the results for download. The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file.

(Gov't's Ex. 8, ¶ 11.)

54. In the affidavit, Erdely recounted how he determined the IP address associated with the 300 GUID was assigned to Kozikowski and that he determined Kozikowski's computers were not sharing or viewing child pornography. The affidavit described that Kozikowski's wireless router was not password-protected, meaning it could be accessed by persons outside Kozikowski's home. (Gov't's Ex. 8, ¶ 17, 21.)

55. The affidavit contained the information that Erdely received from Hoffa's and Eger's investigations. (Gov't's Ex. 8, ¶ 21.)

56. With respect to Hoffa's investigation, the affidavit described that on January 19, at 3:19 p.m., Hoffa was investigating the Gnutella network and discovered the 300 GUID was sharing child pornography using the 215 IP address. (*Id.*) Erdely mistakenly indicated that Hoffa's investigation occurred on January 19, 2010. Erdely realized at a later date that the affidavit should have referred to Hoffa's investigation occurring on January 19, 2011. (5/24/2012 Tr. at 59.)

57. With respect to Eger's investigation, the affidavit describes that on January 19, at 9:50 a.m., the 300 GUID was sharing child pornography. (Gov't's Ex. 8, ¶ 21.)

58. In the affidavit, Erdely explained that the 215 IP address was assigned to Kozikowski, and that Kozikowski gave Erdely permission to access his wireless router to continue his investigation of the person

sharing child pornography via Kozikowski's unsecured wireless router. (*Id.*) Erdely explained:

***10** There are logs on the router which shows [sic] the serial number of the wireless card which is attached to is [sic] and what the internal (private) IP address is that it assigned to the modem. There was a user with IP address 192.168.2.114 assigned to it which has a serial number (MAC Address) of mac=00–lC–B3–48–95.

(Gov't's Ex. 8, ¶ 21.)

59. In the affidavit, Erdely described his use of the Moocherhunter™:

This officer used a publically available tool to locate the MAC address which was attached to the Kozikowski's wireless internet. The tool is “moocherhunter” [sic]. It has a power meter which shows the strength of the wireless signal assicated [sic] with a particular MAC address (serial to a wireless card). I pointed it across the street from the Kozikowski's residence and it initially rose to a level of 67. As I walked toward this apartment building, the signal grew stronger.

(Gov't's Ex. 8, ¶ 21.)

The apartment building has two upstairs residence [sic] and then one down stairs [sic] residence in the vicinity to where I was pointing the antenna. There were only stairs leading up to the apartments next to apartment 1481. The only apartment in the vicinity to the direction I was pointing the antenna, was 1481.

(Gov't's Ex. 8, ¶ 21.) In the Application for Search Warrant and Authorization, Erdely described Stanley's residence as follows:

A two story brick residence with an unenclosed front porch. There are steps leading up to the porch with [sic] It is marked on the front of the building 1481.

(Gov't's Ex. 8 at 1.)

60. In the affidavit, Erdely provided a description of how he used Moocherhunter™ to form the opinion that the computer sharing the child pornography was located in the Stanley residence:

As I pointed to the front door of the apartment, the signal grew to 100 which is the strongest signal which can be reported. I have been trained in the use of this technology by Cpl. Jon Nelson (retired). It is my opinion that the location of the computer sharing the child pornography on all of the afforementioned [sic] dates and times is 1481 Dormont Ave, Pittsburgh, the residence to be searched. The router also showed that this IP address was communicating on a port know [sic] to this officer to be used by clients downloading files over this file sharing network.

(Gov't's Ex. 8, ¶ 21.)

61. Based upon the affidavit, at 9:20 p.m. on January 19, 2011, a district justice issued a search warrant for Stanley's residence. (Gov't's Ex. 8 at 1.)

62. Erdely executed the Stanley search warrant on January 19, 2011. Based on the evidence obtained from the search of Stanley's home and computer, he was indicted for possessing visual depictions of minors engaged in sexually explicit conduct on November 9, 2011. (ECF No. 1.) Stanley asserts that the evidence obtained from that search should be suppressed because it was obtained in violation of the Fourth Amendment to the United States Constitution.

II. Conclusions of Law

*11 Erdely's Use of the Moocherhunter™

1. As a general rule, the burden of proof is on the defendant who seeks to suppress evidence. *United States v. Johnson,* 63 F.3d 242, 245 (3d Cir.1995). Once the defendant establishes a basis for his motion, "the burden shifts to the government to show that the search or seizure was reasonable." *Id.*

2. The Fourth Amendment to the United States Constitution provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures ...". U.S. Const. amend. IV.

3. The Fourth Amendment generally requires police to secure a warrant supported by probable cause before conducting a search. *Maryland v. Dyson,* 527 U.S. 465, 466, 119 S.Ct. 2013, 144 L.Ed.2d 442 (1999) (citing *California v. Carney,* 471 U.S. 386, 390–91, 105 S.Ct. 2066, 85 L.Ed.2d 406 (1985)).

4. The test for determining whether a search has occurred was set forth in *Katz v. United States,* 389 U.S. 347, 360, 88 S.Ct. 507, 19

L.Ed.2d 576 (1967). The *Katz* inquiry "posits a two-part inquiry: first, has the individual manifested a subjective expectation of privacy in the object of the challenged search? Second, is society willing to recognize that expectation as reasonable?" *California v. Ciraolo,* 476 U.S. 207, 211, 106 S.Ct. 1809, 90 L.Ed.2d 210 (1986).[FN6]

FN6. Here, Stanley had a subjective and reasonable expectation of privacy in his home. The Supreme Court held in *United States v. Karo:*
[P]rivate residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant, and that expectation is plainly one that society is prepared to recognize as justifiable. Our cases have not deviated from this basic Fourth Amendment principle. Searches and seizures inside a home without a warrant are presumptively unreasonable absent exigent circumstances.

United States v. Karo, 468 U.S. 705, 714–15, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984).

Stanley did not, however, have an expectation of privacy in all the files on his computer. Although courts have recognized that "viewing and possessing child pornography is, by its nature, a solitary and secretive crime," *State v. Brennan,* 674 N.W.2d 200, 206 (Minn.App.2004), defendant could not have a subjective expectation of privacy in all the files on his computer as evidenced by his participation in the Gnutella network, which allowed other users on the Gnutella network, including Erdely, Eger, and Hoffa, to view and access, i.e. to share, certain files on his computer.

5. Here, the issue is whether a search occurred when Erdely used Moocherhunter ™ to follow the wireless signal being sent from and to the computer identified by the 95 MAC address in order to connect to Kozikowski's wireless router. More specifically, the court must determine whether Stanley had a legitimate expectation of privacy in the wireless signal he caused to emanate from the computer in his home to Kozikowski's wireless router and the wireless signal he received back from Kozikowski's wireless router in order to connect to the internet.

6. "[T]he test of legitimacy is not whether the individual chooses to conceal assertedly 'private' activity," but instead "whether the government's intrusion infringes upon the personal and societal values protected by the Fourth Amendment." *Ciraolo,* 476 U.S. at

212 (quoting *Oliver v. United States,* 466 U.S. 170, 181–83, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984.))

7. The Supreme Court of the United States has held that under the Fourth Amendment, there is no reasonable expectation of privacy in information voluntarily conveyed to third parties. *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *United States v. Miller,* 425 U.S. 435, 442, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976).

8. In *Smith,* the Supreme Court held the use of a pen register ("a mechanical device that records the number dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released") does not constitute a search within the meaning of the Fourth Amendment because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 736 n. 1, 743–44. The court found that the petitioner in that case "entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate' " because he voluntarily conveyed that information to a third party, i.e. the telephone company. *Id.* at 745.

***12** 9. In reaching its decision, the Court distinguished the facts before it from the facts in *Katz,* in which a government agent used an electronic listening device attached to a telephone booth to listen to the contents of a person's telephone call. *Id.* at 739–40 (citing *Katz,* 389 U.S. at 351–53). The Supreme Court in *Katz* found the use of the listening device constituted a search because listening to the contents of the telephone conversation violated the expectation of privacy relied upon when a person uses a telephone booth. *Id.*

10. In *Smith,* the Supreme Court found that (1) pen registers, unlike the listening device used in *Katz,* do not acquire the contents of the communication; and (2) a telephone user cannot have a reasonable expectation of privacy in the numbers dialed because they must "convey" phone numbers to the telephone company to complete a call. *Smith,* 442 U.S. at 742. The Court held, "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret." *Id.* at 743. The Court found:

When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.

Id. at 744.

11. Based upon *Smith's* rationale, the court finds Stanley did not have a legitimate expectation of privacy in the wireless signal he caused to emanate from his **computer** to the Kozikowski wireless router or in the signal being sent from the router back to his **computer**, and therefore, Erdely's use of Moocherhunter™ did not constitute a search in violation of the **Fourth Amendment**.
In *Smith,* the pen register was used to record the telephone numbers people voluntarily dialed and thus, conveyed, to the telephone company by monitoring electrical impulses caused when the dial on the telephone was released. Here, Moocherhunter™ monitored the strength of a signal that Stanley voluntarily caused to send from his computer to Kozikowski's wireless router and to receive a signal back from the wireless router in order to gain unauthorized access to Kozikowski's internet connection. In both cases, the party seeking suppression of evidence assumed the risk that information disclosed to a third party may be turned over to the police. Notably, Moocherhunter™, like the pen register, did not reveal the contents of the communications; it only revealed that communications were taking place.

12. The court finds that Stanley did not have a reasonable expectation of privacy in the wireless signal he caused to emanate from his computer to Kozikowski's wireless router or the wireless signal he received from Kozikowski's wireless router in order to connect to the internet. The information logged on that wireless router was accessible to Kozikowski and through his consent, to Erdely. This information showed the private IP address of Stanley's computer. Stanley, therefore, could have no reasonable expectation of privacy in the signal he was sending to or receiving from Kozikowski's wireless router in order to connect to the internet. An internet subscriber does not have a reasonable expectation of privacy in his IP address or the information he provides to his Internet Service Provider, such as Comcast, in order to legally establish an internet connection, and likewise, a person connecting to another person's wireless router does not have an expectation of privacy in that connection, i.e. the private IP address, when it is available to that third person and anyone with whom that person shares the information.

***13** 13. "[F]ederal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties." *United States v. Christie,* 624 F.3d 558, 543–74 (3d Cir.2010) (citing *United States v. Bynum,* 604 F.3d 161, 164 (4th Cir.2010); *United States v. Perrine,* 518 F.3d 1196, 1204 (10th Cir.2008); *Guest v. Leis,* 255 F.3d 325, 336 (6th Cir.2001)).

14. The subscriber information, which the government may obtain from the Internet Service Provider ("ISP") without violating the Fourth Amendment, may "include information such as subscribers' names, **addresses,** birthdates, and passwords." *Guest,* 255 F.3d at 335 (emphasis added).

15. The Court of Appeals for the Third Circuit has held "no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs." *Christie,* 624 F.3d at 574(citing *United States v. Forrester,* 512 F.3d 500, 510 (9th Cir.2008)).

16. Federal courts have declined to find a reasonable expectation of privacy in an IP address despite the argument "that IP addresses and location information, paired with inferences, are 'intensely revealing' about the interior of their homes." *In re: § 2703(d),* 787 F.Supp.2d 430, 440 (E.D.Va.2011).

17. In *United States v. Wagers,* a district court commented:

[W]eb IP addresses do *not directly* reflect the geographic street address of the office, residence, or building from which an individual accesses his email and/or the internet. Instead, law enforcement officials must conduct research and rely upon the addresses and data provided by internet providers, such as AOL and Insight Communications, as well as billing addresses for those service providers and/or credit card companies.

United States v. Wagers, 339 F.Supp.2d 934, 939 (E.D.Ky.2004) *aff'd,* 452 F.3d 534 (6th Cir.2006). Government agents routinely involve ISPs to learn the name and addresses of subscribers of IP addresses at issue in the government's investigations. *See e.g. Christie,* 624 F.3d at 562; *United States v. Vosburgh,* 602 F.3d 512, 517 (3d Cir.2010); *United States v. Tracey,* 597 F.3d 140, 145 (3d Cir.2010); *United States v. Richardson,* 583 F.Supp.2d 694, 697 (W.D.Pa.2008).

18. Erdely followed that procedure in this case. Erdely discovered the 174 IP address assigned to the computer sharing child pornography, learned Comcast was the ISP of the 174 IP address, and obtained a court order directing Comcast to disclose the name and address of the subscriber of the 174 IP address at the time child pornography was being accessed. Erdely used this procedure to learn a computer was located inside Kozikowski's home and to obtain a search warrant based on probable cause that a computer located inside Kozikowski's home was being used to commit crimes involving child pornography.

***14** 19. Under *Smith* and its progeny, internet subscribers who use ISPs to connect to the internet from their homes do not have a reasonable expectation of privacy in their subscriber information or IP addresses because they have conveyed this information to third parties in order to connect to the internet. *See Smith,* 442 U.S. at 743–44. As illustrated in this case, this information may be used to learn the geographic location of the subscriber's home and that he has a computer inside of that home.

20. Based on the foregoing, society would not be willing to recognize that Stanley, who did not obtain Kozikowski's permission to use the internet connection,[FN7] had a reasonable expectation of privacy in the wireless signal he used to connect his computer to Kozikowski's wireless router.

[FN7] The government argues defendant's use of Kozikowski's internet connection constituted theft under 18 Pa. Cons.Stat. § 3926, which provides:
A person is guilty of theft if he intentionally obtains services for himself or for another which he knows are available only for compensation, by deception or threat, by altering or tampering with the public utility meter or measuring device by which such services are delivered or by causing or permitting such altering or tampering, **by making or maintaining any unauthorized connection, whether physically, electrically or inductively,** to a distribution or transmission line, by attaching or maintaining the attachment of any unauthorized device to any cable, wire or other component of an electric, telephone or cable television system or to a television receiving set connected to a cable television system, by making or maintaining any unauthorized modification or alteration to any device installed by a cable television system, or by false token or other trick or artifice to avoid payment for the service.

18 PA. CONS.STAT. § 3926 (emphasis added).

21. Even though that signal was sent from and to the inside of Stanley's home and revealed there was a computer inside of the home, no expectation of privacy existed. By connecting to Kozikowski's wireless router, Stanley exposed his wireless signal to a third party and assumed the risk that the signal would be revealed to the authorities. Like the defendant in *Smith* who dialed a telephone number from inside his home, Stanley cannot hide behind sending the signal from inside his home and claim he had a reasonable expectation of privacy in the signal.

22. Kozikowski, who purchased his internet connection, did not have a reasonable expectation of privacy in his IP address or subscriber information, which enabled Erdely to learn Kozikowski's home address and that he had a computer and internet connection inside his home. *See Christie,* 624 F.3d at 543–74; *Guest* 255 F.3d at 335. Stanley, who was using Kozikowski's internet connection without permission, does not have a reasonable expectation of privacy in the wireless signal he sent or received in order to connect to that internet connection, even if it led Erdely to know that he had a computer inside of his home. Kozikowski was a third party to whose wireless router that signal was voluntarily sent. Under those circumstances, society would not recognize a reasonable expectation of privacy in the signal.

23. Based on the foregoing, the court finds Erdely's use of the Moocherhunter ™ to trace the 95 MAC address wireless signal from Kozikowski's wireless router to the sidewalk in front of defendant's apartment was not a search of defendant's home.

24. Stanley argues that (1) Moocherhunter™ is a tracking device, and therefore, Erdely should have obtained a tracking device warrant before using the software; and (2) even if Moocherhunter™ is not a tracking device, its use constituted a search of Stanley's home under *Kyllo v. United States,* 533 U.S. 27, 40, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001).

25. Federal Rule of Criminal Procedure 41(b)(4) provides:

[A] magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both[.]

***15** FED. R.CRIM. P. 41(b)(4).

26. Provision (b)(4) was added to Rule 41 as part of the 2006 amendments. The commentary to the 2006 amendments with respect to (b)(4) provides:

> The amendment reflects the view that if the officers intend to install or use the [tracking] device in a constitutionally protected area, they must obtain judicial approval to do so. **If, on the other hand, the officers intend to install and use the [tracking] device without implicating any Fourth Amendment rights, there is no need to obtain the warrant.** *See, e.g., United States v. Knotts, supra,* where the officers' actions in installing and following tracking device did not amount to a search under the Fourth Amendment.

FED. R.CRIM.P. CMT. (2006) (emphasis added).

27. Because the court finds Stanley did not have a reasonable expectation of privacy in the wireless signal he caused to emanate from his computer to connect to Kozikowski's wireless router, his Fourth Amendment rights were not implicated by Erdely's use of Moocherhunter™. It follows that even assuming for the sake of argument that Moocherhunter™ is a tracking device, a tracking device warrant was not necessary for Erdely to trace the signal from Kozikowski's wireless router to the sidewalk in front of Stanley's residence.

28. In *Kyllo,* the Supreme Court held:

> Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.

Kyllo, 533 U.S. at 40. Stanley argues Erdely used Moocherhunter™, a device that is not in general public use, to explore details of Stanley's home that would previously have been unknowable without physical intrusion. (ECF No. 36 at 45.)

29. In *Kyllo,* the government suspected the petitioner was growing marijuana inside his home. *Kyllo,* 533 U.S. at 29. Knowing that "marijuana growth typically requires high-intensity lamps," the government used a thermal-imagine device aimed at the petitioner's

home to determine “whether an amount of heat was emanating from petitioner's home consistent with the use of such lamps.” *Id.* The court described the technology of the thermal-imaging device as follows:

> Thermal imagers detect infrared radiation, which virtually all objects emit but which is not visible to the naked eye. The imager converts radiation into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images.

Kyllo, 533 U.S. at 29–30. The Court described the government's use of this device:

> The scan of Kyllo's home took only a few minutes and was performed from the passenger seat of Agent Elliott's vehicle across the street from the front of the house and also from the street in back of the house. The scan showed that the roof over the garage and a side wall of petitioner's home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex. Agent Elliott concluded that petitioner was using halide lights to grow marijuana in his house, which indeed he was.

***16** *Kyllo,* 533 U.S. at 30.

30. The Court acknowledged the heightened privacy interests one has in his home, noting: “With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no.” *Id.* at 31. The Court sought to define the “limits there are upon the power of technology to shrink the realm of guaranteed privacy.” *Id.* at 34. In defining those limits, the court held:

> We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical “intrusion into a constitutionally protected area,” *Silverman,* 365 U.S., at 512, 81 S.Ct. 679, 5 L.Ed.2d 734, constitutes a search—at least where (as here) the technology in question is not in general public use. This assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted. On the basis of this criterion, the information obtained by the thermal imager in this case was the product of a search.

Kyllo, 533 U.S. at 34. Stanley argues that Moocherhunter™ is a technology that is not in general public use and was used to discover that a **computer** was located inside of Stanley's home, and therefore, Erdely's use of Moocherhunter ™ constituted a violation of his **Fourth Amendment** rights.

31. *Kyllo,* however, is distinguishable from this case, *Smith,* and its progeny. First, in *Smith* and this case, the defendant conveyed information directly to third parties in order to facilitate communication-a telephone call in *Smith*and a signal to connect to the internet in this case. In *Kyllo,* although the defendant caused the heat by using high-intensity lamps, he did not send it to a third party and to the extent he could, he contained the heat in his garage. In*Smith,* the defendant conveyed the telephone numbers directly to the telephone company. When subscribing to the internet, people provide personal information such as their addresses, birthdates, and billing information directly to their ISPs. When browsing the internet, people convey their IP addresses directly to the websites they wish to visit. It follows that there is no reasonable expectation of privacy in this information because it was purposefully conveyed to a third party.

32. When Stanley connected his computer to Kozikowski's wireless router, he clicked on the name of that connection and voluntarily caused a signal to be sent directly to Kozikowski's wireless router, which in turn sent a signal to his computer enabling him to connect to the internet. Under these circumstances, Stanley had to initiate the contact and did not have a reasonable expectation of privacy in that wireless signal simply because it emanated from a computer located inside of his home. The defendant in *Smith* argued that despite conveying the numbers he dialed to the telephone company, he demonstrated an expectation of privacy in making the telephone call because he made the call from his home. *Id.* at 743. The Court rejected this argument finding:

***17** Although petitioner's conduct may have been calculated to keep the contents of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed. Regardless of his location, petitioner had to convey that number to the telephone company in precisely the same way if he wished to complete his call.

Smith, 442 U.S. at 743. Regardless of his location, Stanley had to send his wireless signal to a wireless router to connect to the internet. *See Smith,* 442 U.S. at 743. Had he lawfully made this connection by subscribing to an ISP, he would have disclosed information to the ISP that enabled the government to know his location, just as the government learned about Kozikowski's location. That he established an unauthorized internet connection via the Kozikowski router does not convert his subjective expectation of privacy into a reasonable one.[FN8]

[FN8]. The government's use of the technology further distinguishes this case from *Kyllo.* In *Kyllo,* the government agents sat in front of the petitioner's house and pointed the thermal-imaging device right at the house. Those agents knew the information they received would come from the petitioner's house because that was the exact location they were searching. Erdely, however, started his investigation with Kozikowski's wireless router inside Kozikowski's home. He followed the signal, which was sent by Stanley, outside Kozikowski's home and did not know where it would lead. But-for the information Stanley voluntarily sent to Kozikowski's wireless router, i.e. the signal which caused the router to log his IP address, the 95 MAC address, and which ports he was accessing, Erdely could not have traced the signal from Kozikowski's wireless router to the sidewalk in front of Stanley's home. Stanley conveyed the information to a third party, thus exposing himself to the risk that it may be disclosed to the police. *See Smith,* 442 U.S. at 744.

33. The court finds Erdely's use of Moocherhunter™ was not a search protected by the Fourth Amendment because Stanley did not have a reasonable expectation of privacy in the signal which he voluntarily conveyed to a third party.

The Stanley Search Warrant

34. "Probable cause exists when 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.' " *United States v. Grubbs,* 547 U.S. 90, 96, 126 S.Ct. 1494, 164 L.Ed.2d 195 (2006) (quoting *Illinois v. Gates,* 462 U.S. 213, 238, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983)). Probable cause determinations require the magistrate judge to make a "practical, common-sense decision." *Gates,* 462 U.S. at 238.

35. The role of a reviewing court is not to review the magistrate judge's decision *de novo* but to determine whether " 'the magistrate had a substantial basis for concluding that probable cause existed.' " *United States v. Stearn,* 597 F.3d 540, 554 (3d Cir.2010) (quoting *Gates,* 462 U.S. at 238). This is a deferential standard of review. *Id.* "Doubtful or marginal cases in this area should

be largely determined by the preference to be accorded to warrants." *Gates,* 462 U.S. at 237 n. 10.

36. Stanley assert two arguments with respect to the search warrant for the Stanley residence: (1) the affidavit does not provide probable cause because there is no indication that the computer associated with the 114 IP address or 95 MAC address connected to the Kozikowski router on January 19, 2011 ever shared or accessed child pornography files; and (2) there were material omissions in the affidavit of probable cause with respect to the description of Stanley's residence, how Moocherhunter™ operates and Erdely's training with the device, i.e. he was not certified by the manufacturer and his training consisted of a few minutes with Cpl. Jon Nelson. (ECF no. 36 at 2.)

37. The court will first address whether the magistrate justice had a substantial basis to find probable cause on the face of Erdely's affidavit in support of his application for the Stanley search warrant.

***18** 38. In the affidavit, Erdely indicated that in his initial investigation on November 11, 2010, someone using LimeWire, a file-sharing software on the Gnutella network, with the 174 IP address and 300 GUID, possessed child pornography. Erdely learned this user was connected to the internet through Kozikowski's wireless router. Erdely explained that he forensically determined neither of Kozikowski's computers was the computer he observed sharing child pornography and that Kozikowski's wireless router was not password protected, meaning others could access it.

39. Erdely explained that Kozikowski gave him access to the wireless router to continue his investigation, and that such access allowed him to view any IP addresses, public or private, that were assigned to the wireless router and any wireless cards, including the cards' serial numbers, that were associated with those IP addresses. Erdely also explains that access to Kozikowski's wireless router logs enabled him to determine which ports, if any, an IP address was communicating through while connected to the wireless router.

40. Erdely described the information he learned from Hoffa's and Eger's investigations. Erdely noted that both investigators reported that a person with the 300 GUID, the same GUID he identified as sharing child pornography via Kozikowski's internet connection, was viewing and sharing child pornography. Hoffa's report indicated the user was assigned the 215 IP address.

41. Erdely explained that through access to Kozikowski's wireless router logs, he learned the 215 IP address was assigned to the Kozikowski router. He indicated that he learned the 95 MAC address was connected to the wireless router with the private, meaning internal, 114 IP address. Erdely explained that the 114 IP address was communicating on a port commonly used to share files on the Gnutella network, which Erdely knew was used, among other things, to share child pornography. Based on this information, Erdely used Moocherhunter™ to trace the MAC 95 address signal from Kozikowski's wireless router to the sidewalk in front of Stanley's home, where the Moocherhunter™'s reading was 100, the highest possible reading.

42. Stanley is correct that the affidavit does not explicitly provide that any of the investigators observed the 114 IP address and the 95 MAC address sharing or viewing child pornography. In the affidavit, Erdely explained, however, that persons using the Gnutella file-sharing network are assigned unique numbers, GUIDs, to identify their particular computers, and in each of the investigator's reports, the same 300 GUID was identified as sharing child pornography. In Hoffa's investigation, the public 215 IP address identified was assigned to Kozikowski's wireless router. Erdely determined that the 95 MAC address assigned to the private 114 IP address and connected to Kozikowski's wireless router was communicating with ports used to file share on the Gnutella network. Based on the totality of the information set forth in Erdely's affidavit, the court finds the magistrate justice had a substantial basis for issuing a search warrant for Stanley's home.

***19** 43. The information in the affidavit was sufficient to provide the magistrate justice with a substantial basis for concluding there was a fair probability that evidence that someone was possessing visual depictions of minors engaged in sexually explicit conduct would be found in Stanley's residence.

44. With respect to Stanley's second argument that there were material omissions in Erdely's affidavit of probable cause, the court finds to the extent any omissions were made, they were not material to a finding of probable cause, and therefore, evidence discovered as a result of executing the Stanley search warrant will not be suppressed on this basis.

45. Under *Franks v. Delaware,* 438 U.S. 154, 155–56, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), when a warrant is obtained based upon a false statement made in a supporting affidavit, the fruits of the

search warrant must be excluded if the remaining material, following the excision of the falsity, is independently insufficient to support a finding of probable cause. If the falsity is based upon an omission rather than a misstatement of facts, the court must remove the falsehood by supplying the omitted information to the original affidavit, and subsequently determining if the affidavit with the added information contains sufficient probable cause. *United States v. Yusuf* 461 F.3d 374, 383 (3d Cir.2006);*Sherwood v. Mulvihill,* 113 F.3d 396, 401 (3d Cir.1997).

46. The court must suppress evidence obtained pursuant to a search warrant if the defendant proves by a preponderance of the evidence that: (a) the affiant knowingly and deliberately, or with a reckless disregard for the truth, made false statements or omissions that create a falsehood in applying for a warrant; and (b) such statements or omissions were material, or necessary, to the probable cause determination. *Franks,* 438 U.S. at 155–56; *Yusuf,* 461 F.3d at 383.

47. Stanley does not assert and did not establish that Erdely intentionally, knowingly, or with reckless disregard for the truth omitted material information from his affidavit of probable cause which is required under first part of the*Franks* analysis. Stanley also did not prove that the omissions were material to the magistrate justice's finding of probable cause.

48. Stanley's first argument is that Erdely omitted or used incorrect material information about his apartment building in the affidavit of probable cause. Stanley argues Erdely's descriptions of the building in the application for search warrant and authorization and the description in the affidavit of probable cause are misleading because he does not indicate the residence is an apartment building in the application for search warrant and authorization and although he refers to the residence as an apartment building in the affidavit of probable cause, he refers to the apartment, which has six units, as having only "two upstairs residence [sic] and then one down stairs [sic] residence in the vicinity to where [he] was pointing the antenna." (Gov't's Ex. 8, ¶ 21.)

20** 49. Even if Erdely had reported in the affidavit to the magistrate justice that the apartment building had six apartments, the affidavit would still support a finding of probable cause. In the affidavit of probable cause, Erdely stated that the apartment building had two upstairs apartments and one downstairs apartment ***"in the vicinity" of where he was using Moocherhunter™. (Gov't's Ex. 8, ¶

21) (emphasis added.) He specifically stated that when he pointed to the front door of the apartment, the signal grew to 100, which is the strongest signal which can be reported." (*Id.*) The averment that there were three additional apartments would not negate a finding of probable cause because once Erdely pointed the antenna directly at the front door of Stanley apartment, the signal reached 100.

50. Stanley also argues that Erdely omitted information about how the Moocherhunter™ works, his lack of training, and "the precise circumstances under which it would be deployed." (ECF No. 36 at 61.) The court finds this omitted information is not material to a finding of probable cause.

51. With respect to how Moocherhunter™ works, Erdely provided the following explanation:

This officer used a publically available tool to locate the MAC address which was attached to the Kozikowski's wireless internet. The tool is "moocherhunter" [sic]. It has a power meter which shows the strength of the wireless signal assicated [sic] with a particular MAC address (serial to a wireless card). I pointed it across the street from the Kozikowski's residence and it initially rose to a level of 67. As I walked toward this apartment building, the signal grew stronger.

The only apartment in the vicinity to the direction I was pointing the antenna, was 1481. As I pointed to the front door of the apartment, the signal grew to 100 which is the strongest signal which can be reported.

The court finds if Erdely elaborated on this description about how the Moocherhunter™ functions, it would have supported, not negated, the magistrate justice's finding of probable cause.

52. Stanley argues that Erdely omitted material information with respect to his lack of training and experience with Moocherhunter™. Again, the court does not find that this information would negate the magistrate justice's finding of probable cause. As Stanley suggests, Erdely received only a few minutes of training from Cpl. Jon Nelson and this was the first time he used Moocherhunter ™ in an investigation. If this information was included in Erdely's affidavit, however, it would not negate a finding of probable cause in light of Erdely's other trainings, certifications, and experience in the Computer Crime Division, which included "execution of more than one hundred search warrants related to computer crimes" and various trainings and

certifications relating to computers dating back to 1995. If using Moocherhunter™ for the first time in this investigation necessarily negates a finding of probable cause, the government could never utilize new technologies in its investigations. (Gov't's Ex. 8, ¶ 21.)

***21** 53. Even if Erdely included all this information allegedly omitted from his affidavit of probable cause, the magistrate justice would still have a substantial basis to find a fair probability that evidence of criminal activity would be found in Stanley's residence.

Good Faith Exception

54. Even if a search violates the Fourth Amendment, the exclusionary rule does not always apply to the evidence obtained by the unlawful search. "When police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted 'in objectively reasonable reliance' on the subsequently invalidated search warrant." *Herring,* 129 S.Ct. at 701 (citing *United States v. Leon,* 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

55. The government argues that "[e]ven if the affidavit failed to articulate probable cause that evidence of a crime was inside the Stanley residence, no evidence should be excluded because the search warrant was relied upon in good faith." (ECF No. 37 at 36.)

56. The court agrees with the government's assessment. Erdely acted in objectively reasonable reliance on the search warrant for Stanley's home and computer. Even if Erdely lacked probable cause to conduct that search, the evidence seized will not be suppressed.

57. The exclusionary rule is meant to deter "deliberate, reckless, or grossly negligent conduct, or in some circumstances, recurring or systemic negligence." *Herring,* 129 S.Ct. at 702; *see Stearn,* 597 F.3d at 560 (exclusionary rule's overarching policy is aimed at deterring official lawlessness).

58. The Court of Appeals for the Third Circuit has recently held:

To determine whether to apply the [exclusionary] rule in a particular case, we weigh the benefits of the rule's deterrent effects against the costs of exclusion, which include "letting guilty and possibly dangerous defendants go free." *Herring,* 129 S.Ct. at 700, 701. Because of the high social costs of excluding evidence in a criminal case, the Supreme Court has instructed that the exclusionary rule should only be applied when "police conduct [is] ... sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Id.* at 702. Accordingly, we apply the rule when police conduct is "deliberate, reckless, or grossly negligent," or when it will deter "recurring or systemic negligence." *Id.* Put another way, isolated negligent acts on the part of the police do not warrant application of the exclusionary rule. *See id.*

United States v. Tracey, 597 F.3d 140, 151 (3d Cir.2010).

59. Here, there is nothing in the record to show that Erdely's conduct was deliberate, reckless, or grossly negligent or that the application of the exclusionary rule will deter recurring or systematic negligence. Erdely first learned the 300 GUID was viewing and sharing child pornography on November 11, 2010. After ruling out Kozikowski's computers and with Kozikowski's permission, he placed a computer inside of Kozikowski's home to continue his investigation of the 300 GUID. He did not take any action against Stanley until he saw the search results of Hoffa's and Eger's investigations reporting the 300 GUID was back online and sharing child pornography two months after he initiated the investigation. Erdely used Moocherhunter™ to trace the signal associated with the 95 MAC address to Stanley's front door.

***22** 60. Before conducting the search of Stanley's home, however, Erdely sought a search warrant from a neutral magistrate justice by submitting the ten-page affidavit, which described his experience, computer training, the various technologies involved in the Stanley investigation, the investigative techniques used in that investigation, the results of Hoffa's and Eger's investigations of the 300 GUID, and what he knew and what he did to arrive at the conclusion that the computer sharing and viewing child pornography observed by Erdely, Hoffa, and Eger was the same computer and was located inside Stanley's residence. Erdely acted in reliance upon the neutral magistrate justice's issuance of the search warrant in conducting the search of Stanley's home and computer. Under these circumstances, the court finds Erdely's good faith reliance on the search warrant was objectively reasonable, and even assuming for the sake of argument that probable cause was lacking to search Stanley's home and computer, the good faith exception applies and the evidence seized from that search and Stanley's statements made thereafter will not be suppressed.

61. For the reasons stated above, the motion to suppress must be denied.

III. Order

AND NOW, this 14th day of November, 2012, upon consideration of the parties' filings, the arguments made by counsel at the suppression hearings held on May 24, 2012, and October 15, 2012, and the testimony of witnesses and the evidence introduced at those hearings, IT IS HEREBY ORDERED that, in accordance with the findings of fact and conclusions of law filed herewith, defendant's motion to suppress (ECF No. 24) is DENIED.