No._____

IN THE SUPREME COURT OF THE UNITED STATES

_____

ALEXANDER NATHAN NORRIS,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

_____

ON PETITION FOR A WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

_____

APPENDIX

_____

JOHN BALAZS
COUNSEL OF RECORD
Attorney at Law
916 2nd Street, Suite F
Sacramento, CA 95814
(916) 447-9299
john@balazslaw.com
Attorney for Petitioner

APPENDIX
INDEX

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee*, v. ALEXANDER NATHAN NORRIS, *Defendant-Appellant.*	No. 17-10354 D.C. No. 2:11-cr-00188-KJM-1 OPINION

Appeal from the United States District Court
for the Eastern District of California
Kimberly J. Mueller, District Judge, Presiding

Argued and Submitted February 14, 2019
San Francisco, California

Filed November 4, 2019

Before: Mary M. Schroeder, Diarmuid F. O'Scannlain, and Johnnie B. Rawlinson, Circuit Judges.

Opinion by Judge Rawlinson

Appendix A

SUMMARY*

Criminal Law

The panel affirmed a conviction for distribution and possession of material involving the sexual exploitation of minors, in a case in which an FBI agent used wireless-tracking software to detect the signal strength of the address of the defendant's wireless device.

The panel held that because there was no physical intrusion into the defendant's residence to detect the signal strength of his device's media-access-control (MAC) address, the district court correctly applied the factors set forth in *Katz v. United States*, 389 U.S. 347 (1967), and determined that no search occurred under the Fourth Amendment. The panel wrote that the defendant lacked a subjective expectation of privacy in the signal strength of his MAC address emanating from his unauthorized use of a third-party's password-protected wireless router. The panel concluded that society is not, in any event, prepared to recognize as reasonable an expectation of privacy predicated on unauthorized use of a third-party's internet access.

The panel held that the district court did not err in denying the defendant's request for a *Franks* hearing, where the defendant failed to make a substantial preliminary showing that the search warrant affidavit included any knowingly, intentionally, or recklessly made material misrepresentations or omissions; and where a corrected

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

and/or supplemented affidavit would not have affected the probable cause determination.

COUNSEL

John Paul Balazs (argued), Sacramento, California, for Defendant-Appellant.

Matthew G. Morris (argued) and Shelley D. Weger, Assistant United States Attorneys; Camil A. Skipper, Appellate Chief; McGregor W. Scott, United States Attorney; United States Attorney's Office, Sacramento, California; for Plaintiff-Appellee.

OPINION

RAWLINSON, Circuit Judge:

To resolve this case, we must once again venture into the intersection of technology and the Fourth Amendment. Defendant-Appellant Alexander Nathan Norris (Norris) seeks to have us apply the protections of the Fourth Amendment to the use of a wireless tracking program to identify the address of his wireless device. Under the facts of this case, we conclude that no Fourth Amendment search occurred in the course of identifying Norris's wireless device, and we affirm his conviction.

I. BACKGROUND

This case originated in December, 2010, when Federal Bureau of Investigation (FBI) Special Agent Nicholas G.

Phirippidis (Special Agent Phirippidis) initiated an investigation into the possession and distribution of child pornography through a peer-to-peer file-sharing network (P2P network).[1] Special Agent Phirippidis downloaded child pornography from username "boyforboys1," using an Internet Protocol address (IP address)[2] of 67.172.180.130 registered to Comcast Communications (Comcast). Comcast could not determine the physical address for "boyforboys1."

In March, 2011, "boyforboys1" logged into the same P2P network, using a different IP address of 64.160.118.55 registered to AT&T Internet Services (AT&T), and Special Agent Phirippidis again downloaded child pornography from "boyforboys1." In response to a subpoena, AT&T identified the subscriber associated with the IP address as residing in Apartment 242. After conducting a public records search and confirming with the apartment manager that the subscriber still resided at Apartment 242, Special Agent Phirippidis obtained a search warrant for Apartment 242.

Upon execution of the search warrant, Special Agent Phirippidis discovered that the password-protected wireless internet router (router) located in Apartment 242 used an IP address of 69.105.80.128 rather than the 64.160.118.55 IP

[1] P2P file-sharing software "allows network computer users, connected to the Internet, to share many types of files; these files typically include music, graphics, images, movies, and text. In this way, [P2P network] users are able to collect large numbers of files, including child pornography."

[2] An IP address "refers to a unique number used by a computer to access the Internet." IP addresses can be dynamic (the number changes each time the computer accesses the Internet) or static (the number remains the same each time the computer accesses the Internet).

address connected to "boyforboys1." The search revealed that no devices in Apartment 242 contained any evidence of child pornography or of the P2P file-sharing program used by "boyforboys1."

FBI agents identified all the devices that had recently connected to the router located in Apartment 242 and pinpointed two unknown devices, "bootycop" (media access control [MAC] address unknown) and "CK" (with a MAC address of 00.25:d3:d4:c4:73).[3] Because the apartment residents could not identify either unknown device, Special Agent Phirippidis concluded that "CK" and "bootycop" accessed the router in Apartment 242 without permission. Neither computer was connected to the router when Special Agent Phirippidis executed the search warrant, but agents attempted to identify the location of the "CK" device using Moocherhunter software (Moocherhunter)[4] and the 00.25:d3:d4:c4:73 MAC address.

With Moocherhunter in passive mode and using a wireless antenna, Special Agent Phirippidis and his colleagues captured signal strength readings to locate the 00.25:d3:d4:c4:73 MAC address. Specifically, Moocherhunter was installed on a laptop computer and connected to a directional antenna. The Moocherhunter

[3] A MAC address is "a unique identifier assigned to a network device for communication on a physical network. A MAC address is most often assigned by the manufacturer of a network device," and differs from an IP address.

[4] As its name implies, Moocherhunter is an open-source wireless tracking software program designed to identify computers trespassing on wireless computer networks. Moocherhunter enables the detection of wireless traffic without directly accessing any device.

program was provided the 00.25:d3:d4:c4:73 MAC address, and approximately seventeen location readings were taken in the vicinity of Apartment 242. The readings were significantly higher when the antennae was aimed in the direction of Apartment 243. As a result, the agents concluded that Apartment 243 housed the "CK" device. After identifying the target apartment, Special Agent Phirippidis waited for "boyforboys1" to log on to the P2P network.

A week later, "boyforboys1" logged onto the P2P network and distributed child pornography from the 69.105.80.128 IP address linked to the wireless router in Apartment 242. Special Agent Phirippidis downloaded child pornography files from "boyforboys1," and went to Apartment 242 to confirm whether "boyforboys1" utilized "CK" or "bootycop" devices to distribute the child pornography. With the consent of a resident of Apartment 242, Special Agent Phirippidis and his colleagues determined that "CK" (with the 00.25:d3:d4:c4:73 MAC address) and "bootycop" (with a MAC address of 00:1f:1f:49:d3:11) were logged into the wireless router belonging to the residents of Apartment 242.

After a period of time, "CK" disconnected from the router, leaving only "bootycop" connected to the router. Again using the Moocherhunter software and a wireless antenna, Special Agent Phirippidis measured the signal strength of MAC address 00:1f:1f:49:d3:11, taking readings from Apartment 242 and from a nearby vacant apartment (with permission from the apartment manager). He concluded that: (1) "CK" and "bootycop" exhibited similar signal strengths; (2) "CK" and "bootycop" were associated with each other; (3) Apartment 243 housed both devices; and (4) both had gained unauthorized access to the password-protected router in Apartment 242.

Based on the Moocherhunter data, Special Agent Phirippidis obtained a search warrant for Apartment 243. When Special Agent Phirippidis and his colleagues executed the search warrant, they discovered evidence of child pornography.

II. PROCEDURAL HISTORY

The government indicted Norris on one count of distribution of material involving the sexual exploitation of minors, in violation of 18 U.S.C. § 2252(a)(2), and one count of possession of material involving the sexual exploitation of minors, in violation of 18 U.S.C. § 2252(a)(4)(B). Norris subsequently moved to suppress the evidence obtained as a result of the search warrant, alleging that use of the Moocherhunter software amounted to a warrantless search in violation of the Fourth Amendment. Norris also moved for a *Franks*[5] hearing on the basis that the search warrant affidavit contained misrepresentations and omissions that materially misled the magistrate judge and negated any probable cause determination. The district court denied both motions.

Addressing the motion to suppress, the district court held that no Fourth Amendment search occurred, because, unlike in *Florida v. Jardines*, 569 U.S. 1 (2013), the agents did not encroach upon Norris's curtilage to determine the location of contraband inside the house. *See id.*, 569 U.S. at 3, 11 12 (holding that a Fourth Amendment search occurred when police brought a drug-sniffing dog to defendant's porch to determine the presence of drugs inside the residence). In *Jardines*, the Supreme Court clarified that the focus in a

[5] *Franks v. Delaware*, 438 U.S. 154 (1978).

Fourth Amendment inquiry should be on "the traditional property-based understanding of the Fourth Amendment." *Id.* at 11. Thus, if "the government gains evidence by physically intruding on constitutionally protected areas," such as the curtilage of a home, a search has occurred, and no further inquiry is required, including whether the defendant had a reasonable expectation of privacy. *Id.*

Having found that the agents did not physically intrude upon Norris's property as in *Jardines*, the district court proceeded to analyze whether Norris could nevertheless establish that a search occurred under the analysis set forth by the Supreme Court in *Katz v. United States*, 389 U.S. 347 (1967). The *Katz* test has been described as encapsulating two questions. The first question "is whether the individual, by his conduct, has exhibited an actual (subjective) expectation of privacy." *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (citation and internal quotation marks omitted). The second question measures the objective reasonableness of an individual expectation of privacy by inquiring "whether the individual's subjective expectation of privacy is one that society is prepared to recognize as reasonable." *Id.* (citation and internal quotation marks omitted). The district court answered both questions in the negative as applied to Norris.

The district court concluded that Norris lacked a subjective, reasonable expectation of privacy, because he connected to a third-party's router without authorization and assumed the risk that his signal would reveal the MAC address to authorities. The district court distinguished *Kyllo v. United States*, 533 U.S. 27 (2001), involving the use of thermal-imaging devices to scan the residence to determine the existence of fluorescent lights used in growing marijuana.

The district court also ruled that society was not prepared to recognize an expectation of privacy for an individual who gains unauthorized access to a third-party's password-protected router.

Finally, the district court ruled that Norris failed to meet the standard for a *Franks* hearing. Although the alleged misrepresentations and omissions would likely provide a more complete picture of the reliability of the software, the district court concluded that the alleged misrepresentations and omissions did not invalidate the probable cause finding.

Following trial, the jury convicted Norris on both counts. The district court sentenced Norris to 72 months' imprisonment and 180 months' supervised release. The district court entered final judgment, and Norris timely appealed.

III. JURISDICTION AND STANDARD OF REVIEW

The district court had subject matter jurisdiction under 18 U.S.C. § 3231, and we have jurisdiction under 28 U.S.C. § 1291. We review denial of a motion to suppress *de novo*, and the district court's factual findings for clear error. *See United States v. Zapien*, 861 F.3d 971, 974 (9th Cir. 2017). We also review *de novo* the denial of a *Franks* hearing. *See United States v. Kleinman*, 880 F.3d 1020, 1038 (9th Cir. 2018), *as amended*.

IV. DISCUSSION

A. Fourth Amendment Search

It is undisputed that there was no actual physical intrusion into Norris's apartment. Therefore, we apply the *Katz* test to determine if the agents engaged in a search under the Fourth Amendment. *See Jardines*, 569 U.S. at 11.

1. *Subjective Expectation of Privacy*

To connect to the internet, Norris's devices sent a wireless signal transmitting the MAC address of the devices to the password-protected wireless router in Apartment 242. Once connected, Norris accessed the router to utilize the internet connection without authorization.

Although physically located in his home, Norris's wireless signal reached outside his residence to connect to the wireless router in Apartment 242. The FBI captured Norris's wireless signal strength outside Norris's residence to determine the source of the signal. The FBI's actions may be likened to locating the source of loud music by standing and listening in the common area of an apartment complex. Although the music is produced within the apartment, the sound carries outside the apartment. Just as no physical intrusion "on constitutionally protected areas" would be required to determine the source of the loud music, no physical intrusion into Norris's residence was required to determine the strength of the wireless signal emanating from the devices in his apartment. *Jardines*, 569 U.S. at 11.

We conclude that no subjective expectation of privacy exists under these circumstances, where information is openly

available to third parties. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351 (citations omitted); *see also California v. Ciraolo*, 476 U.S. 207, 213 14 (1986) (holding that use of an aircraft in public airspace to view marijuana plants in the backyard of a home did not violate the Fourth Amendment); *California v. Greenwood*, 486 U.S. 35, 40 41 (1988) (concluding that search of publicly exposed garbage did not violate the Fourth Amendment); *United States v. Borowy*, 595 F.3d 1045, 1047 48 (9th Cir. 2010) (upholding search of computer files using file-sharing software available to the public).

We agree with the district court that *Kyllo* does not dictate the conclusion that a Fourth Amendment search occurred in this case. In *Kyllo*, police officers utilized thermal-imaging technology to scan the inside of a house to detect the presence of heat in amounts consistent with the presence of high-intensity lights used to grow marijuana. *See* 533 U.S. at 29 30. The Supreme Court ruled the scan a search under the Fourth Amendment because the government used "sense-enhancing" technology to obtain information from the *inside* of a home that the police could not otherwise obtain "without physical intrusion into a constitutionally protected area." *Id.* at 34. Unlike in *Kyllo*, where the defendant confined his illegal activities to the interior of his home and relied on the privacy protections of the home to shield these activities from public observation, Norris's activities reached beyond the confines of his home, thereby negating any expectation of privacy. *See Katz*, 389 U.S. at 351.

United States v. Karo, 468 U.S. 705 (1984), is equally distinguishable. In *Karo*, the United States Supreme Court held that the government's monitoring of a beeper inside a

private residence violated the Fourth Amendment because the beeper provided location information that could not have been obtained from outside the curtilage of the house. *See id.* at 708, 714; *see also Silverman v. United States*, 365 U.S. 505, 506, 509 12 (1961) (holding that a Fourth Amendment search occurred when police inserted a "spike mike" into a house to overhear conversations of the house next door); *Jardines*, 569 U.S. at 4 (concluding that a Fourth Amendment search occurred when police used a drug-sniffing dog along the front porch (the curtilage) to establish the location of marijuana inside a house). Unlike in *Karo*, *Silverman*, and *Jardines*, the agents in this case collected information from non-constitutionally protected areas, and they collected no information from inside Norris's residence. Thus, Norris lacked any expectation of privacy in the emission of the signal strength of the MAC address emanating from outside his apartment. *See Borowy*, 595 F.3d at 1047 48.

2. *Societal Recognition of Expectation of Privacy as Reasonable*

Even if Norris harbored a subjective expectation of privacy, that expectation was not one society is prepared to recognize as reasonable. The concept of society's recognition of an expressed expectation of privacy is consistent with the overall focus in Fourth Amendment jurisprudence on reasonableness. *See Brigham City, Utah v. Stuart*, 547 U.S. 398, 403 (2006) ("[T]he ultimate touchstone of the Fourth Amendment is reasonableness . . .") (citations and internal quotation marks omitted). If society is not prepared to recognize an expectation of privacy as reasonable, intrusion upon that expectation does not violate the Fourth Amendment's overall reasonableness requirement. *See Kyllo*, 533 U.S. at 33. As the Supreme Court articulated in *Rakas v.*

Illinois, 439 U.S. 128, 143 n.12 (1978), "[o]ne of the main rights attaching to property is the right to exclude others, and one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy." (citation omitted). Conversely, one has no legitimate expectation of privacy in property for which he lacks any possessory or ownership interest. *See United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003).

We have also generally concluded that society is not prepared to recognize as reasonable a subjective expectation of privacy in the content of property obtained through unauthorized means. In *United States v. Caymen*, 404 F.3d 1196, 1197 98 (9th Cir. 2005), Caymen used a third-party's credit card to fraudulently purchase a laptop. The police obtained a search warrant for Caymen's residence and discovered the laptop. *See id.* The police contacted the store owner for approval to review the contents of the laptop. *See id.* at 1198. Once the police discovered child pornography, they immediately ceased their search and obtained another warrant to search for child pornography. *See id.* Caymen was indicted for possession of child pornography and moved to suppress seized photographs on the basis that the police conducted an illegal search. *See id.*

On appeal, we rejected Caymen's challenge of the search, ruling that the Fourth Amendment "does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that society is prepared to accept as reasonable." *Id.* at 1200 (internal quotation marks omitted).

We also find instructive the Third Circuit's decision in *United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014). *Stanley* also involved use of the Moocherhunter software to detect the signal strength of a MAC address from outside the suspected residence. *See id.* at 116. As in our case, the defendant accessed child pornography via a neighbor's wireless service. *See id.* at 115 16. The only difference is that in *Stanley*, the neighbor's wireless service was not password-protected. *See id.* at 116. Under these similar circumstances, the Third Circuit determined that "Stanley's expectation of privacy [in his MAC address signal] is not one that society is prepared to recognize as legitimate." *Id.* at 119 (footnote reference omitted). The Third Circuit concluded that "while Stanley may have justifiably expected the path of his invisible radio waves to go undetected, society would not consider this expectation legitimate given the unauthorized nature of his transmission." *Id.* at 120. Although we do not adopt the entire reasoning espoused by the Third Circuit, we agree that even if a person in Norris's position had a subjective expectation of privacy in the wireless signal transmitted outside his residence, society is not prepared to recognize this expectation as legitimate, given the unauthorized access used to generate the wireless transmission. *See id.* Indeed, it strains credulity to suggest that society would be prepared to recognize an expectation of privacy as reasonable when an individual gains access to the internet through the unauthorized use of a third-party's password-protected router located outside his residence. *See id.*

In sum, we affirm the district court's application of the *Katz* factors to conclude that no Fourth Amendment search occurred. Even if Norris had a subjective expectation of

privacy, it was not one society was prepared to accept as reasonable.

B. *Franks* hearing

A *Franks* hearing determines "the validity of the affidavit underlying a search warrant." *Kleinman*, 880 F.3d at 1038 (citation omitted). To obtain a *Franks* hearing, a defendant must make a substantial preliminary showing that: (1) "the affiant officer intentionally or recklessly made false or misleading statements or omissions in support of the warrant," and (2) "the false or misleading statement or omission was material, *i.e.*, necessary to finding probable cause." *United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017) (citation, alteration, and internal quotation marks omitted). Once the defendant makes that showing, to prevail at the subsequent hearing, he must establish both prongs by a preponderance of the evidence. *See United States v. Martinez-Garcia*, 397 F.3d 1205, 1214 15 (9th Cir. 2005).

Norris failed to satisfy the first requirement because he did not present any evidence that Special Agent Phirippidis acted knowingly, intentionally, or with reckless disregard for the truth in preparing the affidavit.

In any event, Norris also failed to satisfy the second requirement for a *Franks* hearing because none of the alleged false statements or omissions materially affected the probable cause determination. "Probable cause to search a location exists if, based on the totality of the circumstances," a "fair probability" exists that the police will find evidence of a crime. *Perkins*, 850 F.3d at 1119 (citation omitted). The key inquiry in resolving a *Franks* motion is whether probable cause remains once any misrepresentations are corrected and

any omissions are supplemented. *See id.* If probable cause remains, the defendant has failed to establish a material omission. *See id.*

Norris argues that the FBI falsely identified Moocherhunter as open-source software rather than proprietary software. Norris also alleges that the following omissions were material: (1) the FBI used a free version of Moocherhunter instead of the law enforcement version; (2) the FBI did not authorize its agents to use Moocherhunter in criminal investigations; (3) the FBI did not train its agents to use Moocherhunter; (4) the FBI did not formally test the software; (5) the FBI disregarded any reading believed to be anomalous or not of value; (6) the FBI agents used an incomplete method; (7) the FBI agents did not provide the magistrate judge with location information in relation to the signal strength; (8) the Moocherhunter developer did not subject the software to any objective or peer-review testing; and (9) Moocherhunter will give false readings when a party changes the MAC address to conceal identity.

If the alleged misrepresentations and omissions were corrected and supplemented, the probable cause determination would not be affected, as a "fair probability" remained that Apartment 243 housed devices containing child pornography. *Id.* (citation omitted). The district court did not err in denying the requested *Franks* hearing. *See id.*

V. CONCLUSION

Because there was no physical intrusion into Norris's residence to detect the signal strength of the MAC address of his device, the district court correctly applied the *Katz* factors and determined that no search occurred under the Fourth

Amendment. Norris lacked a subjective expectation of privacy in the signal strength of his MAC address emanating from his unauthorized use of a third-party's wireless router. In any event, we conclude that society is not prepared to recognize as reasonable an expectation of privacy predicated on unauthorized use of a third-party's internet access. Finally, Norris failed to make a substantial preliminary showing that the search warrant affidavit included any knowingly, intentionally, or recklessly made material misrepresentations or omissions. Moreover, a corrected and/or supplemented affidavit would not have affected the probable cause determination. The district court did not err in denying Norris a *Franks* hearing.

AFFIRMED.

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT COURT OF CALIFORNIA

UNITED STATES,

Plaintiff, No. 2:11-cr-00188-KJM

vs.

ALEXANDER NATHAN NORRIS,

Defendant. ORDER

_____/

On May 29, 2013, the parties appeared for hearing on defendant Alexander Norris's motion to suppress evidence and for a *Franks* hearing. Matthew Morris, Assistant United States Attorney, appeared for the government; Alexandra Paradis Negin and Matthew Scoble, Assistant Federal Defenders, appeared for defendant Norris, who was present out of custody. For the reasons set forth below, the court DENIES defendants' motions.

I. BACKGROUND

Defendant is charged with possessing child pornography under 18 U.S.C. § 2252(a)(2) and 18 U.S.C. § 2252(a)(4)(B). Some of the evidence in this case was gathered through a search of Norris's apartment at [redacted], Apartment 243, Davis, California ("Apartment 243"). This search was authorized by a warrant issued by a United States

/////

Magistrate Judge on April 11, 2009, based on an affidavit prepared by FBI Special Agent Nicholas G. Phirippidis.

Agent Phirippidis explained in his affidavit that his investigation leading to Norris began while he was working undercover and identified a user of Peer to Peer (P2P) file sharing software with the screen name "boyforboys1" who was distributing images of child pornography. (Phirippidis Aff. ¶¶ 35-40, Ex. A, ECF 42-1.) P2P file-sharing programs allow computer users to share files with each other directly, rather than through a central server. *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 919-20 (2005). Agent Phirippidis was able to identify boyforboys1's IP address – that "unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network" -- as registered to AT&T Internet Services. (*Id.* ¶ 44; *see* Oxford Dictionaries Online (2013)). He learned from AT&T that the subscriber associated with the IP address lived at [redacted], Apartment 242, Davis, California ("Apartment 242") and obtained a search warrant for Apartment 242. (*Id.* ¶¶ 46, 49.)

Agent Phirippidis and other FBI agents executed the warrant on April 1, 2011, and determined that neither the apartment residents nor their regular visitors had child pornography on their computers. With consent, the agents then reviewed Apartment 242's wireless router log, which revealed that other devices had connected to Apartment 242's password-protected router. (*Id.* ¶¶ 50-53.) A router is "a device which forwards data packets to the appropriate parts of a computer network." Oxford Dictionaries Online (2013). The router log listed the Media Access Control ("MAC") address of each device. (*Id.* ¶ 51.) The affidavit defines a MAC address as "a unique identifier assigned to a network device for communication on a physical network. MAC addresses are most often assigned by the manufacturer of a network device." (*Id.* ¶ 11ab.)

Two of the devices that had connected to the network were listed in the router log as "CK" and "bootycop." (*Id.* ¶¶ 53-54.) Special Agents then used software described in the affidavit as "an open-source wireless tracking utility" that uses "a wireless antenna in a passive mode" to determine if the "CK" device was located in the vicinity of Apartment 242.

(*Id.* ¶ 55.) The software tracks a device's physical location through the device's MAC address. (*Id.*) Although not identified by name in the affidavit, the parties agree that the software is that known as "Moocherhunter." Using the software, the agents took signal strength readings from Apartment 242, from Apartment 240, which was a vacant apartment accessed with the apartment complex manager's permission, and from the outdoor common areas of the apartment complex. (*Id.*) The readings indicated that the CK device was most likely located in Apartment 243 of the same building. (*Id.*)

On April 8, 2011, Agent Phirippidis signed back on to the P2P file sharing program and saw that boyforboys1 was logged in and sharing child pornography. (*Id.* ¶ 56.) Several hours later, Agent Phirippidis returned to Apartment 242 and observed that "CK" and "bootycop" devices were both at that time, accessing Apartment 242's network. (*Id.* ¶ 58.) "CK" then disconnected, while "bootycop" stayed connected, with boyforboys1 still logged into the P2P file sharing program. (*Id.* ¶ 59.)

Agent Phirippidis then used the Moocherhunter software program to ascertain the physical location of the bootycop device. (*Id.* ¶ 60.) He took "numerous signal strength readings at various locations within Apartment 242 and Apartment 240," which was vacant and entered with the consent of the building manager. Based on the readings, the agent determined the most likely location of the "bootycop" device was Apartment 243. (*Id.* ¶ 60.)

An FBI investigative report, submitted with the government's opposition, describes Moocherhunter as

> a free, downloadable, mobile tracking software tool, for the geo-location of wireless devices. MOOCHERHUNTER has the ability to identify the location of an 802.11-based wireless device by the traffic sent across a network. MOOCHERHUNTER enables the user to detect traffic from a wireless client passively. No data is transmitted from the computer running MOOCHERHUNTER, data is only monitored. MOOCHERHUNTER does not collect packets of data, it only displays the number of packets encountered and the signal strength of each.

(Ex. G at 5, ECF 43-7.) The parties agree that on April 8, 2011, Agent Phirippidis used

/////

Moocherhunter in the passive mode described above and that no data were transmitted from the agents' device running the Moocherhunter software into Apartment 243.

During discovery, defendant requested "any and all video or audio recording, and photographs take [sic] during the investigation, particularly of the process of using MOOCHERHUNTER to track the signal in this investigation." (Ex. K ¶ 6, ECF 44-1.) The government responded that there were no video or audio recordings that it had not already provided to defendant. (Ex. L ¶ 6, ECF 44-1.) However, the agents reported that "[s]everal pictures and a video were taken of [the] process" of taking "approximately 16 readings" with the software during the April 8 investigation. (ECF 43-7.) At hearing on July 8, both parties agreed that discs containing these pictures and video were not in the investigatory file and that their location was unknown, assuming that they existed. (Tr. at 3:24-4:4, 5:23-6:17, ECF 47.)

II. MOTION FOR *FRANKS* HEARING

In *Franks v. Delaware*, the Supreme Court held:

> where the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant's request.

438 U.S. 154, 155-56 (1978). The Court continued that "to mandate an evidentiary hearing, the challenger's attack must be more than conclusory. . . . There must be allegations of deliberate falsehood or reckless disregard for the truth, and those allegations must be accompanied by an offer of proof." *Id.* at 171. It cautioned that "[a]llegations of negligence or innocent mistake are insufficient." *Id.* "[D]eliberate or reckless omissions of facts that tend to mislead" may also trigger a *Franks* hearing. *United States v. Stanert*, 762 F.2d 775, 781 *as amended by* 769 F.2d 1410 (9th Cir. 1985).

In the Ninth Circuit, a defendant is entitled to a *Franks* hearing if he makes specific allegations that identified portions of the affidavit necessary to a finding of probable cause are false or misleading, and a sufficient showing that the statements or omissions were deliberately false or made with a reckless disregard for the truth. The latter showing, in turn,

requires an offer of proof challenging the veracity of the affiant, not that of any informant. *United States v. Kiser*, 716 F.2d 1268, 1271 (9th Cir. 1983). At the pleading stage, a defendant need not present clear proof of deliberate or reckless misrepresentations or omissions; it is sufficient if he makes a substantial showing to support a finding of recklessness or intent. *United States v. Gonzalez, Inc*., 412 F.3d 1102, 1111 (9th Cir. 2005), *amended on denial of rehearing by* 437 F.3d 854 (9th Cir. 2006).

Defendant asserts there are numerous material misrepresentations and omissions in Agent Phirippidis's affidavit. Defendant first contends that Agent Phirippidis misled the Magistrate Judge by not disclosing the true total number of unauthorized users of the Apartment 242 router. (ECF 42 at 13-14.) When the FBI agents served the warrant for Apartment 242 on April 1, 2011, the Apartment 242 wireless router log revealed that 33 devices had connected to the router, but the log did not indicate when each device had been connected. (Ex. F, ECF 42-6.) The agents identified four of the devices as belonging to the residents of Apartment 242 or an agent, leaving 28 devices unaccounted for. (*Id.*) Defendants argue that Agent Phirippidis's affidavit in support of the warrant for Apartment 243 is misleading because it states there were only two devices connected to the router, rather than 33. However, as the government credibly explains, only two of the devices on the log, "CK" and "bootycop," were connected to the Apartment 242 router at the same time that boyforboys1 was connected to the P2P network. (ECF 43 at 13.) The agents had narrowed their search for the boyforboys1 transmissions to these devices, and it was immaterial to their establishment of probable cause to search the apartment containing the device using the bootycop moniker that, at some other time, 26 other devices had connected to the router.

Defendant also argues that the description of a MAC address in the affidavit was misleading because it omitted the fact that a device owner can alter a MAC address, so a MAC address is not necessarily unique to a particular device. (ECF 42 at 13.) This information also is not material to the finding of probable cause. At the time the agents tracked defendant's bootycop device with Moocherhunter, the agents knew that the MAC address was assigned to the bootycop device and that the device was being used to access the P2P network under the

boyforboys1 username. (ECF 43 at 15.) Thus, any prior alteration of the device's MAC address before April 8, 2011, did not affect the reliability of the investigation. (*Id.*)

Defendant further asserts that Agent Phirippidis's affidavit omitted the following information about the Moocherhunter software, without identifying the software by name: (1) that Moocherhunter is an open-source software instead of proprietary; (2) that the FBI had not tested Moocherhunter, trained its agents in its use, or authorized agents to use it; (3) that the agents downloaded and used the free version of Moocherhunter instead of the law enforcement version of the software; (4) that Moocherhunter was made in Singapore; (5) that the makers of Moocherhunter warned that it could be inaccurate if not used properly; (6) any description of the number of readings or locations from which the agents took readings when locating the CK device. (ECF 42 at 15-16.) Additionally, defendant claims he is unable to challenge the agents' methods properly because the pictures and videos of the April 8, 2011 investigation are missing. (ECF 44 at 3.) The government contends that each of these criticisms is either immaterial or incorrect, while conceding that the CD is missing is troubling.

According to defendant, each of the alleged omissions is relevant to whether Moocherhunter is a reliable source of information, and therefore relevant to the finding of probable cause. (ECF 42 at 20.) Defendant has not made the substantial showing required under *Franks*. In response to defendant's claims that the agents withheld the information that they did not have authorization or training to use Moocherhunter, the government has submitted a declaration from Darren Holtz, FBI Special Agent, explaining that he and Special Agent Michael G. Cahoon tested Moocherhunter before it was used on April 8, 2011. (Holtz Decl., Ex. D, ECF 43-4.) The government has also submitted a declaration from Agent Cahoon, stating he learned about Moocherhunter and similar software at a FBI Cyber Division course before assisting with the April 8 investigation, along the curricula vitae of the three agents, including Phirippidis, who deployed Moocherhunter on April 8. (Cahoon Decl., Ex. D, ECF 43-4; Holtz CV, Cahoon CV, Phirippidis CV, Ex. C, ECF 43-3.) The agents' familiarity with Moocherhunter, combined with their general expertise in computer science, shows that

/////

additional information about their training with the software would not have been material to the finding of probable cause; in any event it further supports such a finding.

The court also finds that additional information about warnings on the Moocherhunter website would have been immaterial because there is no indication that the agents used the software incorrectly. The agents complied with the website's advisement to use the proper chipset and antenna. (Holtz Decl. ¶ 3.) The warning that Moocherhunter can give false readings if a MAC address has been changed was not material because as explained above, the agents were certain of the MAC address of the bootycop device at the time they were searching for it. Moreover, defendant does not explain how the mere fact that Moocherhunter was made in Singapore and downloaded for free raises questions about the software's reliability.

The government does not dispute that Moocherhunter is proprietary and not open-source, and that the terminology used in the affidavit was incomplete. If the affidavit had included the information that defendants assert is required, the magistrate judge would have had a more complete picture about Moocherhunter, but this would not have significantly altered the determination of probable cause. *See United States v. Flyer*, 633 F.3d 911, 917 (9th Cir. 2011) (statement about investigator's inability to download multiple child pornography files from defendant's computer did not need to be included in affidavit when affidavit already contained sufficient information for probable cause).

Finally, defendant argues that a *Franks* hearing is necessary to determine the import of the missing videos and photographs of the April 8 Moocherhunter readings. At the court's invitation, the parties submitted supplemental briefing to clarify whether this missing information by itself warrants a *Franks* hearing. (ECF 49, 50, 51.) After careful consideration, the court concludes it does not.

Defendant asks the court to infer that the missing documentation of the readings would demonstrate that the Moocherhunter software did not, in fact, show that the wireless signal was coming from Apartment 243, negating probable cause. (ECF 49 at 1, 3.) In arguing that the loss of evidence merits this inference, defendant relies on *United States v. Sivilla*, 714

F.3d 1168 (9th Cir. 2013). The defendant in *Sivilla* was arrested after border patrol agents found drugs hidden inside the engine manifold of his jeep. *Id.* at 1170. In response to the defendant's request, the government agreed to preserve the jeep as evidence, and the court subsequently granted the defendant's motion to preserve evidence. *Id.* However, without the knowledge of the Assistant U.S. Attorney or the case agent, the Department of Homeland Security forfeited the jeep. *Id.* at 1170-71. The Ninth Circuit affirmed the district court's determination that the government acted negligently but not in bad faith, *id.* at 1172, but held that the district court abused its discretion in not granting a remedial jury instruction to the defendant, *id.* at 1174.

Defendant asserts that *Sivilla* stands for the proposition that there must be a remedy for the government's negligence here. (ECF 49 at 3.) While this may be true, the court is not convinced that drawing an inference that the missing photographs and video were exculpatory so as to justify a *Franks* hearing is the appropriate remedy. That several photographs and video are missing, without any other indication they were exculpatory, does not meet the standard for a "substantial preliminary showing" that contradicts the "presumption of validity" of Agent Phirippidis's statements in the affidavit describing the Moocherhunter readings. *Franks*, 438 U.S. at 171. Under *Franks*, allegations that the statements in the affidavit are false must be accompanied by "[a]ffidavits or sworn or otherwise reliable statements of witnesses . . . or their absence satisfactorily explained." *Id.; cf. United States v. Jeffus*, 22 F.3d 554, 557-58 (4th Cir. 1994) (the possibility that missing witnesses had information to refute the information in the affidavit submitted in support of a warrant was insufficient grounds for a *Franks* hearing). Defendant has not made such a proffer here.

Defendant's request for a *Franks* hearing is denied, although defendant may seek a remedial jury instruction addressed to the missing records at trial.

III. MOTION TO SUPPRESS

Defendant contends the government's use of Moocherhunter software to detect defendant's Internet transmissions constituted a warrantless search in violation of the defendant's Fourth Amendment rights. (ECF 42 at 9.) A search occurs when the government

trespasses on the "persons, house, papers, or effects" of the defendant, or there is a violation of a reasonable expectation of privacy. *United States v. Jones*, 565 U.S. ___, 132 S. Ct. 945, 949-50 (2012).

The government argues there was no violation of defendant's Fourth Amendment rights because there was no trespass onto defendant's property, and defendant had no reasonable expectation of privacy in the signals transmitted through his neighbor's wireless internet connection. (ECF 43 at 5-11.) As explained below, the undisputed facts support the conclusion that use of Moocherhunter was not a search.

A. No Trespass

Defendant argues that using Moocherhunter to "sniff the air waves coming from inside Mr. Norris' bedroom, to discover the location of a computer inside his bedroom that otherwise could not have been seen without actually being in the home, intrudes into areas of his home that he has a reasonable expectation of privacy will not be trespassed." (ECF 42 at 9-10.) The government contends no trespass occurred as the Moocherhunter was only "passively" detecting Internet traffic coming from defendant's home. (ECF 43 at 5.)

Defendant relies heavily on the recent case of *Florida v. Jardines*, ___ U.S. ___, 133 S. Ct. 1409 (2013). In *Jardines*, the police used a drug-sniffing dog on a suspect's front porch without a search warrant. *Id.* at 1413. The Court held this use was a search, explaining that the front porch "is the classic exemplar of an area adjacent to the home" and is considered the home's "curtilage," which has been widely protected by the Fourth Amendment. *Id.* at 1415. By using the drug-sniffing dog in this area, the police made an unwarranted physical intrusion. *Id.* at 1414. In this case, however, law enforcement made no physical intrusion into the defendant's property or anything equivalent to the curtilage; rather, agents obtained permission to use Moocherhunter only passively while standing with permission in other apartments or in common areas. (ECF 42 at 5.) Thus, no physical trespass onto the defendant's property occurred.

/////

/////

B. No Reasonable Expectation of Privacy

Defendant contends he had a reasonable expectation of privacy in his bedroom, and a reasonable expectation of privacy in the location of his computer within that bedroom. (ECF 42 at 11.) The government argues he had no expectation of privacy because defendant "knowingly and intentionally transmitted radio signals from inside his apartment to a location defendant knew had to be outside his apartment[.]" (ECF 43 at 7.)

In determining whether a reasonable expectation of privacy has been violated the court conducts a two-part analysis: "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 (1986) (citing *Katz v. United States*, 389 U.S. 347, 360 (1967) (Harlan, J, concurring)). In *Katz*, the Court held government agents' use of a listening device on a telephone booth constituted a search in violation of the Fourth Amendment because the defendant had a reasonable expectation of privacy in his telephone conversation. *Katz*, 389 U.S. at 351. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Id.* at 351.

Later, the Court in *Smith v. Maryland* determined that the government's use of a pen register to record the phone numbers that a suspect dialed on his telephone, without a warrant, was not a violation of the Fourth Amendment. 442 U.S. 735, 745 (1979). The Court reasoned, "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. In *Smith*, the Court distinguished *Katz* based on the fact that unlike the listening device used by the authorities in *Katz*, pen registers do not obtain the contents of the conversations. *Id.* at 741.

Here, the use of Moocherhunter is more analogous to the use of the pen register in *Smith* than the listening device used in *Katz*, in that Moocherhunter does not capture the

contents of the target user's Internet activity, only the strength of the target signal. (ECF 43 at 4.) Defendant had no expectation of privacy when he initiated a wireless signal from his computer to the wireless router located in Apartment 242, as he "assumed the risk" his information would be conveyed to law enforcement by Apartment 242's occupants. *See Smith*, 442 U.S. at 744.

Defendant also argues, however, that the agents' actions here were similar to those of the agents in *Kyllo v. United States*, 533 U.S. 27 (2001), in which the Supreme Court reversed the district court's denial of a defendant's motion to suppress. (ECF 42 at 10-11). In *Kyllo*, government agents stood on the public street outside the home of a suspected marijuana grower and used thermal imaging devices to scan his home. 533 U.S. at 29-30. The imaging devices detected thermal "hot spots," suggesting there were fluorescent lights used inside for growing marijuana. *Id.* Agents then used this information to obtain a search warrant for the defendant's residence. *Id.* Even though the agents were outside a constitutionally protected area when they conducted their scans, the Court reasoned "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, constitutes a search." *Id.* at 34 (internal citations omitted). In this case the agents used Moocherhunter to pick up signals the defendant was voluntarily transmitting to the Apartment 242 router, not information confined to the private area of defendant's home. And Moocherhunter in the passive mode did not enhance the agent's senses in a way that allowed for intrusion into Apartment 243.

Generally there is no expectation of privacy for internet data voluntarily turned over to third parties. *See Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 905 (9th Cir. 2008), *reversed and remanded on other grounds by City of Ontario, Cal. v. Quon*, ___ U.S. ___, 130 S. Ct. 2619 (2010); *United States v. Forrester*, 512 F.3d 500, 509 (9th Cir. 2008) (citing *Smith* and holding the use of computer surveillance techniques that revealed email addresses was not a search because Internet users have no expectation of privacy in content that is voluntarily communicated to third parties). In *United States v. Stanley*, another district court

recently denied the defendant's motion to suppress evidence obtained by government agents with Moocherhunter software. No. CRIM. 11-272, 2012 WL 5512987 (W.D. Pa. Nov. 14, 2012). The court reasoned the defendant "did not have a legitimate expectation of privacy in the wireless signal he caused to emanate from his computer to [a third party] wireless router or in the signal being sent from the router back to his computer, and therefore, [government's] use of Moocherhunter did not constitute a search in violation of the Fourth Amendment." *Id.* at *12. This court's understanding of the Moocherhunter software is consistent with that of its sister court in Pennsylvania.

Moreover, societal interests do not support recognizing defendant's reasonable expectation of privacy in data transmitted without authorization to Apartment 242's password-protected wireless router. In *United States v. Caymen*, the defendant obtained a laptop from a store through the use of a fraudulent credit card. 404 F.3d 1196, 1197 (9th Cir. 2005). Police later recovered the laptop, and obtained the store's permission to search the computer. *Id.* at 1198. Police recovered child pornography from the laptop and the defendant was charged. *Id.* In denying the defendant's motion to suppress the evidence obtained from the computer, the court reasoned "one who takes property by theft or fraud cannot reasonably expect to retain possession and exclude others from it once he is caught. Whatever expectation of privacy he might assert is not a legitimate expectation that society is prepared to honor." *Id.* at 1201.

Similar to the defendant in *Caymen*, the defendant here transmitted information through an internet connection he did not have permission to use. (ECF 43 at 7.) Specifically, defendant hacked into Apartment 242's wireless Internet router and used the Internet without those occupants' consent. (*Id.*) The agents used Moocherhunter to detect the router activity with permission of the router's owners. (ECF 43 at 3.) Any expectation of privacy the defendant may have had is trumped by the lawful owners' authorization given to the government. *See Caymen*, 404 F.3d at 1201.

Because there was no trespass on the defendant's property and defendant had no reasonable expectation of privacy society is willing to protect, the court denies his motion to suppress.

ACCORDINGLY, the court orders as follows:

1. Defendant's motion for a *Franks* hearing is denied.

2. Defendant's motion to suppress on Fourth Amendment grounds is denied.

IT IS SO ORDERED.

DATED: August 30, 2013.

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

---oOo---

BEFORE THE HONORABLE KIMBERLY J. MUELLER, JUDGE

---oOo---

UNITED STATES OF AMERICA,

Plaintiff,

vs. No. 2:11-cr-0188

ALEXANDER NATHAN NORRIS,

Defendant.

_____/

---oOo---

REPORTER'S TRANSCRIPT

MOTION HEARING

THURSDAY, MAY 29, 2013

---oOo---

Reported by: DIANE J. SHEPARD, CSR #6331, RPR

Appendix C

APPEARANCES

For the Government:

BENJAMIN B. WAGNER
UNITED STATES ATTORNEY
501 I Street, Suite 10-100
Sacramento, California 95814
BY: MATTHEW G. MORRIS
Assistant U.S. Attorney

For the Defendant:

HEATHER WILLIAMS
FEDERAL DEFENDER
801 I Street, Third Floor
Sacramento, California 95814
BY: LEXI NEGIN
MATTHEW SCOBLE
Assistant Federal Defenders

SACRAMENTO, CALIFORNIA

THURSDAY, MAY 29, 2013

---oOo---

THE CLERK: Calling criminal case 11-188, United States versus Alexander Nathan Norris. This is on for a motion hearing.

THE COURT: Good morning, appearances, please.

MR. MORRIS: Good morning, Your Honor. Matt Morris for the United States.

THE COURT: Good morning, Mr. Morris.

MS. NEGIN: Good morning, Your Honor. Lexi Negin and Matt Scoble on behalf of Alexander Norris, who is present. He is out of custody, Your Honor.

THE COURT: Good morning to you both and to Mr. Norris.

This is on based on the defense motion for suppression and a Franks hearing. I have two primary questions. First is, is there a discovery motion pending?

MS. NEGIN: There is not, Your Honor. And I wanted to bring that up today as well.

THE COURT: Is it possible that you should exhaust a discovery motion before I resolve whether or not to grant you a hearing?

MS. NEGIN: Your Honor, well, it sort of is. I believe, from what the Government has told me, and I think the

Government agrees with us, that the -- affirmatively the evidence does not exist. It existed and it's been lost, or misplaced, or something has happened to it. That seems to be the affirmative conclusion of where that evidence is.

I would like to file something with respect to the import of that especially given new case law, recent case law.

THE COURT: So would you be filing a motion to compel in front of the magistrate judge? Or you'd be filing something for a determination by this Court of the legal conclusions to be drawn?

MS. NEGIN: The latter. That's where I feel we are. I can certainly do the former. I think we can shortcut that because Mr. Morris and I have been working with each other. Mr. Morris has been very cooperative about the discovery. And, you know, I think unless he wants to say something additional, I think the evidence just doesn't exist anymore.

And the question is whether -- I suppose there is a question of whether it ever existed in the first place, and it's been lost or destroyed, and whether that was negligent or in bad faith.

I don't know of any evidence, from what Mr. Morris is telling me, that there would be evidence of bad faith. It would be evidence that it was lost negligently.

THE COURT: All right.

MS. NEGIN: So I think, presuming those things, that

the next place would be the legal significance of that. And I do think that that affects very much the outcome of the Franks portion of the motion.

On the first part of the motion, Your Honor, I wanted to say to the Court that we submit on the pleadings. I don't think there is a reason to have any kind of evidentiary hearing on the first part of the motion.

THE COURT: On the motion to suppress?

MS. NEGIN: Right. Well, the whole thing is a motion to suppress, but on the argument about the search issue.

THE COURT: Well, I have a question about that.

But, first, Mr. Morris, anything to add to the record on whether or not there is further discovery that could be produced?

MR. MORRIS: Let me kind of explicitly kind of go through what we're talking about. There is, to my knowledge, nothing else that can be produced in response to the request.

We have traded some e-mails, compared Bates numbers, compared what's in the discovery. I think we've ironed out some -- I think what both of us were confused on with respect to some handwritten notes and where they fell into the scheme of what happened on these various dates.

The items that Ms. Negin is referring to are the report that was written on the 14th of April about the 8th of April investigation mentions taking photographs of and video of

the Moocherhunter device in process and states that those are burned to a CD and saved in the file. There is no CD with those documents on them or those files on them in the file.

That same report refers to another disk which has packet capture information on it. That is in the file there.

So I think what I can proffer to the Court, I have actually reviewed the file personally, and I don't think that disk is in there.

Assuming that the report is correct, that the items were burned to a disk, that disk is missing. I have spoken with all of the agents who were involved in that transaction, and they can't give me -- and therefore I can't give the Court or defense -- any further explanation.

We could speculate, but I think it's -- I think we can agree that at this point my best understanding is that that disk with those photos and video, assuming it was made, is no longer in the file.

THE COURT: And it was entirely photos of the Moocherhunter device?

MR. MORRIS: That is what the report states, and that's what the agent's recollection is that that was what they did. I think Agent Phirippidis says he had directed Agent Holtz to take some photographs in the course of the process. Agent Holtz's report from the 14th states that he did take those photos, burned them to a disk. That disk can't be found.

So assuming that the disk was made as Agent Holtz says it was, and that as Agent Phirippidis directed him to, if that disk existed at one point, we can't find it now.

THE COURT: So you agree that describes, Ms. Negin, what has not been produced and is apparently no longer available, if it ever existed?

MS. NEGIN: Right.

And, Your Honor, I would just point out to the Court that the report that Mr. Morris is talking about has been submitted to the Court as Exhibit J to the defense motion. It's Bates stamp number 170. It's the pictures and the video.

And then also, this is less clear, but 17 readings were taken on one day, and 16 readings were taken on the other day. It's not clear whether those readings were written down. It's probably the case that those readings appeared in these photographs and video of the Moocherhunter process, but those things -- I don't have those readings -- what those readings were either. And it's less clear whether that ever existed in a different form than the photographs and the video.

THE COURT: But you've received no other discovery that contains the results of those readings?

MS. NEGIN: Right. Except for those two diagrams that are in the pleadings that we submitted to the Court. And one of them seems to have about seven readings, and the other one seems to have about six.

And I believe Mr. Morris has told me that those are both from April 1st, which is not really as important as the readings from April 8th. Because the readings from April 8th were the ones taken while the agent knew that the child pornography was being traded. And actually, the April 1st device that they were picking up was not a device that had any child pornography associated with it. Except the agents were making a conclusion that those two things were associated with each other.

THE COURT: Anything to add to that record?

MR. MORRIS: There is.

I think with respect to the handwritten notes, again, after receiving Ms. Negin's reply to the opposition, we talked to make sure that I hadn't inadvertently left something out.

I went back and re-looked at the reports over the weekend, a couple weekends ago, and my reading of the report -- this is Bates 10, which details the April 1st investigation -- says handwritten notes were taken. And the report detailing the April 8th investigation, written on the 14th of April, does not mention handwritten notes. I have spoken to the agents, and they've confirmed any handwritten notes related to the April 1st investigation. So those --

MS. NEGIN: What?

MR. MORRIS: Related to the April 1st investigation.

THE COURT: So there is no documentation of readings

on April 8th unless they were in the CD that is no longer available?

MR. MORRIS: Correct. In terms of actual numbers, correct. The documentation that exists is Agent Phirippidis' affidavit, Agent Holtz's report, and that would be it.

I would also say that it is true that the April 8th readings were substantial. In fact, we wouldn't have asked the magistrate for the search warrant without the April 8th reports. But it's not true that the April 1st reports were not relevant to the probable cause. It is listed in the affidavit. And, in fact, Agent Phirippidis when he says -- when he talks about the April 8th readings says, we got readings pointing to this location. And he says they were consistent with the readings on April 1st. He refers back to that previous paragraph.

So while it is true that there were two independent days, it isn't as if the April 1st readings were not even included amongst the probable cause that was presented to Judge Hollows on that second affidavit.

MS. NEGIN: I'm sorry. The Government said that the April 1st readings notes were taken, but those notes don't exist?

MR. MORRIS: No. As I wrote in the e-mail to you, that Bates 178 to 179, handwritten notes, router settings. Then we talked about the videos, the router, the investigation

on April 1st. And then Bates 176 to 177, handwritten notes of readings from April 1st.

MS. NEGIN: Those are the diagrams.

THE COURT: Yeah, I understand that.

Help me understand the defense position. The Government has responded addressing the argument that the search warrant affidavit erroneously created the impression that there was only one possibility for evaluation when there were these 28 other or so other possible users.

MS. NEGIN: Right.

THE COURT: The Government has responded saying at the relevant time there were only, I guess, two -- at one point two users and then ultimately only one user with the MAC address that led to Mr. Norris' apartment.

MS. NEGIN: Right.

Your Honor, what the Government says is true is that on the date, April 8th, that they were actively engaged with that device. That there was only one device connected.

THE COURT: But that was the same date when they were back by consent in the one apartment and by consent in the vacant apartment.

MS. NEGIN: Right.

The point that I was trying to make in the motion about the 28 other devices is that there is -- according to the report, there were 33 devices connected, and there was no --

the router did not indicate when those things had been connected.

Four were identified as known to the people in the apartment and the agents. So the remainder were not. The reason why that's relevant is because of how much traffic is going on in this area to this router from different apartments around.

And what's important about that is what -- is how it connects to Moocherhunter. Because what Moocherhunter is doing -- what they are doing by using Moocherhunter, supposedly, is finding probable cause for one apartment over -- to the exclusion of the other 200 apartments or the public space. When -- so the fact that there is a lot of --

THE COURT: I understand the argument, but if they've narrowed it down -- if they actually have a single user with a certain MAC address, why can't that establish probable cause?

MS. NEGIN: Your Honor, the point being was that the information in the affidavit was misleading with respect to leading the Court to believe that there was always only one or two. I think the affidavit fairly says two.

And so you have to look within the four corners of the affidavit to see if the information is accurate. It just factors into what the agent is doing here to sort of, you know, color this --

THE COURT: I understand that.

MS. NEGIN: That's all. But I agree --

THE COURT: Why didn't the agent mention -- I mean, I can't look at all the exhibits now attached to your motion. I look at what was in the affidavit.

Why wasn't it a little more helpful? Why describe the -- I mean, it never used the word Moocherhunter.

MR. MORRIS: It didn't. I think that's correct.

THE COURT: Why not just lay it out there and say this is the tool we're using, this is what we know about it.

MR. MORRIS: Because I don't think it was necessary, Your Honor.

For the same reason, for example, that when we see an affidavit where an investigator says, you know, I conducted a publically accessible database search to learn who lives at that house. We don't ask them to say, I logged into my Dell computer, I started up Internet Explorer 9.0, and I used it to access this other database. We don't even go to the point necessarily of asking the agents to say, I accessed Westlaw or Lexis Nexis database. We say, I used a tool that let's me do X, and it gave me the following information.

So I don't think there was any requirement, necessarily, to tell Judge Hollows that he used Moocherhunter, as opposed to Shadow, as opposed to -- there is a device called Flying Squirrel that's made by the military that does the same thing.

I don't think that adds anything. And as the agent writes in this affidavit, as he does -- as all of our agents write in their affidavits -- I've presented only the items that are necessary to establish probable cause. It's not an exhaustive cataloging of everything I know about the investigation.

I'm not sure whether naming Moocherhunter would have necessarily helped Judge Hollows. I certainly don't think it would have detracted from probable cause not to have it in there. What's relevant to probable cause is this is a device that allows a directional antenna to locate a transmitting radio beacon.

THE COURT: Do you agree that the DOJ's position has changed since the time the affidavit was presented with respect to Moocherhunter?

The defense argues that some of what's attached to your motion wasn't in effect at the time of the affidavit's presentation?

MR. MORRIS: To the contrary. In fact, the motion makes clear that, in fact, an entire year prior to this affidavit, the Department of Justice was teaching the use of Moocherhunter. That was at the ICAC Law Enforcement National Training Symposium in May of 2010 in Jacksonville, Florida.

And that's the -- that's related to the declaration regarding the detective from Florida. He was invited by the

Department of Justice to provide national training. That was a year prior to it.

And then in addition I said that one of the agent's -- one of the agent's declarations says and four months later he received FBI training that talks about Moocherhunter.

So the Government's position is that the Department of Justice, both through the ICAC Law Enforcement Training and then through FBI training, bookends this. Both a year prior and four months after, Moocherhunter is being taught as an acceptable investigative technique.

Ms. Negin only hones in on the second one. She mentions the fact that this one happens in August of 2011. Ignoring the fact that what I'm saying is that from 2010 through 2011, DOJ is saying it's an accepted technique.

THE COURT: Clarify your position in response to that argument.

MS. NEGIN: Your Honor, the -- this -- apparently this sheriff -- I was relying originally on the Government's discovery letter to me saying there was no training. That was my initial --

THE COURT: Forget about what's water under the bridge. Respond to that argument you just heard.

MS. NEGIN: Your Honor, this doesn't say that any of our agents here went to that training. And the mention of it in an FBI training was after the fact. So I don't know about

whether these agents went to the 2010 Internet Crimes Against Children Law Enforcement Training Conference. And I also don't know what they trained about Moocherhunter.

Because there is nothing here from Detective Speakman. There's only the information from Mr. Morris talking to Detective Speakman with Polk County Sheriff's Department in Florida. He apparently spoke at that conference. But I don't know that that means that any of these agents received any training in it.

And if they had, Your Honor, I submit that it should have been in the affidavit. It should have been in the affidavit seeking this warrant.

The problem that the Government -- well, I'll let the Court continue to ask questions.

THE COURT: Here's my final question.

With respect to the technology itself, I can't tell if there's a real dispute about the way in which the technology works.

And is it possible for the parties to reach a stipulation about the way in which the technology works?

I know some courts have written about it. I don't have to defer or rely on another court's description. But is it agreed that this passive directional antenna, there is nothing like pinging? There's nothing, even if invisible, that penetrates a space? That the --

MS. NEGIN: No.

THE COURT: -- the tool is entirely outside of the space and is simply receiving information?

MS. NEGIN: I agree that in this particular instance they used the mode that required the computer they were looking for to be connected to the router, and so that was a passive -- that was a passive use of it.

And I believe that based on what my expert told me and based on what the Government has represented about what they did, that that's true. That they did not -- there is a different way to use Moocherhunter --

THE COURT: You said that.

MS. NEGIN: -- MAC address. And if they had done that, it would have gone into the apartment.

THE COURT: What happened here? So is it essentially stipulated, and therefore that means -- the passive use means that this tool was outside of Mr. Norris' apartment, and it was not in any way entering the physical space of the apartment electronically or otherwise?

MS. NEGIN: Right. I agree with the Court about what the Court just said. The only difference -- the only nuance there is that the location of the computer is inside the apartment. And to the extent that the Moocherhunter program is reading information that comes from inside the apartment, they are getting inside the apartment.

THE COURT: But it's reading it entirely outside?

MS. NEGIN: Yes. I think so.

MR. MORRIS: We would agree, Your Honor.

MS. NEGIN: Well, it's reading it -- sorry to interrupt. It's reading it -- that's not really true because it's reading it from the device which is inside the apartment.

THE COURT: It's because that device is sending out signals.

MS. NEGIN: That's correct.

THE COURT: It's not because the Moocherhunter is sending any kind of signal or any wave, or whatever it might be. It's not sending anything into the apartment.

MS. NEGIN: I agree with that in this case.

MR. MORRIS: We would agree also, Your Honor. And I'm less familiar with the other mode of operation as far as the sending a signal in to make the computer respond. Because my explicit instructions to the agents was don't even use that mode. So the instruction was absolutely only use it in a mode that would only listen and would not send any kind of a signal into the apartment.

THE COURT: All right. With that essential stipulation there is no need for an evidentiary hearing on that --

MS. NEGIN: Right.

THE COURT: -- question.

So then there is the Franks question. I need to go read the search warrant affidavit closely again to see if I think there is a need for a Franks hearing. So I'm going to take that matter under submission.

If there is anything else I really need to know despite what's in the briefing, you can let me know in a few minutes now.

MR. MORRIS: If I can have one item, Your Honor. And that is this, it's not necessarily clear from how we talked about this, but an aspect of the timeline that I think is relevant to the Court's potential Franks concerns -- and I'll lay it out from April 8th onward.

April 8th they go to the neighbor's house, again with their consent, and they do the investigation. And that's recorded on a 302 that is actually written on the 14th of April.

So Friday, April 8th, they go to that apartment. Agent Phirippidis sends the draft search warrant to me the evening of Sunday, April 10th. That's not in discovery, but I can send the e-mail to the defense if they want.

But what is in discovery is that it was presented to Judge Hollows then on Monday, the 11th. Judge Hollows signs it on Monday, the 11th. They execute the search warrant on April 12th. The report about the April 8th investigation was written April 14th, so two days after the search warrant is executed.

To the extent that the Court is concerned about the missing photos and video, a concern frankly that the Government shares and has expressed to the FBI, to the extent that that would cause the Court to question the report from that date, that report post dates the execution of the warrant.

The warrant affidavit is Agent Phirippidis' affidavit relying on his own independent recollection. It couldn't have been relying on the report because the report was written six days later.

And so while I accept that there are concerns about the potential loss of the equivalent of notes, frankly, this photographic equivalent of notes for that April 8th day, and to the extent that that causes the Court to be concerned about the reliability of that 302, that 302 could not have formed the basis for Agent Phirippidis' affidavit for Judge Hollows that he signed on April 11th.

THE COURT: Any response to that Ms. Negin, Mr. Scoble?

MS. NEGIN: Well, Your Honor, the April 8th affidavit -- I'm sorry -- the April 8th 302 report, I believe, is also penned -- wait, let me just check for one second, Your Honor. May I have one moment?

THE COURT: The representation is on August 14th. Do you dispute that?

MS. NEGIN: So the report -- the 302 is penned by

both Agent Holtz and Agent Phirippidis. So it's not the fact of the 302 that matters. It's the information in it was available to Agent Phirippidis on the 11th.

I don't think the report about the readings -- about taking the readings and taking the pictures and the video is wrong. I think the agents did take pictures. And I think they did take video. And I think they did take readings. We just don't have them.

So the report is only being referenced with respect to the fact that that evidence doesn't exist anymore and certainly was discoverable evidence.

My suggestion to the Court, on the first prong of Franks we believe -- the first part of Franks we believe we've established that there was a deliberate omission of material information.

But the second part of Franks having to do with whether or not if that material had been included would have affected the probable cause search determination, I believe that this discovery issue does factor into that.

So if the Court would allow, I would like to present something to the Court about the legal import of this lost information. Because I do believe it factors into what the Court should do with respect to the second part of Franks; in other words, my showing that probable cause would have been affected by the omission.

THE COURT: I understand that. Is that really the order in which it needs to be determined?

MS. NEGIN: It isn't. But if the Court wanted me to file something about that?

THE COURT: I understand where you're going with that. I think the real question is, should the record be developed with respect to the missing information and why it might be missing.

MS. NEGIN: Right. And then next --

THE COURT: What it might have said.

MS. NEGIN: And then next is what the import is to probable cause.

THE COURT: Right.

MS. NEGIN: Okay. Then I agree, Your Honor.

THE COURT: All right. So the Franks question is submitted. I'll let you know in an order shortly.

MS. NEGIN: And, Your Honor, if we do -- we could, if the Court wanted to -- I know that your calendar is extremely busy. And if we do have a hearing, I would need to have experts here. We were looking with the clerk at an August date for a hearing if the Court -- I would just suggest that now so if the Court issues an order and does grant a hearing, we could do it on the date that we've cleared with everybody. The date is August 26th.

The Government and I both agree that if this is a

hearing, it might take a couple days. So the clerk looked at August 26th and 27th as fairly clear. Two days is outside. Is a very outside guess.

But we were -- so if the Court issued an order and did ask for a hearing, I would ask that the Court schedule that for August 26th.

MR. MORRIS: And the 26th is fine with the Government. I think it may be a one- or two-day process. I think that may be driven perhaps by the -- I know the Court's previous practice has been the order -- and again the Government doesn't think we need a hearing. But I note in previous cases the Court has issued an order with respect to the only -- this will be the following question which will be at issue in the hearing. I think that if it's narrowed, that could affect questions about how many witnesses might come.

But, again, you know, the Government's view being that evidence that may have gone missing days, if not months afterwards, could not possibly have had any effect on the affidavit, and therefore couldn't affect probable cause for the warrant.

THE COURT: I understand that position. Would it be just Agent Phirippidis or would it be the second agent as well on the 302 report?

MS. NEGIN: I would certainly -- I would probably end up, if the Government didn't put on many of the agents that

were present, I would probably put them on depending on what the question -- the Court wanted. I mean, those --

THE COURT: We don't need to get into those details now. So I'll keep in mind those August dates. There are quite a few trials showing this summer, so that's also a factor. But those often have a way of resolving. All right. You'll know shortly what my view is. Thank you.

(End of transcript.)

CERTIFICATION

I, Diane J. Shepard, certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/s/ DIANE J. SHEPARD
DIANE J. SHEPARD, CSR #6331, RPR
Official Court Reporter
United States District Court

FILED

FEB 4 2020

MOLLY C. DWYER, CLERK
U.S. COURT OF APPEALS

UNITED STATES COURT OF APPEALS

FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, Plaintiff-Appellee, v. ALEXANDER NATHAN NORRIS, Defendant-Appellant.	No. 17-10354 D.C. No. 2:11-cr-00188-KJM-1 Eastern District of California, Sacramento ORDER

Before: SCHROEDER, O'SCANNLAIN, and RAWLINSON, Circuit Judges.

The panel has voted to deny the Petition for Panel Rehearing. Judge Rawlinson voted, and Judges Schroeder and O'Scannlain recommended, to deny the Petition for Rehearing En Banc.

The full court has been advised of the Petition for Rehearing En Banc, and no judge of the court has requested a vote.

Defendant-Appellant's Petition for Panel Rehearing and Rehearing En Banc, filed December 27, 2019, is DENIED.

EXHIBIT A

(Affidavit in Support of Search Warrant for Apt 243)

FILED

APR 11 2011

CLERK, U.S. DISTRICT COURT
EASTERN DISTRICT OF CALIFORNIA
DEPUTY CLERK

UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of
(Name, address or brief description of person, property or premises to be searched)

[redacted], APARTMENT 243
DAVIS, CALIFORNIA 95616

APPLICATION AND AFFIDAVIT FOR SEARCH WARRANT

Case Number:
2 1 1 - SW - 1 5 0 GGH

I, NICHOLAS G. PHIRIPPIDIS, being duly sworn depose and say:

I am an FEDERAL BUREAU OF INVESTIGATION SPECIAL AGENT and have reason to believe that
☐ on the person of or ☒ on the property or premises know as (name, description and/or location)

SEE ATTACHMENT A, ATTACHED HERETO AND INCORPORATED BY REFERENCE,

in the EASTERN District of CALIFORNIA
there is now concealed a certain person or property, namely (describe the person or property to be seized)

SEE ATTACHMENT B, ATTACHED HERETO AND INCORPORATED BY REFERENCE,

which is (state one or more bases for search set forth under Rule 41(c) of the Federal Rules of Criminal Procedure)

PROPERTY THAT CONSTITUTES EVIDENCE, FRUITS AND INSTRUMENTALITY OF A CRIMINAL OFFENSE

concerning violations of Title 18 United States Code, Sections 2252 and 2252A - Illegal Production, Distribution, Receipt and Possession of Visual Depictions of Minors Engaged in Sexually Explicit Conduct and Child Pornography. The facts to support a finding of probable cause are as follows:

See Attached Affidavit of Federal Bureau of Investigation Special Agent Nicholas G. Phirippidis attached hereto and incorporated by reference.

Continued on the attached sheet and made a part hereof: ☒ Yes ☐ No

Signature of Affiant
NICHOLAS PHIRIPPIDIS
FEDERAL BUREAU OF INVESTIGATION

Sworn to before me and subscribed in my presence,

APRIL 11, 2011 at SACRAMENTO, CALIFORNIA
Date City State

GREGORY G. HOLLOWS

GREGORY G. HOLLOWS
Name of Judge Title of Judge

Signature of Judge

AFFIDAVIT OF SPECIAL AGENT NICHOLAS G. PHIRIPPIDIS IN SUPPORT OF SEARCH WARRANT

I, Nicholas G. Phirippidis, being duly sworn, depose and state:

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), presently assigned to the Sacramento Division Cyber Squad. I have been employed by the FBI since November 2007.

2. My formal education includes a Bachelor of Science degree in Computer Science, through the University of California, San Diego. My coursework involved the study of programming languages, computer systems, and Internet security. Prior to my employment with the FBI, I was a software application engineer for a Department of Defense contractor.

3. At the outset of my employment with the FBI, I attended 22 weeks of training at the FBI Academy in Quantico, Virginia. Part of that training included courses addressing basic criminal law, federal court procedures, and various investigative techniques. Particularly, I received instruction regarding computer forensic examinations and techniques pertaining to cyber investigations. I have also completed a 40 hour Internet Investigations – Online Certification Course that focused on conducting Innocent Images investigations online.

4. I have also taught and assisted with several Internet security classes for the general public and other law enforcement agencies. Specifically, I have presented on such topics as Internet social networking sites, like "MySpace" and "Facebook", and safe Internet practices for parents and students.

5. My daily duties as an FBI agent include the investigation of criminal violations relating to child exploitation, including violations pertaining to the illegal production, distribution, receipt and possession of visual depictions of minors engaged in sexually explicit conduct and child pornography (as those terms are defined in 18 U.S.C. § 2256 and hereinafter referred to collectively as "child pornography") in violation of 18 U.S.C. §§ 2251, 2252(a) and 2252A. I have received training in the area of identifying and investigating child pornography and child exploitation crimes, and as part of my duties have observed and reviewed numerous examples of child pornography in all forms of media, including computer media. In the course of my duties, I have assisted in the execution of numerous search warrants, including several relating to child exploitation investigations.

INTRODUCTION

6. The FBI is currently investigating the possession, receipt, and distribution of child pornography through the use of a sophisticated peer to peer file sharing program/network. As discussed more fully within, investigation thus far has demonstrated that there is probable cause to believe that a computer user at [redacted], **Apartment 243, Davis, California, 95616** (the "SUBJECT PREMISES") possessed, received, and distributed child pornography through a computer network for files to be shared. For that reason, this affidavit is made in support of an application for a warrant to search the SUBJECT PREMISES. I believe that located within the SUBJECT PREMISES are evidence, fruits, and instrumentalities of criminal violations relating to the knowing possession, receipt, and distribution of child pornography.

7. The SUBJECT PREMISES to be searched is more particularly described in "Attachment A" of this affidavit, affixed hereto and fully incorporated herein. I request authority to search the entire SUBJECT PREMISES, including the residential dwelling and any computer and computer media located therein, where the items specified in Attachment B may be found, and to seize all items listed in Attachment B as instrumentalities, fruits, and evidence of the crimes enumerated in the affidavit. The search is to include all rooms, attics, basements, and all other parts therein, and surrounding grounds, garages, storage rooms, or outbuildings of any kind, attached or unattached, associated with the SUBJECT PREMISES. In addition, because I know that it is common practice for persons involved in the trafficking of child pornography to hide and transport child pornographic materials and/or their instrumentalities in vehicles, I request that the search warrant authorize the search of vehicles located at or near the residence that fall under the dominion and control of the person or persons associated with said residence. The search of these vehicles is to include all internal and external compartments and all containers, of the size that could store child pornographic materials, media, or their instrumentalities, located within the aforementioned vehicles.

8. The statements in this affidavit are based in part on information provided by other law enforcement agents, as well as my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. §§ 2252(a) and 2252A are presently located at the SUBJECT PREMISES.

9. To my knowledge, there have been no applications to obtain information pursuant to 18 U.S.C. § 2703 and no attempts through earlier search warrants to obtain the evidence, fruits, and instrumentalities sought in this warrant from the SUBJECT PREMISES.

RELEVANT STATUTES

10. This investigation concerns alleged violations of 18 U.S.C. §§ 2252 and 2252A, relating to possession, receipt, distribution, and transportation of material involving the sexual exploitation of minors. The statutes, in pertinent part, are set forth below:

18 U.S.C. § 2252

(a) Any person who

(1) knowingly transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mails, any visual depiction, if

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(2) knowingly receives, or distributes, any visual depiction using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer, or knowingly reproduces any visual depiction for distribution using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or through the mails, if

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(3) ...

(4) either

(A) ...; or

(B) knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if

(i) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(ii) such visual depiction is of such conduct;

shall be punished as provided in subsection (b) of this section.

18 U.S.C. § 2252A

(a) Any person who

(1) knowingly mails, or transports or ships using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any child pornography;

(2) knowingly receives or distributes

(A) any child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or

(B) any material that contains child pornography that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

(3) knowingly

(A) ...; or

(B) advertises, promotes, presents, distributes, or solicits through the mails, or using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, any material or purported material in a manner that reflects the belief, or that is intended to cause another to believe, that the material or purported material is, or contains

(i) an obscene visual depiction of a minor engaging in sexually explicit conduct; or

(ii) a visual depiction of an actual minor engaging in sexually explicit conduct;

(4)...;

(5) either

(A) ...; or

(B) knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

... shall be punished as provided in subsection (b).

Pursuant to 18 U.S.C. §§ 2253, 2254, "any visual depiction described in [Title 18, United States Code,] sections 2251, 2251A, or 2252 2252A, 2252B, or 2260 of this chapter, or any book, magazine, periodical, film, videotape, or other matter which contains any such visual depiction, which was produced, transported, mailed, shipped or received in violation of this chapter" is subject to criminal or civil forfeiture. In addition, pursuant to 18 U.S.C. §§ 2253, 2254, "any property, real or personal, used or intended to be used to commit or to promote the commission of such offense or any property traceable to such property" is subject to criminal or civil forfeiture.

DEFINITIONS

11. The following non exhaustive list of definitions applies to this Affidavit and Attachments A, B and C to this Affidavit:

a. "Child Pornography" includes the definition in 18 U.S.C. § 2256(8), any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual

depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. "Child Erotica" means materials or items that are sexually arousing to certain individuals but that are not in and of themselves obscene or do not necessarily depict minors in sexually explicit conduct or poses. Such material may include non sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), sexually provocative drawings, or sketches, written descriptions/stories, or journals.

c. "Visual depictions" include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

d. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

e. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital genital, oral genital, or oral anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any persons. See 18 U.S.C. § 2256(2).

f. "Computer" is defined pursuant to 18 U.S.C. § 1030(e)(1), as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device

performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

g. "Computer hardware" consists of all equipment that can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. Hardware includes, but is not limited to, any data processing devices (such as central processing units, self contained laptop and notebook computers, hand held electronic organizers, personal digital assistants, and WebTV/DVR units), removable media, internal and external storage devices (magnetic storage devices such as hard disk drives, diskette drives, and tape drives; optical storage devices such as CD ROM drives, CD R/CD RW recorders, and DVD drives/recorders; and other memory storage devices), and related communication devices such as modems, cables, connectors, programmable telephone dialing or signaling devices, and electronic tone generating devices, and any devices, mechanisms, or parts that can be used to restrict access to computer hardware such as physical keys and locations.

h. A "system peripheral" is a piece of equipment that sends data to, or receives data from, a computer. Keyboards, mouses, cameras, webcams, video cameras, printers, scanners, plotters, video display monitors, and certain types of facsimile machines are examples of peripherals.

i. "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

j. Storage media includes any material capable of storing information in a manner that can be used by computer hardware to save and/or retrieve information. Examples of storage media include diskettes, CD ROMs, DVDs, DVRs, magnetic tapes, ZIP disks, JAZ disks, thumb drives, and EPROMS.

k. "Computer related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

l. "Computer passwords" and "data security devices" consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data to make it inaccessible or unusable, as well as reverse the progress to restore it.

m. The "Internet" is defined as a non commercial, worldwide network of computers. It is a self governing network devoted mostly to communication and research and has millions of users worldwide. The Internet is not an online service but a collection of tens of thousands of computer networks, online services, and single user components.

n. The Uniform Resource Locator (URL) is the address of a resource or file located on the Internet, also called a "domain name".

o. "Internet Service Providers" or "ISPs" are commercial organizations, which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e mail, remote storage, and co location of computers and other communications equipment. ISPs can offer various means by which to access the Internet including telephone based dial up, broadband based access via a digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth that the connection supports. Many ISPs assign each subscriber an account name such as a user name or screen name, an e mail address, and an e mail mailbox and the subscriber typically creates a password for the account. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and password.

p. "ISP Records" are records maintained by ISPs pertaining to their subscribers (regardless of whether those subscribers are individuals or entities). These records may include account application information, subscriber and billing information, account access information (often times in the form of log files), e mail communications, information concerning content uploaded and/or stored on or via the ISP's servers, and other information, which may be stored both in computer data format and in written or printed record format. ISPs reserve and/or maintain computer disk storage space on their computer system for their subscribers' use. This service by ISPs allows for both

temporary and long term storage of electronic communications and many other types of electronic data and files.

q. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet.

r. The terms "records", "documents", and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, DVRs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

s. "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such

as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices..

t. "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

u. "Hash value" refers to a mathematical algorithm generated against data to produce a numeric value that is representative of that data. A hash value may be run on media to find the precise data from which the value was generated. Hash values cannot be used to find other data.

v. "Steganography" refers to the art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, a child pornography image can be hidden inside another graphic image file, audio file, or other file format.

w. "Compressed file" refers to a file that has been reduced in size through a compression algorithm to save disk space. The act of compressing a file will make it unreadable to most programs until the file is uncompressed.

x. "Metadata" is data contained in a file that is not usually associated with the content of a file but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that

contains information identifying the camera that manufactured it and the date the image was taken.

y. A "JPEG" is a graphic image file. Other known graphic image files include "GIF", "TIFF", "RAW", and "BMP".

z. An "MPEG" is a video image file. MPEG files are generally larger than JPEG files and require the user to have a computer with sufficient processor speed, internal memory, and empty hard disk space. MPEG viewer software is also needed to play the files.

aa. "Malicious Software" ("malware") is software designed to infiltrate a computer without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch all phrase to include all types of malware, including true viruses. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, crimeware, and other malicious and unwanted software.

ab. "Media Access Control address" ("MAC address") is a unique identifier assigned to a network device for communication on a physical network. MAC addresses are most often assigned by the manufacturer of a network device.

CHARACTERISTICS COMMON TO PERSONSWHO DOWNLOAD AND POSSESS CHILD PORNOGRAPHY

12. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that the following

characteristics are oftentimes found in varying combinations in people who possess, receive, distribute, or transport child pornography:

a. These people view children as sexual objects.

b. These people collect sexually explicit and other erotic images of minors that they use for their own sexual gratification and fantasy.

c. These people rarely, if ever, dispose of sexually explicit images of minors because the images are treated as prized possessions. They store such images in different formats including photos, printouts, magazines, videotapes, and forms of digital media such as hard drives, diskettes, and CD ROMs. They store such images in different places including their home, their car, and other areas under their control. For example, laptops, electronic storage media, and child pornography are often secreted in compartments or trunks of vehicles so that those persons may hide, transport, or take the material to Internet or wi-fi locations so that they can access, trade, or add to their child pornography collections.

d. These people may use sexually explicit images of minors as a means of reliving fantasies or actual sexual encounters. They also use the images as keepsakes and as a means of gaining acceptance, status, trust, and psychological support by exchanging, trading, or selling the images to other people with similar interests.

e. These people go to great lengths to conceal and protect from discovery their collection of sexually explicit images of minors. They may use encryption software to protect their child pornographic files. They may have passwords to access programs or to control encryption that are written down and located in the vicinity of their computer, or located on their person. They may place child pornographic files in directories or

folders on their computer or other digital storage media not typically reserved for image or video files. They may change file names of sexually explicit images in an attempt to hide such images from a forensic review. They may change the extension on such image files in an effort to disguise them as a word processing file. They may also transfer such files downloaded from the Internet to removal storage media including but not limited to computer disks, thumb drives, digital cameras, smart cards, and cellular phones, and then attempt to erase the files from computer hard drives, in an effort to hide evidence of their download activity.

f. If child pornography collectors have had sexual contact with a minor, they frequently have visual depictions of the minor(s) with whom they have had sexual contact. If a picture of a minor is taken by such a person depicting the minor in the nude, there is a high probability the minor was used to produce sexually explicit images to be traded with people with similar interests. If pornographic depictions of a minor were produced as mentioned above, an analysis of the cameras, scanners, or webcams in the possession of the subject may yield clues as to what device was used in the commission of such crime. Such analysis would require the removal of the device to a laboratory setting.

g. If child pornography is found on the hard drive of a child pornography collector's computer, and his computer was connected to the Internet, there is a strong likelihood that the person received the images of child pornography from the Internet, either from Internet websites or groups devoted to child pornography, or from other individuals who sent the images via e-mail or file sharing program.

h. Child pornography collectors who acquire sexually explicit images of minors from the Internet, will frequently bookmark the locations (i.e. websites, news groups, and other locations) on the Internet from which they accessed child pornographic images. By bookmarking such locations, these collectors can readily gain access to such sites.

i. Child pornography collectors also tend to collect child erotica because it is more readily available, partially satisfies their sexual fantasies, and is often intermixed with child pornography on the Internet.

TOOLS OF THE INTERNET

13. Based upon my knowledge, training and experience in child exploitation and child pornography investigations and the experience and training of other law enforcement officers with whom I have had discussions, I know that the development of computers has also revolutionized the way in which child pornography collectors interact with, and sexually exploit, children. Computers serve four basic functions in connection with child pornography: production, communication, distribution, and storage. More specifically, the development of computers has changed the methods used by child pornography collectors in these ways:

a. Producers of child pornography can now produce both still and moving images directly from a common video or digital camera. The camera is attached, using a device such as a cable, or digital images are often uploaded from the camera's memory card, directly to the computer. Images can then be stored, manipulated, transferred, or printed directly from the computer. Images can be edited in ways similar to how a photograph may be altered. Images can be lightened, darkened, cropped, or otherwise

manipulated. The producers of child pornography can also use a device known as a scanner to transfer photographs into a computer readable format. As a result of this technology, it is relatively inexpensive and technically easy to produce, store, and distribute child pornography. In addition, there is an added benefit to the pornographer in that this method of production does not leave as large a trail for law enforcement to follow.

b. The Internet allows any computer to connect to another computer. By connecting to a host computer, electronic contact can be made to literally millions of computers around the world. A host computer is one that is attached to a network and serves many users. Host computers are sometimes operated by commercial ISPs, such as America Online, Inc., AT&T, and Comcast, to name a few, that allow subscribers to dial a local number and connect to a network that is, in turn, connected to the host systems. Host computers, including ISPs, allow e-mail service between subscribers and sometimes between their own subscribers and sometimes between their own subscribers and those of other networks. In addition, these service providers act as a gateway for their subscribers to the Internet. Individuals who use the Internet can communicate electronically by using e-mail. E-mail messages can contain text, data, or graphic images. This type of communication is private in that it is directed from one Internet user to another. Internet users can also communicate and trade images of child pornography using Instant Messaging. Instant Messaging is "real time" communication in that the persons communicating are engaging in online dialog. This means of communication, like e-mail, is private in that it is one Internet user communicating specifically, and exclusively, with another.

c. The Internet allows users, while still maintaining perceived anonymity, to easily locate (i) other individuals with similar interests in child pornography; and (ii) web sites and social networking sites that offer images of child pornography. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other and to distribute child pornography. These communication links allow contacts around the world to be made as easily as calling next door. Additionally, these communications can be quick and relatively secure. The ease of trading and downloading child pornography via the Internet allows such collectors to increase the number of images in their collections quite rapidly. All of these advantages, which promote anonymity for both the distributor and recipient, are well known and are the foundation of transactions between child pornography collectors over the Internet. Sometimes the only way to identify both parties and verify the transportation of child pornography over the Internet is to examine the recipient's computer, including the Internet history and cache to look for "footprints" of the web sites and images accessed by the recipient.

d. A computer's capability to store images in digital form makes it an ideal repository for child pornography. A single USB flash drive can store thousands of images and millions of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Hard drives with the capacity of 500 gigabytes are not uncommon. These drives can store hundreds of thousands of images at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a

computer with a video capture board, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail. Digital evidence of the results of web browsing can often be found on the hard drive of a computer during a forensic examination. In addition, the dialog and image downloads created when corresponding via e-mail and instant message are generally stored in the hard drive of a computer until overwritten by other correspondence, and are usually retrievable during a forensic examination of the computer.

OVERVIEW OF PEER TO PEER FILE SHARING

14. The present investigation was initiated as a result of the law enforcement community's ongoing concern related to the escalating prevalence of the distribution of child pornography via Peer to Peer (P2P) file sharing software. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that, presently, millions of people throughout the world use P2P file sharing networks to share many types of files with others. P2P application software allows network computer users, connected to the Internet, to share many types of files; these files typically include music, graphics, images, movies, and text. In this way, users are able to collect large numbers of files, including child pornography.

15. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that the most prevalent P2P file sharing network presently in use today is known as the "Gnutella" network.

Gnutella is a system that allows individuals to use their computers to exchange files directly over the Internet without having to go through or access a specific web site in an arrangement that can best be described as computer to computer (or person to person, hence the name "Peer to Peer"). Unlike a web site, Gnutella enables persons to obtain files directly from one another as long as they are connected to the Internet. Furthermore, Gnutella enables an individual to view the files of other Gnutella users made available to share. Upon installation and enabling of Gnutella on one's computer, that computer then becomes both a client and a server in the network and is able to share desired files, which have been placed in what is referred to as a "share folder" on a user's hard drive, with other Gnutella users. The Gnutella network is presently utilized by numerous P2P file sharing programs, including, but not limited to "eMule" and "Limewire". These aforementioned programs connected to the Gnutella network have software that, if installed on a computer, facilitates the trading of images and other files.

16. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that because of its relative ease of use and perceived anonymity, P2P networks provide readily available access to child pornography. As a result, law enforcement officers/agents have initiated undercover investigations via the Internet to identify persons using P2P software to traffic in child pornography.. Law enforcement officers/agents assigned to these types of investigations know, from their experience using P2P software, that users can find images and movies of child pornography by using search terms or browsing another user's shared folders.

17. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that one new type of P2P software allows users to set up their own private P2P network of contacts. File sharing through this software is limited only to other users who have been added to a particular user's private list of "friends". A new user is added to a user's list of friends through a "friend request" or "invite". Once accepted as a "friend" the new friends "screen" or "user name" is added to the list of other such friends of the computer user. Acceptance of a friend request will allow that new user to download file(s) from the user who sent the friend request. The new user can then browse the list of files the other user has made available to share/download, select the file(s) from this list, and download the selected file(s). The download of a file is achieved through a direct connection between the computer requesting the file and the computer containing the file. The software allows users to browse a friend's files, by navigating a file structure similar to that of a desktop computer. Additionally, thumbnails of images can be viewed by a user prior to actually downloading the file. This allows a user to browse images and select those that s/he wants to download. The software also contains a "Transfers" screen that provides information on all files being uploaded or downloaded. This not only allows a user to see the files s/he is downloading from other users, but also who is uploading files from him/her.

18. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that once a person becomes a "friend" of the user of the target computer, and acquires access to that target

computer's shared folders, that friend's user or screen name is contained, usually in a "friends" listing, on the target computer.

19. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that Internet computers identify each other by an Internet Protocol or IP address. I know that these IP addresses can assist law enforcement in finding a particular computer on the Internet. These IP addresses can lead the law enforcement officer to a particular ISP, and that company can identify the account that used the IP address to access the Internet.

20. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that third party software is available to identify the IP address of the P2P computer sending the file. Such software monitors and logs Internet and local network traffic.

SEARCH AND SEIZURE OF COMPUTERS AND RELATED STORAGE MATERIALS IN GENERAL

21. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that information stored in an electronic format may be found not only on the hard disk drive of a computer, but also on other computer hardware, peripherals, and storage media. In addition, to conduct a thorough search of computers, agents are often required to seize most or all of the computer hardware, peripherals, and other storage media, to be searched later by a qualified expert in a laboratory or other controlled environment. This is true for the following reasons:

a. Nature of the Evidence: As described, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a

computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. Volume of Evidence: Computers and storage devices (like hard disks, diskettes, tapes, CD ROMs, DVDs, and zip drives) can store the equivalent of thousands of pages of information. Also when the user wants to conceal criminal evidence, he or she may store it in many places, in random order, and with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take several weeks to conduct, and it would be impractical to attempt this kind of data search on site.

c. Technical Requirements: Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment needed to conduct a thorough search. In addition, it may be necessary to consult with personnel who have specific expertise in the type of computer, software application, or operating system that is being searched.

d. Retrieval of Electronically Stored Data: In order to retrieve electronically stored evidence from a computer, agents may be required to seize most or all of a computer system's equipment, including hardware, peripherals, software, documentation, security devices, and passwords. This is true because of the following:

1) Certain operating systems and hardware can be configured to operate only with a precise set of hardware, software, and peripherals.

2) Peripheral devices that allow users to enter or retrieve data from the storage devices may vary in their compatibility with other hardware and software.

3) The searching authorities may have to install software used by the suspect on a government computer in order to retrieve the information the suspect may have stored using that software. The searching authorities may also need to refer to hardware and software documentation maintained by the suspect to complete an analysis in a timely manner. The suspect's computer documentation may also contain hand written notes specific to the seized computer system.

e. The Nature of Data Storage: Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache". The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently

viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits. The search for these files and file fragments can take considerable time, depending on the computer user's practices. It often takes weeks or months to complete such a search, particularly if many hard drives and other storage media are seized from the location to be searched. A thorough search for such relevant evidence would be impractical during an on site preview.

22. As further described in Attachment B, this warrant seeks permission to locate in the SUBJECT PREMISES not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how computers were used, the purpose of their use, and who used them.

23. Further, as described above and in Attachment B, this application seeks permission to search and seize records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is electronic, in that they are stored on a computer's hard drive, or other electronic media. Some of these electronic records might take the form of files, documents, and other data that is user generated. Some of these electronic records, as explained below, might take a form that becomes meaningful only upon forensic analysis of the computer(s) or other electronic storage media seized.

24. Although some of the records called for by this warrant might be found in the form of user generated documents (such as word processor, picture, and movie files), computer hard drives can contain other forms of electronic evidence as well. In

particular, records of how a computer has been used, the purposes for which it was used, and who has used it are called for by this warrant. As described above, data on the hard drive not currently associated with any file can provide evidence of a file that was once on the hard drive but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the hard drive that show what tasks and processes on the computer were recently used. Web browsers, e mail programs, and chat programs store configuration information on the hard drive that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals (e.g., cameras and printers for creating or reproducing images), the attachment of USB flash storage devices, and the times and dates the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can sometimes be evidence of a crime, or can point toward the existence of evidence in other locations. Evidence of this type often is not simply "data" that can be merely reviewed by a review team and passed along to investigators; rather, evidence of this type is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand the evidence described in Attachment B is included within the scope of the warrant.

25. In finding evidence of how a computer has been used, the purposes for which it was used, and who has used it, sometimes it is necessary to establish that a particular thing is not present on a drive. For example, I know from training and experience that it

is possible that malicious software can be installed on a computer, often without the computer user's knowledge. This software can allow a computer to be used by others. To investigate the crimes described in this warrant, it might be necessary to investigate whether any such malicious software is present on the computer, and, if so, whether the presence of that malicious software might explain the presence of other things found on the computer's hard drive.

26. Law enforcement personnel trained in searching and seizing computer data will seize the computers, computer hardware, storage media, associated system peripherals, and digital devices that are believed to contain or constitute fruits, evidence and instrumentalities as described in Attachment B to the warrant, and transport the same to an appropriate law enforcement laboratory for off site review, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search these items on site for the evidence, fruits and instrumentalities. The computer equipment and storage devices will be reviewed by a review team in accordance with and as defined by the review protocols described below in order to extract and seize any data that falls within the list of items to be seized as set forth in Attachment B.

27. In order to fully retrieve data from a computer system, the analyst needs all electronic storage devices as well as the computer's central processing unit (CPU). The analyst may also need the computer's storage devices, the monitor, keyboard, modem, and other related hardware. As in this case where the evidence consists partly of graphic files, the monitor and printer are essential to show the nature and quality of the graphic images that the system could produce. In addition, the analyst needs all the system software (operating systems or interfaces and hard drive drivers) and any application

software that may have been used to create the data (whether stored on hard drives or on external media).

SPECIFIC METHODS FOR SEARCH OF DIGITAL EVIDENCE

28. I am seeking authority to search for, among other things, items containing digital data, more particularly described in Attachment B. As many devices commonly found in a residence may contain digital data, I will make every reasonable effort to minimize seizures to only those devices for which there is reason to believe might be found: 1) evidence or fruits of the aforementioned crimes; 2) contraband implicated by this affidavit; and 3) property/instrumentalities designed for use, intended for use, or used in the commission of the aforementioned crimes. If personnel trained in the forensic preview of digital evidence are available, and if doing so will not extend the duration of the search to an unreasonable time and is consistent with the review protocol detailed below, I intend for there to be an on scene preview of the digital evidence in order to minimize the amount of material that needs to be removed from the premises. I know that certain tools are available to trained personnel that make such previews possible under certain circumstances. Such a preview generally consists of reviewing images and videos contained on digital media, and searching for filenames that appear to contain references to child pornography. These previews are done in a manner that preserves the integrity of the data on the device. A forensic preview is not a substitute for a forensic examination, but in certain instances (such as when it is possible through interviews to determine which items belong to uninvolved third parties), an on site forensic preview can be a useful tool in minimizing the number of digital devices that need to be removed from the premises for a full forensic examination. If an item that may reasonably contain

evidence of child pornography cannot be eliminated from suspicion, I intend to remove it to a laboratory setting for a more detailed forensic examination, in accordance with the parameters described below.

29. As previously mentioned, the search of a computer hard drive or other computer storage medium is a time consuming manual process often requiring months of work. I know that the seizure of a computer hard drive, by necessity, provides the seizing agency with potential access to data outside the scope of this warrant. A search protocol will be used to uncover solely evidence, instrumentalities and contraband set forth in Attachment B for which there is probable cause. As part of the search protocol, I intend to direct the review team to search any computer and computer storage medium only for those items contained in Attachment B. As it concerns this particular case, I intend to direct the review team to search digital media with some or all of the following methods, not listed in any particular order; however, the listing of these methods is not a representation that these specific techniques will be employed in this case:

a. Keyword Searches: I know that computer forensic utilities provide the capability for a user to search for specific key words that may exist on a piece of digital media. I intend to use specific keywords known to be related to either the subject's illicit internet activities or child pornography. As it concerns child pornography, examples of such keywords include, but are not limited to, "preteen", "hussyfan", and "r@ygold". Those keyword searches will indicate files and other areas of the hard drive that need to be further reviewed to determine if those areas contain relevant data. A list of keywords utilized will be maintained with the records of the forensic examination.

b. Data Carving: I know that, as previously mentioned, data residue may be left in the "free", "unallocated", or "slack" space of a computer hard drive, that is, the space not currently used by active files. I further know that, as previously mentioned, many operating systems utilize temporary storage often referred to as "swap space" on the hard drive to store contents from main system memory. Such unallocated and swap space may contain the residue of files that can be carved out, often in an automated or semi automated fashion. I intend to use forensic tools to carve out files, in particular, image files such as JPEG and GIF files. The mere act of carving out such files does not expose me to the contents of such recovered files, but makes those files available for further relevancy checks, such as keyword searches (explained above) and hash value comparisons (explained below).

c. Hash Value Comparisons: I know that computer forensic utilities provide the capability to utilize a function known as a hash algorithm. A hash algorithm uses a mathematical formula to analyze the data composing a file, and to generate a unique "fingerprint" for that file. The act of hashing a piece of data does not reveal to an investigator any information about the contents of that data. However, I know that computer forensic applications often contain databases of known hash values for files. Some of those files are "ignorable", which enables other forensic processes to ignore files (such as the Windows operating system) that are not evidentiary in nature. Some of the files are "alert" files, such as the Child Victim Identification Program (CVIP) hash set that contains hash values for a small subset of the identified picture and video files for known victims of child pornography. CVIP alert files notify an examiner that a file appears to contain known depictions of child pornography. I seek permission to utilize

automated hash value comparisons to both exclude irrelevant files, and to locate known child pornography files. Hash value comparisons are useful, but not definitive, as even a single bit change to a file will alter the hash value for the file. The forensic review team does not intend to rely solely on hash value comparisons, but intends to utilize them in order to assist with identifying relevant evidence. The use of this search method is intended to narrow the search. A search of known hash values, however, will not be used exclusively, because I know that when previously identified images of child pornography are found on a target's computer, typically there are many more images of child pornography depicting unknown child victims. Using a hash value search method exclusively would not uncover these images of unknown child victims as well as other evidence authorized by this warrant and described in Attachment B.

d. Opening Container Files, Encrypted Volumes, Embedded Files: I know that relevant data may be compressed, encrypted, or otherwise embedded in other files or volumes. It is often not possible through any automated process to examine the contents of such containers without opening them, just as it is not possible to examine the contents of a locked safe without first opening the safe. In the event that compressed, encrypted, or otherwise embedded files or volumes may exist on the seized items, I intend to use sophisticated forensic tools to attempt to open any such container files that may reasonably contain evidence of child pornography.

e. File Header / Extension Checks: I know that individuals involved in illegal activities on a computer often change the extension of a file (such as .jpg) to some other incompatible extension (such as .txt) in order to disguise files from casual observers. The extension of a file, however, is not necessarily linked to the "header" of a

file, which is a unique marking imbedded automatically in many types of files. By comparing the extension of a file with the "header information" of a file, it is possible to detect attempts to disguise evidence of illegal activities. Such a comparison can be made in an automated process by computer forensic tools. I intend to run an automated header comparison to detect such efforts, and intend to review any such files that reasonably may contain evidence of child pornography.

f. Thumbnail / Image Views: Although hash value comparisons can positively identify known child pornography depictions, a negative hash value comparison does not exclude an image from suspicion. There is no known alternative for visually inspecting each image file. I therefore intend to examine at least a thumbnail image of each image file on the digital media whether "live", "data carved", or identified by header.

g. Registry / Log File Checks: I know that it is necessary in any criminal case to establish not only that a crime has occurred, but also to establish what person committed that crime. Operating systems and computer programs often maintain various administrative files such as logs that contain information about user activities at certain times. In the Windows operating system, for example, some of these files are collectively referred to as "the registry". Such files contain specific information about users, often including e-mail addresses used, passwords stored, and programs executed by a particular user. These files may also contain evidence regarding storage devices that have been connected to a computer at some time. Multiple backup copies of such files may exist on a single computer. I intend to examine these files to attempt to establish the identity of any user involved in the receipt, possession, distribution, and transportation of

child pornography, and to establish methods (such as software used) and dates of this activity.

h. Metadata / Alternative Data Streams: I know that many file types, operating systems, and file systems have mechanisms for storing information that is not immediately visible to the end user without some effort. Metadata, for example, is data contained in a file that is not usually associated with the content of a file, but is often associated with the properties of the application or device that created that file. For example, a digital camera photograph often has hidden data that contains information identifying the camera that manufactured it, and the date the image was taken. Some file systems for computers also permit the storage of alternate data streams, whereby a file such as a text file may hide an image file that would not be immediately visible to an end user without some action taken. I know that both metadata and alternative data streams may contain information that may be relevant to child pornography offenses. Metadata and alternative data streams are often identified and processed automatically by computer forensic utilities. I intend to review any such data that is flagged by any process above as being relevant to the receipt, possession, distribution, and transportation of child pornography.

30. With rare exception, the above listed search techniques will not be performed on original digital evidence. Instead, I know that the first priority of a digital evidence forensic examination is the preservation of all data seized. As such, original digital media will be, wherever possible, copied, or "imaged", prior to the start of any search for evidence. The copy will be authenticated digitally as described in the paragraph below.

31. I know that a digital forensic image is the best possible copy that can be obtained for a piece of digital media. Forensic imaging tools make an exact copy of every accessible piece of data on the original digital media. In general, the data contained on the original media is run through a hashing algorithm as described above, and a hash value for the entire device is generated. Upon completion of the imaging process, the same hash algorithm is run on the imaged copy to insure the copy is an exact duplicate of the original. Upon the completion of the search processes described above, which are performed on the image of the hard drive, the hash algorithm is again run on the image copy to insure no alterations of the data occurred during the examination process.

32. In the event that a piece of original digital media is found not to be (a) an instrumentality of the offense, (b) a fruit of the criminal activity, (c) contraband, or (d) evidence of the offenses specified herein, it will be returned as quickly as possible, not to exceed 120 days.

33. A 120-day review window is requested due to the delay that may be caused by the review protocols explained below.

34. I also hereby request judicial authorization to retain copies of all seized storage media after the review is complete. That judicial authorization is justified in this case in part because:

a. Should the execution of the warrant uncover data that may later need to be introduced into evidence during a trial or other proceeding, the authenticity and the integrity of the evidence and the government's forensic methodology may be contested issues. Retaining copies of seized storage media can be required to prove these facts and

the investigator may retain a copy of seized or electronically stored information pursuant to Fed. R. Crim. P. 41(f)(1)(B):

b. Returning the original storage medium to its owner will not allow for the preservation of that evidence. Even routine use may forever change the data it contains, alter system access times, or eliminate data stored on it.

c. Because the investigation is not yet complete, it is not possible to predict all possible defendants against whom evidence found on the storage medium might be used. That evidence might be used against persons who have no possessory interest in the storage media, or against persons yet unknown. Those defendants might be entitled to a copy of the complete storage media in discovery. Retention of a complete image assures that it will be available to all parties, including those known now and those later identified. Specifically in this case, based on the nature of P2P file sharing, forensic analysis may identify the user names and screen names of those distributing child pornography to the user of the target computer(s).

d. The act of destroying or returning a storage medium could create an opportunity for a defendant to claim, falsely, that the destroyed or returned storage medium contained evidence favorable to him. Maintaining a copy of the storage medium would permit the government, through an additional warrant if necessary, to investigate such a claim.

e. Similarly, should a defendant suggest an explanation for the presence of evidence on a storage medium or some defense, it may be necessary to investigate such an explanation or defense by, among other things, re-examining the storage medium with that explanation/defense in mind. This may require an additional examination of the

storage medium for evidence that is described in Attachment B but was not properly identified and segregated previously.

f. I have not attempted to acquire the sought after material through any other investigative or judicial process.

REVIEW PROTOCOL

Government personnel will utilize the following computer review protocol:

A. Contextual evidence that establishes how computers were used, the purpose of their use, and who used them is a conclusion, based on a review of all available facts and the application of knowledge about how a computer behaves. Therefore, such evidence necessary to understand the evidence described in Attachment B is included within the scope of this warrant and will be seized.

B. Although it is not possible to accurately predict the exact composition of the review team, given the very limited computer forensic examination resources available at present, it is possible that the team may include one or more agents, computer specialists, analysts, and/or attorneys including members of the investigative team. The team will not necessarily consist only of persons with those job descriptions, and by referencing those job descriptions, I do not intend to represent anything about the manner in which the team will conduct its review. It is also possible that the review "team" will consist of a single person.

PROBABLE CAUSE TO SEARCH THE SUBJECT PREMISES

35. During this investigation, I identified computers and persons located within the Eastern District of California that are distributing images and/or movie files of child

pornography via the Internet through the use of P2P file sharing software. Among them was a computer user with the screen name "boyforboys1".

36. On 12/27/2010, while working in an undercover capacity, I signed on to a P2P file sharing program via an Internet connected computer located at the FBI Sacramento office using an undercover screen name.

37. I observed that the user "boyforboys1" was logged into the network. While recording the session by means of screen capture software, I browsed through the sub-folders of "boyforboys1" and observed numerous files had titles and thumbnails indicative of child pornography (CP). I was able to download approximately 5 image files directly from "boyforboys1"; with at least 3 of the 5 images depicting child pornography. Using the software program CommView, I was able to identify that the files were being downloaded from "boyforboys1" at the Internet Protocol (IP) address 67.172.180.130, registered to Comcast Communications.

38. Additionally, on 1/3/2011, while working in an undercover capacity, I signed on to the same P2P file sharing program via an Internet connected computer located at the FBI Sacramento office using an undercover screen name.

39. I observed that the user "boyforboys1" was again logged into the network. While recording the session by means of screen capture software, I browsed through the sub-folders of "boyforboys1" and observed numerous files had titles and thumbnails indicative of child pornography (CP). I was able to download approximately 8 image files and 6 videos directly from "boyforboys1"; with at least 5 of the images and 2 of the videos depicting child pornography. Using the software program CommView, I was able

to identify that the files were being downloaded from "boyforboys1" at the Internet Protocol (IP) address 67.172.180.130, registered to Comcast Communications.

40. Two administrative subpoenas were served on Comcast Communications for the IP addresses and times listed above. Comcast Communications responded to both administrative subpoenas with negative results, stating that they were unable to find information relating to the subpoenas and that their logs were either incomplete or contained errors. I spoke with a Comcast technical representative regarding the negative results, who advised that negative results typically indicate an individual is using an unauthorized and/or unregistered cable modem.

41. The following are a sample of the filenames and descriptions of the files depicting child pornography that I downloaded from "boyforboys1" on December 27, 2010 and January 3, 2011:

"aaaa boylove gay pedo preteen boy sex child porn 045.jpg"

This image file depicts a nude prepubescent male minor orally copulating another nude prepubescent male minor's penis. In the lower left hand corner of the image there is another picture of a prepubescent male's penis, and the words "ALL-MALE CHILD PORN- KIDSEX ROCKS!".

"1 Noah asleep sucked by dad.wmv"

This video file is approximately 2 minutes and 1 second in duration and depicts an adult male orally copulating a prepubescent male minor's penis, and then stroking the boy's penis while the boy appears to be sleeping.

"__hr_cab3.jpg"

This image file depicts a nude prepubescent male minor holding his hands at the base of his erect penis.

42. The user "boyforboys1" was also observed logging into the same P2P file sharing network using the IP address 64.160.118.55 on several different dates including 3/13/2011 and 3/28/2011.

43. On 3/28/2011, while working in an undercover capacity, I signed on to the same P2P file sharing program via an Internet connected computer located at the FBI Sacramento office using an undercover screen name.

44. I observed that the user "boyforboys1" was logged into the network. While recording the session by means of screen capture software, I browsed through the sub-folders of "boyforboys1" and observed numerous files had titles and thumbnails indicative of child pornography (CP). I was able to download approximately 64 image files and 5 videos directly from "boyforboys1"; with at least 36 of the images and 4 of the videos depicting child pornography. Using the software program CommView, I was able to identify that the files were being downloaded from "boyforboys1" at the Internet Protocol (IP) address 64.160.118.55, registered to AT&T Internet Services.

45. The following are a sample of the filenames and descriptions of the files depicting child pornography I downloaded from "boyforboys1" on March 28, 2011 from IP address 64.160.118.55:

"boys with boners.avi"

This video file is approximately 3 minutes and 41 seconds in duration and depicts two prepubescent male minors masturbating and playing with their erect penises.

"cp_220.bmp"

This image file depicts a nude prepubescent male minor orally copulating another male minor.

"PIC_0016.JPG"

This image file depicts two nude prepubescent male minors in a shower while one boy is bending over and holding the other boy's erect penis.

46. An administrative subpoena was served on AT&T Internet Services for the IP address 64.160.118.55 for 3/13/2011. The AT&T Internet Services response indicated the subscriber associated with IP address 64.160.118.55 resides at [redacted] Apartment 242, Davis, California, 95616. The subpoena results listed the subscriber account as currently active (as of 3/29/11) and further stated that the IP address 64.160.118.55 was first issued to that subscriber on 02/08/2011.

47. On 3/29/2011, I spoke with the apartment manager of Greystone Apartments, [redacted] Davis, California, 95616 regarding this investigation. The manager confirmed that the subscriber named by AT&T resides in Apartment 242 along with two other people.

48. A public records database check identified the AT&T subscriber's name as being associated with [redacted] Apartment 242, Davis, California, 95616.

49. On 4/1/11, a federal search warrant signed by Magistrate Judge Gregory Hollows was executed at [redacted] Apartment 242, Davis, California, 95616.

50. Two people, (Cooperating Witness #1, "CW1", and Cooperating Witness #2, "CW2"), were at home at the time the warrant was executed. I interviewed CW#1 who advised that she lived at [redacted] Apartment 242, Davis, California, 95616, with two other roommates, including CW2. CW1 stated that her she is the subscriber named

by AT&T, and that her home wireless network was named "2WIRE703" which was confirmed by agents on-scene. Additionally, the wireless network was password protected using a 10-digit numeric password using the Wired Equivalent Privacy (WEP) protocol.

51. Special Agent Michael Cahoon, who was present during the execution of the search warrant, was able to analyze the AT&T internet wireless router which provided wireless internet to the residents of Apartment 242. Agent Cahoon was able to identify all internet devices that had recently connected to the internet connection in Apartment 242 via internal IP addresses and Media Access Control (MAC) addresses. Agent Cahoon also determined that the external IP address currently assigned to Apartment 242 by AT&T was 69.105.80.128.

52. All of the devices belonging to the residents of Apartment 242 and their friends were accounted for in the router log and forensically reviewed on-scene, none of which possessed any evidence of child pornography, nor any evidence of the P2P file sharing program used by "boyforboys1".

53. It was determined that there was still one more device that had recently accessed the password-protected wireless network in Apartment 242 that was not located during the search. The device was listed in the router as "CK" with a MAC address of: 00:25:d3:d4:c4:73. "CK" was not connected to the wireless internet belonging to Apartment 242 at the exact time of the search, however it was listed as a device that had recently been connected. None of the residents in Apartment 242 recognized the device name "CK".

54. Additionally, in another area of the AT&T wireless router logs, another device named "bootycop" had recently accessed the wireless Internet connection in Apartment 242, but was unaccounted for and not known by any of the residents.

55. During the execution of the search warrant, Special Agent Derren Holtz and Special Agent Laura Giouzelis used an open-source wireless tracking utility to determine if the Internet device "CK" was in the vicinity of Apartment 242. The tool was a wireless antenna in a passive mode which allows it to detect if a specific MAC address is currently within range by filtering out all other MAC address information Using signal strength readings from inside Apartment 242, from Apartment 240 (a vacant apartment which the apartment manager allowed us to access), and the outdoor common areas of the apartment complex, Agents Holtz and Giouzelis concluded that the device "CK" with MAC address 00:25:d3:d4:c4:73 was most likely located in the second floor of [redacted] **Apartment 243, Davis, California, 95616.** The residence [redacted] **Apartment 243, Davis, California, 95616,** is a corner apartment situated between Apartments 242 and 240.

56. On 4/8/11, while working in an undercover capacity, I signed onto the same P2P file sharing program via an Internet-connected computer located at the FBI Sacramento office using an undercover screen name. I observed that user "boyforboys1" was logged into the network. While recording the session by means of screen capture software, I browsed the subfolders of "boyforboys1" and observed that the user was sharing two videos depicting child pornography. Using the software program CommView, I was able to identify that the files were being downloaded from "boyforboys1" at the Internet Protocol (IP) address 69.105.80.128, registered to AT&T Internet Services. This is the

same IP address observed a week prior at Apartment 242. The following are the two videos of suspected child pornography downloaded:

"!!!!kids piss play.flv"

This video is approximately 17 seconds in duration and depicts two nude prepubescent male minors urinating on each other.

"_Nick_gets_sucked_by_yng_boy"

This video is approximately 18 seconds in duration and depicts a nude prepubescent male minor orally copulating a nude male minor.

57. On 4/8/2011, a few hours after my undercover session, I spoke with CW1 and she consented to allowing me and my colleagues to return to her residence.

58. We returned to Apartment 242 at approximately 12:30pm on 4/8/2011 and, with the consent of CW1, re-examined the AT&T wireless router. There were two wireless devices currently active and logged into the AT&T wireless router: "CK" with MAC address 00:25:d3:d4:c4:73 and "bootycop" with MAC address 00:1f:1f:49:d3:11. No other devices, other than the FBI computer used to log into the router, were currently accessing the wireless router and using the Internet.

59. I determined there were only two computers accessing the network, and none of those computers were physically located in Apartment 242. Using an undercover laptop with separate internet access, I verified that "boyforboys1" was still logged into the P2P file sharing program, which it was. I also re-verified that the IP address 69.105.80.128 being used by "boyforboys1" was still the IP address assigned to Apartment 242, which it was. After some time in the residence, the device named "CK" disconnected from the

network, leaving the only connected computer as "bootycop" while "boyforboys1" was still logged into the P2P file sharing program.

60. Using the same open source wireless networking tool and passive mode directional antenna used on 4/1/2011 during the execution of the search warrant, I was able to determine that the internet device named "bootycop" with MAC address 00:1f:1f:49:d3:11 was most likely located in the second floor of [redacted] **Apartment 243, Davis, California, 95616.** I determined this to be the case by taking numerous signal strength readings at various locations within Apartment 242 and Apartment 240 (a vacant apartment which we entered with the consent of the apartment manager), with [redacted], **Apartment 243, Davis, California, 95616** being the only apartment between the two other apartments. The signal strengths were similar to the readings of internet device "CK" taken on 4/1/2011, and I believe that "CK" and "bootycop" are associated with each other and located in the same apartment, inasmuch as they both were able to connect to a password-protected wireless router in an unauthorized manner.

61. Based upon my training and experience and the training and experience of other agents with whom I work and with whom I have spoken, I know that it is possible to gain unauthorized access to a password protected wireless network using the WEP protocol, however it requires advanced computer knowledge and tools. An individual with the knowledge necessary to crack a password-protected network would likely also have a strong understanding of IP addresses and how law enforcement might use them to identify a subject. It is reasonable to suspect that an individual in the SUBJECT

PREMISES may have intentionally stolen internet access from Apartment 242 in an effort to conceal his/her identity while distributing child pornography online.

CONCLUSION

62. Based on the aforementioned factual information, I respectfully submit that probable cause exists to believe that an individual who resides at the SUBJECT PREMISES, described in Attachment A, is involved in child pornography offenses. I respectfully submit that probable cause exists to believe that an individual residing in the SUBJECT PREMISES violated 18 U.S.C. §§ 2252 and 2252A and that evidence, fruits, and instrumentalities of those, as more particularly described in Attachment B, will be found at the SUBJECT PREMISES.

I swear, under penalty of perjury, that the foregoing Information is true and correct, to the best of my knowledge, information and belief.

NICHOLAS G. PHILIPPIDIS
Special Agent
Federal Bureau of Investigation

Read and approved as to form.

MATTHEW MORRIS
Assistant United States Attorney

Subscribed and sworn to before me
this 11th day of April, 2011

GREGORY G. HOLLOWS

Gregory G. Hollows
United States Magistrate Judge
Eastern District of California
Sacramento, California

ATTACHMENT A
LOCATION TO BE SEARCHED

A 3 bedroom, 2 story apartment located at [redacted] **Apartment 243, Davis, California, 95616**. The subject residence is located within the Greystone Apartment Complex on the second floor. The front door is beige in color with dark orange trim. The numbers "243" are located to the left side of the front door. This address is located in Yolo County in the State and Eastern District of California. Besides the residence, the property to be searched will include any garages, outbuildings, and vehicles that fall under the domain and control of the person(s) associated with said residence.

Moreover, the property to search includes any computer, computer system and related peripherals, digital device, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drive and other computer related operation equipment, digital cameras, scanners, computer photographs, graphic interchange formats and/or photographs, undeveloped photographic film, slides, cellular telephones/hybrids, and other visual depictions of such Graphic Interchange formats (including, but not limited to, JPG, GIF, TIF, AVI, and MPEG), and any electronic data storage devices including, but not limited to, hardware, software, diskettes, CD ROMs, DVDs, DVRs, flash memory devices, and other storage mediums, any input/output peripheral devices, including but not limited to passwords, data security devices and related documentation, and any hardware/software manuals related thereto found within the location to be searched. **END OF ATTACHMENT A**

ATTACHMENT B

ITEMS TO BE SEIZED

The following items, images, documents, communications, records, materials, and information are to be seized wherever they may be stored or found on location to be searched, see Attachment A, and in any form that they may be stored or found:

1. Any child pornography or visual depictions of minors engaged in sexually explicit conduct in any form;

2. Any child erotica;

3. Any information pertaining to any individual's interest in child pornography, visual depictions of minors engaged in sexually explicit conduct, or erotica;

4. Any items, images, documents, communications, records, and information related to the distribution, receipt or possession of child pornography or visual depictions of minors engaged in sexually explicit conduct;

5. Books and magazines containing child pornography or visual depictions of minors engaged in sexually explicit conduct;

6. Originals, copies, and negatives of child pornography or visual depictions of minors engaged in sexually explicit conduct;

7. Motion pictures, films, videos, and other recordings of child pornography or visual depictions of minors engaged in sexually explicit conduct;

8. All screen names, user names, and true names of others who may have operated as the source of child pornography or visual depictions of minors engaged in sexually explicit conduct, in any format, downloaded and possessed by the target computer(s).

9. Any items, images, documents, communications, records, and information pertaining to the possession, receipt, transmission, sale, purchase, trade, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct that affected or were transmitted or received via computer, some other facility or means of interstate or foreign commerce, common carrier, or the U.S. mail, including:

a. envelopes, letters, and other correspondence including, electronic mail, chat logs, and electronic or other instant messages, establishing possession, access to, affect on, or transmission through interstate or foreign commerce, including by United States mail or via computer, of child pornography or visual depictions of minors engaged in sexually explicit conduct;

b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind affecting interstate or foreign commerce or involving the transmission via interstate or foreign commerce, including by U.S. mail or by computer, of any child pornography or visual depiction of minors engaged in sexually explicit conduct;

c. credit card information, including bills and payment information, regarding: Internet service; purchase of computer hardware, software, or storage media; purchase of or payment for memberships to web sites; and possession, receipt, sale, purchase, trade, transportation, or distribution of child pornography or visual depictions of minors engaged in sexually explicit conduct;

d. records evidencing occupancy or ownership of the premises described above, including utility/telephone bills or addressed correspondence; and

e records or other items that indicate ownership or use of computer equipment found in the above residence, including sales receipts, bills for Internet access, and handwritten notes.

9. For any computer hard drive, cellular telephone/hybrid, or other electronic media (hereinafter, "COMPUTER") found to contain information otherwise called for by this warrant:

a. evidence of who used, owned, or controlled the COMPUTER at the time the items described in this warrant were created, edited, viewed, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history, to include bookmarked sites;

b. evidence of malicious software ("malware"), which is software designed to infiltrate a computer without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. The term "computer virus" is sometimes used as a catch all phrase to include all types of malware, including true viruses. Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, crimeware and other malicious and unwanted software.

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices, disks, CD ROMS, or similar containers for electronic evidence;

e. evidence of the times the COMPUTER was used;

f. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

g. evidence identifying the location from which images of child pornography were downloaded, including date and time of such downloads;

h. evidence identifying whether image and/or video files containing child pornography were ever viewed, to include date and time of such viewing;

i. evidence identifying whether images and/or videos files were deleted, to include date and time of deletion;

j. evidence relevant to the creation dates of all visual depictions of minors engaged in sexually explicit conduct, to include evidence derived from metadata obtained from child pornographic videos and images;

k. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER; and

l. contextual information necessary to understand the evidence described in this attachment.

DEFINITIONS

- Minor - a person under the age of 18 years. 18 U.S.C. § 2256(1)
- Visual Depiction - includes undeveloped film and videotape, data stored on computer disk or by electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. 18 U.S.C. § 2256(5).

Sexually Explicit Conduct -

(A) Except as provided in subparagraph (B), "sexually explicit conduct" means actual or simulated

(i) sexual intercourse, including genital genital, oral genital, anal genital, or oral anal, whether between persons of the same or opposite sex;

(ii) bestiality;

(iii) masturbation;

(iv) sadistic or masochistic abuse; or

(v) lascivious exhibition of the genitals or pubic area of any person;

(B) For purposes of subsection 8(B) of this section, "sexually explicit conduct" means

(i) graphic sexual intercourse, including genital genital, oral genital, anal genital, or oral anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;

(ii) graphic or lascivious simulated;

(I) bestiality;

(II) masturbation; or

(III) sadistic or masochistic abuse; or

(iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person. 18 U.S.C. § 2256(2).

- Child Erotica - materials or items that are sexually arousing to certain individuals but that are not in and of themselves obscene or do not necessarily depict minors in sexually explicit poses or positions. Such material may include non sexually explicit

photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals. Child Pornography - means any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

(B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. 18 U.S.C. § 2256(8).

- The terms "items," "images," "documents," "communications," "records," "materials," and "information" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD ROMs, DVRs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic

notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

- "Digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes, and memory chips; and security devices.

- "Image" or "copy" refers to an accurate reproduction of information contained on an original physical item, independent of the electronic storage device. "Imaging" or "copying" maintains contents, but attributes may change during the reproduction.

END OF ATTACHMENT B

ATTACHMENT C
Protocol for Search and Seizure of Computers, Electronic Storage Devices and Any Computer/Electronic Storage Media
(Collectively "Computer and Electronic Media")

1. If agents executing the search warrant conclude that would be impractical to search the computer and electronic media on site for the evidence, contraband, fruits of crime and instrumentalities specified in the warrant, agents will seize the same and conduct an off site search of the same.

2. Any search of computers and electronic media, on site or off, will be performed by a review team which may include agents, computer specialists, analysts, and/or attorneys and personnel presently involved in the investigation or otherwise, or any combination thereof (the "review team"). Original computer and electronic media will be, wherever possible, copied, or imaged, prior to the start of any search for evidence. The review team conducting the search will follow a protocol designed to uncover the information permitted by the terms of the warrant as set forth in attachment B.

3. If the original digital device was seized, law enforcement personnel will perform an initial search of the original digital device within a reasonable amount of time not to exceed 120 days from the date of execution of the warrant. If, after conducting the initial search, law enforcement personnel determine that an original digital device contains any data falling within the list of items to be seized pursuant to this warrant, the government will retain the original digital device to, among other things, litigate the admissibility/authenticity of the seized items at trial, ensure the integrity of the copies, ensure the adequacy of chain of custody, and resolve any issues that potentially might be raised regarding changed conditions of the evidence. If the government needs additional time to determine whether an original digital device contains any data falling within the

list of items to be seized pursuant to this warrant, it may seek an extension of time from the Court within the original 120-day period from the date of execution of the warrant.

4. If an original digital device does not contain any data falling within the list of items to be seized pursuant to this order, the government will return that original device to its owner and seal any image previously made of the device and not review the sealed image absent further authorization from the Court.

5. Notwithstanding the foregoing, if devices are evidence in and of themselves, or are subject to forfeiture as contraband, fruits or instrumentalities of the crimes set forth in the warrant, the government may retain the devices (and any software and data therein) in their original seized condition.

6. In addition, the review team will make one complete copy of all seized computer and electronic media.

END OF ATTACHMENT C

AO 93 (Rev. 12/03) Search Warrant

UNITED STATES DISTRICT COURT

EASTERN District of CALIFORNIA

In the Matter of the Search of

[redacted], APARTMENT 243
DAVIS, CALIFORNIA 95616

SEARCH WARRANT

Case Number: 2:11-SW-0150 GGH

TO: **FEDERAL BUREAU OF INVESTIGATION SPECIAL AGENT NICHOLAS PHIRIPPIDIS** and any Authorized Officer of the United States.

Affidavit(s) having been made before me by **NICHOLAS PHIRIPPIDIS** who has reason to believe that ☐ on the person of, or ☒ on the premises known as (name, description and/or location)

2505 5TH STREET, DAVIS, CALIFORNIA, as more particularly described in Attachment A, attached hereto and incorporated by reference.

in the Eastern District of California there is now concealed a certain person or property, namely (describe the person or property)

SEE ATTACHMENT B, ATTACHED AND INCORPORATED BY REFERENCE.

I am satisfied that the affidavit(s) and any record testimony establish probable cause to believe that the person or property so described is now concealed on the person or premises above-described and establish grounds for the issuance of this warrant.

YOU ARE HEREBY COMMANDED TO search on or before April 21, 2011 (extended 14 days from date of issuance)
Date

(not to exceed 10 days) the person or place named above for the person or property specified, serving this warrant and making the search ☒ in the daytime – 6:00 A.M. to 10:00 P.M. ☐ at anytime in the day or night as I find reasonable cause has been established and if the person or property be found there to seize same, leaving a copy of this warrant and receipt for the person or property taken and prepare a written inventory of the person or property seized and promptly return this warrant to **GREGORY G. HOLLOWS** as required by law.

U.S. Magistrate Judge (Rule 41(f)(f4))

APRIL 11, 2011 2:50 pm at **SACRAMENTO, CALIFORNIA**
Date and Time Issued City and State

GREGORY G. HOLLOWS
U.S. MAGISTRATE JUDGE
Name and Title of Judge

GREGORY G. HOLLOWS
Signature of Judge

RETURN	Case Number:	
DATE WARRANT RECEIVED	DATE AND TIME WARRANT EXECUTED	COPY OF WARRANT AND RECEIPT FOR ITEMS LEFT WITH
INVENTORY MADE IN THE PRESENCE OF		
INVENTORY OF PERSON OR PROPERTY TAKEN PURSUANT TO THE WARRANT		

CERTIFICATION

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

_____

Subscribed, sworn to, and returned before me this date.

EXHIBIT C

(March 29, 2011 FBI 302)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 3/29/2011

On November 30, 2010, an Administrative Subpoena was served on Comcast, requesting subscriber information for IP address 98.208.56.194 on 11/18/2010 from 13:00 and 14:00 PDT.

On December 1, 2010, Comcast responded to the subpoena stating that they were unable to find any information responsive to the request, and that their logs were either incomplete or contained an error associated with the registration of the cable modem or other device in question.

On December 28, 2010, an Administrative Subpoena was served on Comcast, requesting subscriber information for IP address 67.172.180.130 on 12/27/2010 from 07:00 and 08:00 PDT.

On January 12, 2011, Comcast responded to the subpoena stating that they were unable to find any information responsive to the request, and that their logs were either incomplete or contained an error associated with the registration of the cable modem or other device in question.

On March 22, 2011, an Administrative Subpoena was served on AT&T Internet Services, requesting subscriber information for IP Address 64.160.118.55 on 3/13/2011 from 16:00 and 18:00 PDT.

On March 29, 2011, AT&T Internet Services provided the following response:

Subscriber Name: Caitlin [redacted]
Address: [redacted] Apt 242, Davis, CA, 95618
Email: [redacted]@att.net
Telephone: [redacted]

[Writers Note: While the response listed " Caitlin Fitzgrald" as subscriber's name, open source database checks confirm "Caitlin Fitzgerald" is the accurate spelling.]

The subpoenas and results are attached and considered a part of this investigative report.

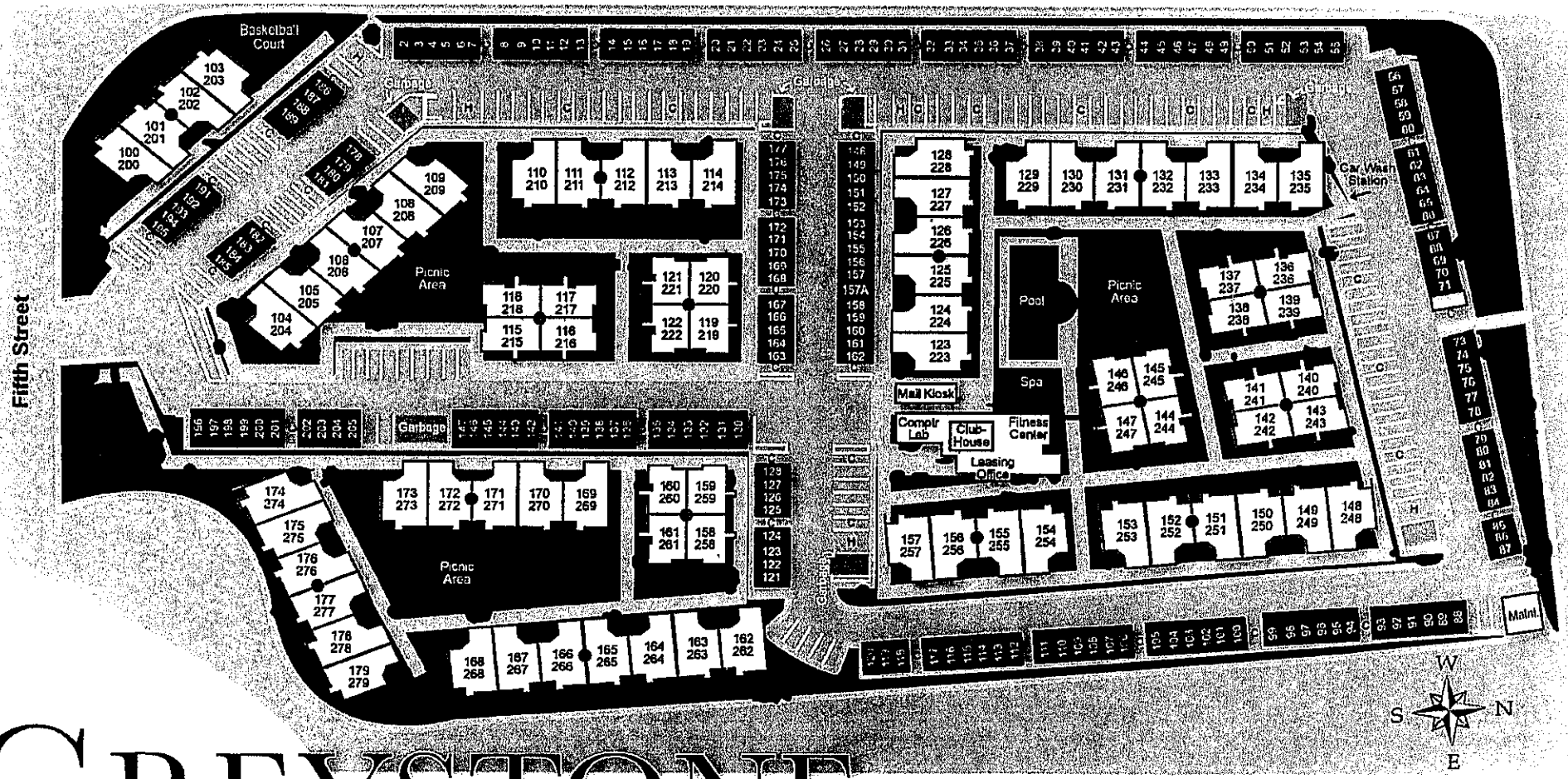
Investigation on 3/29/2011 at Sacramento, California

File # 305A-SC-36939, 270 305A-SC-44885 N68 5 Date dictated

by SA Nicholas G. Phirippidis 88ngp01.302

EXHIBIT D

(Greystone Apartment Complex)



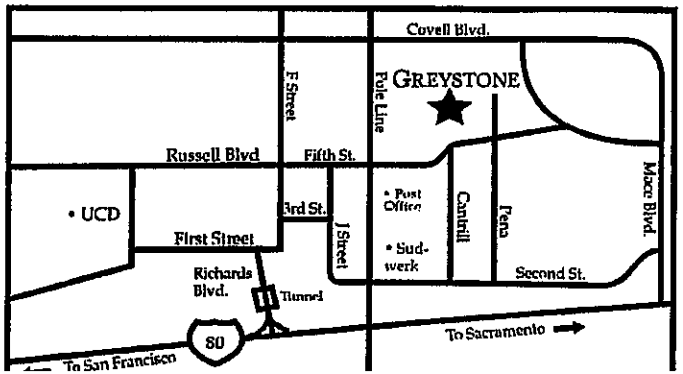
GREYSTONE Apartment Homes

2505 Fifth Street, Davis, CA 95616
(530) 758-2200 • fax (530) 758-2441

App. 118

Welcome to comfort, convenience, and a better lifestyle.

STONESFAIR



From Sacramento:
Take I-80 West to Mace Blvd. Exit. Take Mace Blvd north to 2nd Street. Turn left on 2nd Street. Turn right on Cantrill. Turn left on 5th Street. Greystone is on the right, directly across from Cantrill.

From San Francisco:
Take I-80 East toward Davis, past UC Davis & Richard Blvd exits. Take Mace Blvd north to 2nd Street. Turn left on 2nd Street. Turn right on Cantrill. Turn left on 5th Street. Greystone is on the right, directly across from Cantrill.

EXHIBIT E

(March 30, 2011 FBI 302)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/30/2011

On 3/29/2011, Special Agent (SA) Nicholas G. Phirippidis and Scott A. Schofield spoke with CORINA GARCIA, Apartment Manager, Greystone Apartments, [redacted], Davis, California, 95618, telephone number [redacted], cell phone number [redacted]. After being advised of the identities of the interviewing agents, and the nature of the interview, GARCIA provided the following information:

Caitlin Fitzgerald resides at [redacted], Apartment 242, Davis, California, 95618, and has lived there with two other females since 2009. The tenants in Apartment 242 are all college students at the University of California, Davis.

Apartment 242 is a three-bedroom, two-story residence that is located on the second floor of the apartment complex. There are two parking stalls associated with apartment 242: stalls 79 and 274 which are next to each other.

GARCIA provided the interviewing agents with a floor plan, apartment unit map, and a business card with her contact information. GARCIA provided basic demographic information about the adjoining apartments which were notated by SA Phirippidis on the map provided. The items provided by GARCIA have been placed in the 1-A subsection of the file.

Investigation on 3/30/2011 at Davis, California

File # 305A-SC-44885 Date dictated

by SA Nicholas G. Phirippidis 89ngp02.302
SA Scott A. Schofield

EXHIBIT F

(April 4, 2011 FBI 302)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/04/2011

On 04/01/2011, Special Agent Michael G. Cahoon conducted the following investigative activities:

With consent from the wireless network owner at [redacted], Apartment #242, Davis, California, 95618, SA Cahoon collected the following information:

Router Make:	AT&T
Router Model:	2701 HG-B Gateway
Serial Number:	370819109703
Router MAC Address:	00:22:A4:D5:F6:F0/1
Connection Type:	DSL
External (Public) IP Address:	69.105.80.128
Network SSID:	"2WIRE703"
Web Management IP Address:	192.168.1.254
System Password:	LoveShack703
Encryption Type:	WEP
Encryption Key:	2290548086

The following network devices appeared to be recently connected to the "2WIRE703" network due to being listed on the initial page of computers connected to the "Home Network"; NOTE: device "F2365524" was the device SA Cahoon used to connect to the network:

DEVICE NAME	INTERNAL IP ADDRESS	MAC ADDRESS
"192.168.1.114"	192.168.1.114	00:1b:63:ca:96:20
"F2365524"	192.168.1.66	N/A
"CHDwhitemacbook"	192.168.1.64	00:17:f2:43:bd:fc
"192.168.1.105"	192.168.1.105	00:1b:63:bf:46:60
"CK"	192.168.1.78	00:25:d3:d4:c4:73

A review of advanced router settings labeled "Wireless MAC Filtering" for allowed devices, showed an additional 28 wireless devices have connected to this network. Writer was unable to determine when logging began and duration of connections for each device.

Investigation on 04/01/2011 at Davis, California

File # 305A-SC-44885 Date dictated 04/04/2011

by SA Michael G. Cahoon:mgc 094mgc03.302

After discussions with the Case Agent and search team, it was determined that devices "192.168.1.114", "CHDwhitemacbook", and "192.168.1.105" were known devices to the network owner. The device "CK", with MAC address 00:25:d3:d4:c4:73 was not known to the network owner.

By using the software tool KISMET, it was determined that MAC address 00:25:d3:d4:c4:73, had a live connection to an unsecured wireless access point named "KT_WLAN", and assigned IP address 172.30.1.12.

KISMET is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. KISMET will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 801.11g, and 802.11n traffic. KISMET identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic. KISMET is unlike most other wireless network detectors in that is works passively. This means that without sending any loggable packets, it is able to detect the presence of both wireless access points and wireless clients, and associate them with each other.

KISMET passively collected the following identifiers on the wireless network "KT_WLAN":

SSID:	"KT_WLAN"
BSSID:	0A:0E:DC:2A:BF:F5
Type:	Access Point
Channel:	5
IP Address:	172.30.1.0
IP Netmask:	255.255.255.240

Digital videos of the investigative activities were burned to a compact disc and stored in a 1A envelope for retention and retrieval purposes.

EXHIBIT G

(April 5, 2011 FBI 302)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/05/2011

On 04/01/2011, Special Agent (SA) Darren M. Holtz and SA Laura E. Giouzelis conducted the following investigative activities:

With consent from the wireless network owner at [redacted], Apartment #242, Davis, California, 95618, the AT&T wireless router with Machine Address Code (MAC) address 00:22:a4:d5:f6:f0 was searched.

One computer identified connected to the wireless router and was not found in the residence. This computer connected via a wireless device with MAC address 00:25:d3:d4:c4:73.

MOOCHERHUNTER was installed on a laptop and connected to a directional antenna. The program was given the MAC address 00:25:d3:d4:c4:73 and approximately 17 readings were taken in the vicinity of the residence. A review of the data identified that readings were significantly higher when the directional antenna was pointed at the third floor southern most bedroom of apartment #243.

It was concluded that the wireless device with MAC address 00:25:d3:d4:c4:73 was located in the third floor southern most bedroom of apartment #243. Notes of these readings were placed in the 1A section of this file.

MOOCHERHUNTER is a free, downloadable, mobile tracking software tool, for the geo-location of wireless devices. MOOCHERHUNTER has the ability to identify the location of an 802.11-based wireless device by the traffic sent across a network. MOOCHERHUNTER enables the user to detect traffic from a wireless client passively.

According to the website securitystartshere.org, "In residential and commercial multi-tenant building field trials held in Singapore in March 2008, MOOCHERHUNTER allowed a single trained operator to geo-locate a wireless moocher with a geographical positional accuracy of as little as 2 meters within an average of 30 minutes."

Investigation on 04/01/2011 at Davis, California

File # 305A-SC-44885 Date dictated 095dmh01.302.wpd

by SA Darren M. Holtz:dmh
SA Laura E. Giouzelis

EXHIBIT H

(MoocherHunter Webpage)

http://securitystartshere.org/page-training-oswa-assistant.htm#moocherhunter

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).
(for **MoocherHunter™ Law Enforcement Edition**, please see below)

100% Made-In-Singapore with **ThinkSECURE**-proprietary code, MoocherHunter™ was first unveiled to Southeast-Asian law enforcement officials at the Singapore Police Force's invitation-only CyberCrime Investigation Workshop 2008 held in Singapore in April 2008.

MoocherHunter™ is licensed under the **MoocherHunter™License** as part of the OSWA-Assistant™ wireless auditing LiveCD toolkit (note: only on version 0.9.0.3b and above) which is free for end-user download at **http://oswa-assistant.securitystartshere.org**.

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.

Because it is not based on fixed or statically-positioned hardware, MoocherHunter™ allows the user to move freely and walk towards the actual geographical location of the moocher/hacker. And of course, as part of the free **OSWA-Assistant™** wireless auditing LiveCD toolkit, MoocherHunter™ is also **FREE** for end-users to use on their existing laptops (so long as it is ***only*** run within the **OSWA-Assistant™** environment) with off-the-shelf supported wireless cards.

In residential and commercial multi-tenant building field trials held in Singapore in March 2008, MoocherHunter™ allowed a single trained operator to geo-locate a wireless moocher with a geographical positional accuracy of as little as 2 meters within an average of 30 minutes.

Download MoocherHunter™ and the OSWA-Assistant™ **here**.

Notes:
*(i) For accurate and proper results, please remember to **use a directional antenna,** and **not** an omni-directional one, regardless of whether it claims to be high-gain or not.*

*(ii) If you get a Segmentation Fault while running MoocherHunter™ (e.g. your WNIC shuts itself down halfway), please make sure the process is killed before restarting. You can issue a "**ps -eaf**" command, look for the process ID tied in to the segfaulted process and then type "**kill (process ID)**" where (process ID) is the PID number.*

*(iii) As of version 0.6.5, please make sure you select the correct chipset which your wireless card is based on, otherwise your results will be wrong, even if the program starts up. The officially-supported chipsets for MoocherHunter™ ver 0.6.9a & up are: **Prism54G(HARDMAC),Atheros (all models before AR9xxx series),RTL8187, RT2500, RT2570, IPW2200** and **IPW2915**.*

http://securitystartshere.org/page-training-oswa-assistant.htm#moocherhunter

For police and other legitimate Asian law-enforcement organizations in who have auditing compliance requirements, or who require a low-profile, covert solution during prosecution of a wireless-using suspect, we also provide the MoocherHunter™ Law Enforcement Edition to meet your needs.

MoocherHunter™ Law Enforcement Edition is a totally-redesigned, standalone, low-profile/covert-tracking commercial software solution which adds in some additional nifty features such as a remote-control web interface, 802.11a support, AP-hunting, evidence-logging and more. Please note that the MoocherHunter™ Law Enforcement Edition is NOT found on the OSWA-Assistant™!

Please contact us regarding purchasing this separate commercial solution.

(note: please send your enquiry from a law-enforcement or similar corporate/organization address - we will not release any information to enquiries originating from free email service providers)

EXHIBIT I

(Declaration of Brandon Jelinek)

JOSEPH SCHLESINGER, #87692
Acting Federal Defender
LEXI NEGIN, #250376
Assistant Federal Defender
801 I Street, 3rd Floor
Sacramento, California 95814
Telephone: 916/498-5700
Facsimile: 916/498-5710
E-mail: lexi_negin@fd.org

Attorneys for Defendant
ALEXANDER NORRIS

IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. ALEXANDER NORRIS, Defendant.	Case No. 2:11-CR-00188-KJM DECLARATION OF BRANDON JELINEK IN SUPPORT OF DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

DECLARATION

I am over the age of 18; and, competent to testify to the matters contained herein.

I am employed as the Director of E-Discovery, for Global CompuSearch LLC, Spokane, Washington. We also have offices in Palm Springs, California, Sacramento, California, and Portland, Oregon. I am primarily based in Spokane, Washington. I have been consulting with Global CompuSearch since 2006 and began full-time employment in 2013. Global CompuSearch LLC provides consulting, e-discovery, forensics and training services on legal issues related to computers and the Internet.

Prior to my employment at Global CompuSearch, I was employed by the Presbyterian Church as the IT Director for the Synod of Alaska Northwest. My primary responsibility was to assist

organization within the denomination with setup of their network systems, web presence and software usage.

In addition, I have owned and operated Jelpro. Jelpro provided software and database consulting services and assistance with network reconstruction for technology based legal consulting firms. I also designed and programmed a wide variety of database systems and applications ranging from web systems to content management and financial accounting programs. Our services included configuration and administration of wireless networking in a wide variety of environments and scales.

I graduated with a Bachelor of Arts degree from Whitworth University in 1994.

Throughout my career, I have been called on to provide professional services related to wireless networking, software testing and functional hardware validation. I have worked with a wide variety of wireless devices; Cisco, D-link, Ceton, Alpha, Realtech, Linksys, Microsoft, Belkin and many more less-known manufacturers. I have configured networks utilizing wireless bridges over long distances and designed systems for both server-to-server and server-to-client communications. I have built wireless systems for small and medium businesses ranging from contractors to legal firms, to larger church campuses.

Our company was retained by Lexi Negin, Assistant Federal Defender, at the Office of Federal Defender to research and consult with her about a tool called Moocherhunter. In doing so, I reviewed the available discovery in the case and consulted with Ms. Negin about my evaluation of Moocherhunter as a software tool used to track wireless moochers.

In order to learn about Moocherhunter, I went to its website http://securitystartshere.org. I also attempted to locate peer reviews or independent testing of Moocherhunter and I was unable to find any independent testing results, peer reviews, or other independent reporting in my field about Moocherhunter. There were some articles talking about Moocherhunter, but none that would allow me as an expert to conclude anything about the program's reliability or acceptance in my field.

I learned from the website that Moocherhunter is not open-source. The license agreement

states that the source code is proprietary. I have the ability to review source code and cannot do so with Moocherhunter.

As a professional software engineer, e-discovery expert, and former business networking solutions provider, I would not install and use mission critical software like Moocherhunter from an unknown developer in a production environment without positive third party reviews and testing. In addition, I would need to review and test the software myself in a test environment. In my professional experience, I would be suspect of free-to-use programs developed outside of our country from unknown developers, like Moocherhunter. I would be especially weary of the software if it is not open-source and not downloadable from credible repositories. I would be concerned that the program contains malware and could be pretending to perform its function but would in actuality be mining my computer for information.

Moocherhunter uses a Linux distribution that they packaged themselves in 2006. The drivers for the wireless card are part of the operating system. There are 2013 Linux distributions with current wireless drivers but because Moocherhunter's license demands Moocherhunter be used only with their distribution, I am forced to use the 2006 operating system rather than more popular and more up-to-date distributions. This makes it increasingly difficult to scan and test the package for malware because their distribution does not allow me to install current virus scanning utilities to ensure there are no hidden processes.

So that I could use Moocherhunter and examine the program, I downloaded for free the latest available version of the program which I believe is the same version that the FBI used in this case. Moocherhunter is a utility that is part of the OSWA package produced in Singapore by a company called Think Secure.

The advertised goal of Moocherhunter is to locate the source of a wireless signal.

In order to achieve this goal, the user must perform the following actions.

1. Connect a wireless card that utilizes one of the Moocherhunter's supported

chipsets.

2. Connect a directional antennae to the wireless card.
3. Boot their laptop using the OSWA operating system.
4. Start the wireless card and place it in monitor mode.
5. Execute Moocherhunter in either passive mode or active mode.
6. In passive mode, select the MAC address you wish to locate that is connected to the router being examined. In active mode, type in the MAC address of the device you wish to locate.
7. Point the directional antennae in all three dimensions in various directions.
8. Determine the most likely direction, factoring in the Power, Control, Management, and Dataframes readings.
9. Move to a different location in the area.
10. Repeat steps 6 and 7 until you have taken readings all around the most likely direction.
11. Move in towards the most likely location of the device.
12. Repeat steps 7-11 until you discover the source of the wireless signal.

In theory, by aggregating readings in a method similar to the way submarines use sonar to locate objects, one can use Moocherhunter to hone in on the geographical location of the radio signal thus finding the device that has been connected to the router.

There are several factors that will affect the results. Multiple devices could be set to spoof or share the same MAC address. Second, the power reading alone can be misleading and does not provide enough detail to determine the direction of the wireless device. Third, the type of antennae and network card are of critical importance and should to be tested prior to being used in the field to ensure they function as advertised.

Moocherhunter in active mode works by entering the MAC address of the device for which

one is looking. Moocherhunter then looks for a wireless signal emanating from the device with that MAC address. In this mode, Moocherhunter would produce conflicting results if multiple individuals were using the same MAC address. There are several techniques people use to spoof MAC addresses and even the OSWA system that Moocherhunter is installed with has a utility that allows computer users to change their MAC address. In passive mode the user of Moocherhunter would have to look for multi-cast spoofing and other MAC address manipulation techniques and systematically eliminate alternative sources.

According to a video published by Moocherhunter that I viewed, the direction of the wireless device is found by reading and understanding the relationship between the Power reading and the Control/Management/Dataframes (C/M/D). The power reading alone is not enough information to determine the direction of the wireless device. The video instructs that "you have to look at all of these in conjunction with each other to be able to get the idea of the direction of the attacker or moocher..." In fact, they even refer to the power reading from the hardware as "Arbitrary." The FBI reported that it took 16 readings on one date and 17 readings on another however, the complete readings taken by the FBI agents in this case were not available in discovery. The only available indication of the readings taken by the FBI is an overview of an apartment complex and of four apartments with numbers and arrows written in. There was only one number indicated, which I assume might be the agent's recording of highest Power reading when pointing in that direction, but I did not see any indication of the C/M/D readings that according to Moocherhunter must be considered in conjunction with the Power readings. Having used Moocherhunter and tested it in a controlled environment, I know that the power readings constantly fluctuate and sometimes do so faster than the eye can see. To document the power reading of a specific direction it would be more accurate to document the range of power readings taken over short period of time rather than choose one of the results and document only that number. That being said, if the agents only noted the power readings, according to the Moocherhunter video, that would be insufficient to obtain any accurate results. How to read these 4

numbers and determine the direction of the wireless devices is not documented in their program.

According to the Moocherhunter website, the antenna can create false readings depending on its strength and type. I did some testing on Moocherhunter which will not be fully reported here, but I found that depending on the strength of the antenna and the strength of the wireless device, an antenna that is particularly strong could read the power setting of 100 even when pointing in the opposite direction at 15 feet from the location of the device, even when the manufacturer of the antenna clearly labels the antennae as directional.

In reviewing the program and its interface, although Moocherhunter advertises as being user-friendly, it really requires knowledge of Linux and a good understanding of the 802.11 wireless protocols. For example, while using Moocherhunter, a note on the screen indicated:

> ...some wireless cards have a nasty habit of auto-shuting down (sic) halfway. This results in an error message, e.g. segmentation fault, pcap_open error, etc. If your card behaves this way, when you see any error messages similar to the above, please do an 'ifconfig your_interface up' and then do a 'ps-eaf' and ensure you that kill off all existing MoocherHunter processes before restarting MoocherHunter, otherwise MoocherHunter will not work, detect anything or be accurate. Please use a directional antenna when using MoocherHunter. More information regarding GUI commands can be found by pressing 'SHIFT-H' in the GUI screen (pls maximize your terminal screen/window for the help display to appear & press ESC to exit).

This inability for Moocherhunter to detect an error and correct itself indicates to me that the programmers of Moocherhunter did not take the time to develop an error recovery system within the program to address this kind of issue. As a programmer, this concerns me because it makes me wonder what other errors their program might simply ignore. Since there is no logging system for readings taken and no logging system for errors encountered, I am left with guessing if the software is performing as intended.

In summary:

Moocherhunter has not been subjected to peer review, formal testing or coding analysis and as a result its reliability is questionable. Given that there are several other tools used in our profession to accomplish the goal of locating a wireless device, and that those tools are open-source, have substantial

peer review, and work on current operating systems, I would not choose to use Moocherhunter to locate active wireless devices.

The discovery provided to me to date to did not contain more than a single power reading and general direction attributed to that result. Because I would expect a full report to include more specifics about the range of power readings in a single direction, readings in a number of directions at each location and include the other relevant data points (Control/Management/DataFrame) this leads me to conclude that the agents did not adequately record the readings of MoocherHunter and may not have used the appropriate technique to accurately determine the direction of the wireless device in this case.

I swear under the penalty of perjury that the above Declaration is accurate to the best of my ability.

X

Brandon Jelinek
E-Discovery Director
Signed by: Brandon Jelinek

April 1, 2013
Date

EXHIBIT J

(April 14, 2011 FBI 302)

FD-302 (Rev. 10-6-95)

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/14/2011

On 04/08/2011, Special Agent (SA) Darren M. Holtz and SA Nicholas G. Phirippidis conducted the following investigative activities:

With consent from Caitlin Fitzgerald, the wireless network owner at [redacted], Apartment #242, Davis, California, 95618, the AT&T wireless router with Machine Address Code (MAC) address 00:22:a4:d5:f6:f0 was searched.

(Fitzgerald had previously signed an FD-941 "Consent to Search Computer" form, an "Authorization to Intercept the Communications of a Computer Trespasser" form, and a "Consent to Monitor Content of Electronic Communications" form on 4/1/2011.)

Two computers were identified as connected to the above wireless router but were not in the residence. The first computer was identified as "CK" and had the MAC address 00:25:d3:d4:c4:73. The second computer was identified as "bootycop" and had the MAC address of 00:1f:1f:49:d3:11.

MOOCHERHUNTER was installed on a laptop and connected to a directional antenna. The program was given the MAC address 00:25:d3:d4:c4:73. MOOCHERHUNTER was unable to identify any wireless signals in the area broadcasted with the above listed MAC address. A second search of the AT&T wireless router listed the computer "CK" as inactive and not connected to the network.

MOOCHERHUNTER was given the MAC address 00:1f:1f:49:d3:11, and approximately 16 readings were taken in the vicinity of the residence. A review of the data identified that readings were significantly higher when the directional antenna was pointed at the third floor, southern most bedroom of apartment #243. Several pictures and a video were taken of this process. This digital evidence has been placed on an optical disk and will be maintained in the 1A section of this file.

It was concluded that the wireless device with MAC address 00:1f:1f:49:d3:11 was located in the third floor southern most bedroom of apartment #243.

Investigation on 04/08/2011 at Davis, CA

File # 305A-SC-44885 Date dictated 104dmh01.302.wpd

by SA Darren M. Holtz:dmh
SA Nicholas G. Phirippidis

MOOCHERHUNTER is a free, downloadable, mobile tracking software tool, for the geo-location of wireless devices. MOOCHERHUNTER has the ability to identify the location of an 802.11-based wireless device by the traffic sent across a network. MOOCHERHUNTER enables the user to detect traffic from a wireless client passively. No data is transmitted from the computer running MOOCHERHUNTER, data is only monitored. MOOCHERHUNTER does not collect packets of data, it only displays the number of packets encountered and the signal strength of each.

SA Phirippidis verified that only the computer identified as "bootycop" with MAC address 00:1f:1f:49:d3:11 was connected to the AT&T wireless router with Machine Address Code (MAC) address 00:22:a4:d5:f6:f0. SA Holtz then connected a laptop to the AT&T wireless router and started to capture the wireless network traffic. SA Phirippidis conducted an online undercover session where files were downloaded containing child pornography from BOYFORBOYS1.

At the end of the undercover session, SA Holtz discontinued collecting the wireless network traffic. The data file that contained the network traffic was 3.7 Megabytes. SA Phirippidis confirmed that approximately 3.6 Megabytes had been downloaded during this undercover session. The captured data was placed on an optical disc and will be maintained in the 1A section of this file.

DECLARATION

I, Darren Holtz, declare as follows:

1. I am a Special Agent with the Federal Bureau of Investigation; I have been so employed since 2008. I am currently assigned to the Springfield Division of the FBI, Cyber Crime Squad, where I investigate computer crimes. 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 a Bachelor of Science degree in Computer Science from Florida State University and a Master of Science degree in Computer Science from Florida State University. I hold a certificate of Information Systems Security Professional by the NSTISSC. Prior to the FBI, I taught introductory computer applications for Florida State University, Tallahassee, Florida in 2002. I then became software engineer, designing medical software for Cerner, Inc. Kansas City, Missouri for approximately five years.

2. The last week in March, 2011, writer downloaded a Moocherhunter OSWA live CD and tested the application for functionality. Prior to testing, writer reviewed a video published by Think Secure, the creators of Moocherhunter. The video demonstrated the proper setup and use of Moocherhunter.

3. The appropriate network card and directional antenna were used during testing and use. The specific chipset of the network card was RT8187. Three different directional antennas were tested; the antenna with the highest resolution was used during triangulation.

4. Multiple tests of the equipment/system were conducted at writer's personal

residence. For initial testing, the target computer was a Toshiba netbook computer. Testing included the affect of triangulation wireless signal through multiple sheet rock and stucco walls, hallways, waterbed, steel frames, and windows.

5. After testing at personal residence, testing was conducted by FBI SA Darren Holtz and FBI SA Michael Cahoon in an office building. The following devices were triangulated: Apple Ipad, Apple Ipod touch, Apple Macbook, Motorola Droid phone, and a HP laptop.

6. It was noted that the directional antenna would lose effectiveness if placed too close to the laptop. Placing the directional antenna too close to the laptop would cause the antenna to operate as an omni-directional antenna. This was mitigated by working in a two man team. One person would operate the laptop while the second person would operate the directional antenna.

7. The signal strength number is arbitrary, for triangulation purposes the relative signal drop was important. Writer noted a significant signal drop within 30 degrees of deflection when the target device was more than 5 yards away from the directional antenna. The further away the target device, less deflection is needed to see a significant signal drop.

8. The Moocherhunter software functioned without error or crash during testing and satisfactorily identified the location of each target device. Settings recommended by Think Secure were followed.

9. During the triangulation on April 8, 2011 readings were taken from many of the same locations as the triangulation on April 1, 2011.

I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed this 29th day of April 2013.

/s/ Darren Holtz
DARREN HOLTZ
Special Agent
Federal Bureau of Investigation

DECLARATION

I, NICHOLAS PHIRIPPIDIS, declare as follows:

1 I am a Special Agent with the Federal Bureau of Investigation, and have been so employed since November 2007. Prior to my employment with the FBI, I was a Software Application Engineer for approximately 2 years. I have a Bachelor of Science degree in Computer Science from the University of California, San Diego.

2 On approximately March 28, 2011, I opened and became the lead FBI Special Agent on the investigation into "boyforboys1" aka ALEX NORRIS. This investigation concerns the distribution of child pornography through a peer to peer file sharing program, as well as utilizing a wireless internet connection that was illegally obtained through hacking.

3 As the lead Special Agent, I participated in all aspects of the investigation, and concurred with all investigative decisions that were made. I also consulted regularly with the assigned prosecutor from the United States Attorney's Office, AUSA Matthew Morris.

4 Based on the facts of this particular investigation, and specifically the difficulty in identifying ALEX NORRIS via internet subscriber records, I suspected that ALEX NORRIS had an above-average knowledge of computers and the internet (or at a minimum was tampering with internet hardware). With this knowledge, during our initial search warrant, we took specific steps to prepare ourselves in the event that we were dealing with a sophisticated computer hacker. Namely, we executed our search warrant at [redacted] #242, Davis, CA (Apartment 242) in a "low key, knock and talk" style, wearing plainclothes. This was done not only to minimize the intrusiveness and shock on the potential victims residing in

Apartment 242, but also to not alert a would-be hacker living next door. Additionally, we considered researching technologies that would allow us geographically locate a hacker's computer if, in fact, there was a trespasser on the network at Apartment 242.

5 I spoke with Special Agent Darren Holtz about using technology that could locate a rogue computer on a wireless network. During that discussion, MOOCHERHUNTER was mentioned.

6 During the last week of March 2011, Special Agents of the FBI Cyber squad as well Task Force Officers of the Sacramento County High Technology Crimes Task Force conducted a test of MOOCHERHUNTER at the Task Force headquarters located at 3720 Dudley Ave, McClellan, CA. I was present during this test. Before seeing the capabilities of MOOCHERHUNTER firsthand, I was skeptical that it would be accurate enough for our investigative needs. After witnessing MOOCHERHUNTER work in this test, I could immediately see its accuracy in real-time. I observed the relative signal strength on the MOOCHERHUNTER interface directly correlate with the position of our directional antenna in relation to a wireless device.

7 On April 8, 2011, I, along with SA Darren Holtz and Task Force Officer Sean Smith, Sacramento County Sheriff's department used MOOCHERHUNTER to locate ALEX NORRIS' computer "bootycop" as it was trespassing onto the wireless network owned by Apartment 242. I was responsible for holding the directional antenna away from the laptop as the readings were taken. At my direction, photographs were taken of the laptop screen showing the relative change in signal strength as the directional antenna was repositioned as a way to document this activity. Every signal reading that we saw supported the

conclusion that the hacker was located in the upper bedroom of Apartment 243: neither I nor anybody on my team ignored or normalized any signal readings.

8 In using the term "open source" to describe MOOCHERHUNTER on April 11, 2011, I used the term to mean that there was no requirement placed on me by the FBI to acquire the software from a single-source supplier.

9 I declare under the penalty of perjury that the foregoing is true and correct to the best of my knowledge. Executed this 30th day of April 2013.

	/s/ Nicholas Phirippidis NICHOLAS PHIRIPPIDIS Special Agent Federal Bureau of Investigation