UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

UNITED STATES OF AMERICA

v. CASE NO. 6:19-cr-1-Orl-40LRH

RONALD HILL

UNITED STATES' RESPONSE IN OPPOSITION TO DEFENDANT'S MOTION TO SUPPRESS EVIDENCE AT DOC. 35

The United States of America, by Maria Chapa Lopez, United States Attorney for the Middle District of Florida, files its response in opposition to the defendant's motion to suppress evidence at Doc. 35.

I. *Procedural Background*

1. The defendant is facing a two-count Indictment for distribution and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and (5)(B). Doc. 10.

2. On April 17, 2019, the defendant filed a motion to suppress evidence, specifically, alleging that the search warrant executed by the agents in this case only authorized the "seizure of electronic devices and specific data within those devices," but not the "search of the devices without another warrant." Doc. 35. The defense, thus, alleges that the "lack of probable cause finding to search all of the seized electronic devices resulted in a violation of Mr. Hill's Fourth Amendment rights. *Id*. Therefore, the defense requests that all evidence obtained as result of the "unlawful" search be suppressed. *Id*.

3. The United States maintains the affidavit and search warrant at issue in this case were entirely proper, and the affidavit (which was incorporated by reference to the search warrant) supported a finding of probable cause to allow the seizure of electronic devices as well as the search of those devices for evidence of child pornography violations. *See* Exhibit 1, Attachment B.[1] Alternatively, the United States maintains the law enforcement officers who executed the search warrant did so in good faith reliance on a search warrant properly issued by a neutral and detached judge, and thus the evidence found as a result should not be excluded.

II. ***Factual Background***

On December 4, 2018, SA Kevin Kaufman swore an affidavit in support of a search warrant before United States Magistrate Judge Karla R. Spaulding. Exhibit 1. SA Kaufman requested authorization to search Hill's residence (the "PREMISES") for evidence of the crimes of possession and distribution of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B). *Id.* Specifically, paragraph 6 of the Affidavit states:

> I am requesting authority to search the entire PREMISES—**including the curtilage, residential dwelling(s), and any computer, computer media, or electronic storage devices located therein**, where the items specified in Attachment B may be found. I also request to seize all items listed in Attachment B as instrumentalities, contraband, and evidence of criminal activity. *Id.* (emphasis supplied.)

The "Details of the Investigation" section of the affidavit indicated that on November 12, 2018, Federal Bureau of Investigation (FBI) Special Agent (SA) "SA

[1] The defendant's street address was redacted from Exhibit 1, in order to protect his privacy.

[Michelle] Langer—acting in an undercover capacity and using a P2P[, peer-to-peer,] file-sharing program known as Bittorrent Roundup—downloaded multiple images and videos of child pornography from a computer using IP address 184.90.145.34." Exhibit 1, ¶ 33.

SA Kaufman further alleged in the affidavit that on "November 12, 2018, the P2P file-sharing program determined IP address 184.90.145.34 was sharing a torrent with a particular info hash value. This torrent file referenced 23 files, at least one of which was a file of investigative interest to child pornography investigations." *Id.*

According to SA Kaufman's affidavit, "[o]n November 12, 2018, between 5:53 p.m. and 5:56 p.m., SA Langer completed a single-source download from IP address 184.90.145.34. Exhibit 1, ¶ 34. During the single-source download, SA Langer downloaded two complete files and three partially complete files," which contain child pornography. *Id.* SA Kaufman described two of the complete files as follows:

- **"(Pthc) 6Yo Babyj – Bedtime Rape.xxx"**: The video is approximately 1 minute 5 seconds in length. The video features a female child approximately 4-5 years old. The 4-5 year old child is naked on a bed under a bed sheet. An adult male performs oral sex on the child, digitally penetrates the child's vagina, and masturbates until he ejaculates onto the child's vagina.

- **"12 yo girl raped.xxx"**: The video is approximately 2 minutes 1 second in length. The video features a female child approximately 11-12 years old. The child's legs are bounded while an adult male vaginally and anally rapes the child until he ejaculates on the child's stomach. *Id.*

SA Kaufman also indicated in the affidavit that "[a query of IP address 184.90.145.34 was made through the American Registry for Internet Numbers

(ARIN). Exhibit 1, ¶ 36. ARIN reported that IP address 184.90.145.34 was registered to Charter Communications, Inc. (Charter Communications)." *Id.*

Then "[o]n November 15, 2018, a subpoena was served on Charter Communications regarding IP address 184.90.145.34 to obtain certain subscriber information in effect as of November 12, 2018. Exhibit 1, ¶ 37. Charter Communications returned the following information in response to the subpoena:

Customer Name:	R.H. [namely, Ronald Hill]
Service Address:	[xxxx], Sanford, Florida 32773 (Namely, the PREMISES)
Time of Download:	Active since April 26, 2018, and assigned to the PREMISES." *Id.*

According to SA Kaufman's affidavit, "[t]he address listed on the subscriber information was run through the Florida Driver and Vehicle Identification Database (DAVID) and showed it as the primary residence of R.H. and E.H. [xxxx] Sanford, Florida 32773. Additionally, their son R.H., Jr. [namely, the defendant,] had utilized that address as a primary residential address since May 2018." Exhibit 1, ¶ 38.

In paragraph 40, under the heading "COMPUTER DATA," SA Kaufman specifically requested "to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B)."

SA Kaufman clearly articulated in the affidavit the nexus connection between Hill's residence, computer media, and the commission of child pornography offenses. For that reason, SA Kaufman requested permission from the Court to locate computers believed to be at Hill's residence, and to search them in order "to locate not only computer files that might serve as direct evidence of the crimes described in the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES …" Exhibit 1, ¶ 42. The Affidavit also spelled out the search process as it pertains to the examination of computer media, to include the seizure, imaging, copying of storage media that may reasonably appear to contain evidence described in the warrant, as well as the later review of the media or information consistent with the warrant. Exhibit 1, ¶ 40-44.

The search warrant authorized by the Court included the search and seizure of computer media consistent with the limitations set forth by Attachment B. Attachment A described the location of the PREMISES, whereas Attachment B listed the items to be seized in reference to the crimes of distribution and possession of child pornography. The items listed in Attachment B included computer and storage media, electronically stored information, images, and records directly linked to the above mentioned violations. Exhibit 1, Attachment B. Additionally, Attachment B explained that "the terms records, documents, programs, applications or materials include records, documents, programs, applications, files or materials

created, modified or stored in any form, including by computer hard drives, external hard drives, thumb drives, cell-phones, smart phones, floppy disks, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage devices. *Id*.

On December 6, 2018, the FBI executed the search warrant at the above-mentioned address in Sanford, Seminole County, Florida. At approximately 7:00 a.m., Hill answered the front door of his residence. FBI SA Kaufman asked Hill to step out of the residence and Hill exited his residence. SA Kaufman introduced FBI SA Rodney Hyre (Hyre), informed Hill that the FBI had a search warrant to search his residence, and that they were going to clear the residence. Approximately seven agents conducted a protective sweep of the residence and then the residence was searched consistent with the parameters set forth in the search warrant.

During a noncustodial and consensual interview, Hill admitted using a Bittorrent file-sharing program to view child pornography. Hill began viewing child pornography approximately 10 years ago. Hill utilized his laptop computer to view and download the child pornography while in his residence. Hill viewed and masturbated to the videos and images of child pornography he downloaded.

Hill set up the Bittorrent file sharing program to download the videos and images of child pornography to his "C" drive on his laptop computer. Hill purposely altered the Bittorrent program to make downloads slower for users who were attempting to download files from his computer. Hill did this to increase his download speed; thus, demonstrating he knew how the Bittorrent file-sharing program operates

and its file-sharing capabilities. Hill acknowledged that by using the Bittorrent program he was distributing child pornography to other Bittorrent users.

Hill deleted the images and videos after he viewed them. Hill was asked about a child pornography series titled "Baby J" and Hill acknowledged that he had attempted to download the series but was unable to get a complete download of the files within the torrent. This torrent file is consistent with the undercover downloads SA Langer downloaded on November 12, 2018, from Hill's IP address. SA Kaufman showed the downloaded files and file names that SA Langer had downloaded from Hill during the undercover session on November 12, 2018. Hill recognized the file names and videos as the ones he downloaded, possessed, and viewed utilizing a VLC Player application.

During the interview, Hill indicated that he had been arrested for the sexual molestation of one of his relatives; Hill alleged the child was 3 or 4 years old at the time of the alleged incident. Hill indicated that those charges were eventually dropped. However, the FBI pursued this investigative lead and found that on or about October 31, 2003, Hill sexually molested a close relative. The victim is now a young adult willing to testify about the incident. Additionally, the victim's mother corroborated the incident. The incident involved Hill placing his hand under the child's panties and rubbing his fingers against her vaginal area, while the child was sleeping.

An onsite forensic review was conducted of Hill's laptop computer. During the forensic review, SA Alexis Brignoni located the "VLC Player" application on Hill's laptop computer. Inside the VLC Player application there was a log of the recent

videos Hill viewed utilizing the VLC Player application. Within the log, SA Brignoni located several viewed files with names indicative of child pornography content. In particular, two videos titled, "(Pthc) 6Yo Babyj – Bedtime Rape.xxx," and "12 yo girl raped.xxx." were located within the VLC Player log. Per the VLC Player application log, Hill viewed both videos on November 20, 2018. The videos viewed on November 20, 2018, were the same videos that were downloaded during the undercover session on November 12, 2018.

III. *The Search Warrant Is Not Overbroad*

The defendant does not question whether there was probable cause to search the defendant's residence. He erroneously alleges the search warrant did not include the search of computer media found at Hill's residence, by conveniently overlooking the clear definitions, context, and scope outlined in the affidavit and, most importantly, Attachment B.

It bears not that SA Kaufman's affidavit was based on a "Premises Computer Search Warrant Affidavit template provided by the Computer Crime and Intellectual Property Section (CCIPS); the office responsible for implementing the Department of Justice's national strategies in combating computer and intellectual property crimes worldwide. The link to the template indicates: "Use this to search a defendant's home or office. The warrant also authorizes law enforcement to conduct a forensic examination on any computers or storage media found in the home or office, without an additional warrant."

In this case, SA Kaufman had probable cause to believe that a computer located at Hill's residence contained child pornography, but did not know which computer that might be. As a result, the warrant authorized the search of the residence to locate, search, and seize all records, including computer media and storage devices, to search for evidence of child pornography pertaining to the distribution and possession of child pornography. *See* Attachment B. It follows then that the warrant did authorize the search and seizure of computer media and storage devices, the search warrant was not overbroad, and the search of the computers was within the scope of the search warrant.

The Fourth Amendment requires a search warrant "particularly describing the place to be searched and the persons or things to be seized." U.S. Const. amend. IV. "The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant." *Marron v. United States*, 275 U.S. 192, 196 (1927). "[A] warrant which fails to sufficiently particularize . . . the things to be seized is unconstitutionally over broad." *United States v. Travers*, 233 F.3d 1327, 1329 (11th Cir. 2000). However, the scope of a lawful search is "defined by the object of the search and the places in which there is probable cause to believe that it may be found." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987) (citing *United States. v. Ross*, 456 U.S. 798, 824 (1982)). Moreover, a search warrant is not overbroad when it is "limited... to the instrumentalities of the specified offense." *United States v. Osborne,* 630 F.2d 374, 378 (5th Cir. 1980).

With respect to the search of electronic devices and media, those warrants are sufficiently particularized if they limit the search of those devices and media to evidence of certain criminal violations. *United States v. Brooks*, 2014 WL 292194, at *12 (M.D. Fla., January 27, 2014) (collecting cases involving child pornography search warrants for electronic devices).

In *Brooks*, the government obtained a search warrant for a residence, alleging in the affidavit that a computer located therein was downloading and sharing child pornography via the Internet using a P2P file-sharing software. *Id*. at *3-6. The affidavit recited the tools used by the detective to determine that a computer at the residence to be searched was being used to download and share child pornography. *Id*. Thereafter, the detectives obtained a search warrant for the residence that authorized the seizure and off-site search and analysis of the computer for evidence of child pornography violations. *Id*. Brooks alleged that the warrant was facially invalid because it lacked particularity and was overbroad. *Id*. at *8. The district court determined that the warrant was valid, finding that "[t]he scope of the warrant was restricted to a search for evidence of child pornography-related crimes and did not permit a free-ranging search." *Id*. *11. As to the computer related items that the warrant permitted to be searched and seized, "federal courts applying a reasonableness analysis on a case-by-case basis 'have rejected most particularity challenges to warrants authorizing the seizure and search of entire personal or business computers.'" *Id*. The district court recognized the unique challenges of computer searches, and found that a flexible approach to the search protocol or methodology was best suited to avoid

unduly restricting legitimate search objectives. *Id*. at *12.

In *United States v. Brooks*, 648 Fed.Appx. 791, 793 (11th Cir. 2016), the Eleventh Circuit affirmed the district court's finding, rejecting Brooks' contention that the search warrant was unconstitutionally overbroad. The Eleventh Circuit noted:

> In an introductory paragraph, the search warrant stated that probable cause existed to believe that a computer or other digital device at Brooks' residence was being used knowingly to possess child pornography, in violation of Florida's child pornography statutes. The search warrant then set forth a detailed list of items-to-be-seized, including computer hardware, software, and digital storage devices.
>
> When read within the context of the entire warrant, the descriptions are sufficiently particular to enable officers to "reasonably ascertain and identify the things to be seized" as being *only* those items pertinent to an investigation related to child pornography. Given that child pornography images may be stored anywhere on a computer or digital device, the search warrant in this case was 'as specific as the circumstances and nature of activity under investigation [would] permit.' *Id*.

United States v. Conrad, 2013 WL 4028273, at *3 (M.D. Fla., August 7, 2013), involved a similar situation, where the government submitted an affidavit in support of an application for a search warrant for a home. The affidavit indicated that a computer located in the residence to be searched had downloaded and shared child pornography on the Internet using a P2P file-sharing software. The detectives obtained a warrant to search the residence, which authorized the search of computer media for evidence of child pornography violations. The defendant alleged the warrant was facially invalid because it lacked particularity and was overbroad. The district court rejected the defendant's contention, based on the same findings articulated in *Brooks*, namely, that "[t]he scope of the warrant was restricted to a search

for evidence of child pornography crimes and did not permit a free-ranging search." *Id*. at *6. Further, the district court also found that with regards to electronic evidence, a more flexible standard of reasonableness applies as it pertains to particularity challenges. *Id*. at *8.

Like here, in *United States v. Beckett*, 544 F.Supp. 1346 (S.D. Florida, March 12, 2008), the defendant alleged that a premises search warrant only permitted law enforcement to seize the defendant's computer, not to search the files inside the computer. The district court noted that in identifying the property to be seized, agents are not obligated to interpret a warrant narrowly. *Id*. at 1350. *See United States v. Stiver,* 9 F.3d 298, 302–03 (3d Cir.1993), cert. denied, 510 U.S. 1136, 114 S.Ct. 1115, 127 L.Ed.2d 425 (1994). "Stated differently, the particularity requirement requires the search warrant to describe the property to be seized with reasonable specificity, but not with elaborate detail. *See e.g., United States v. Somers,* 950 F.2d 1279, 1285 (7th Cir.1991), cert. denied, 504 U.S. 917, 112 S.Ct. 1959, 118 L.Ed.2d 561 (1992)." *United States v. Beckett*, 544 F.Supp. at 1350.

The district court further noted that "[w]here a search warrant authorizes seizure of evidence of enumerated crimes, even though the evidence was not otherwise described in the warrant the evidence was properly seized." *United States v. Beckett*, 544 F.Supp. at 1350-51. *See Andresen v. Maryland,* 427 U.S. 463, 480, 96 S.Ct. 2737, 2748, 49 L.Ed.2d 627 (1976). Even similar evidence not specified in a search warrant may be seized if it has a sufficient nexus to the crime under investigation. *United States v. Beckett*, 544 F.Supp. at 1351. *United States v. Davis,* 589 F.2d 904, 906 (5th Cir.), cert.

denied, 441 U.S. 950, 99 S.Ct. 2178, 60 L.Ed.2d 1055 (1979). Likewise, the search of unspecified computer files has been approved, where their functional equivalent was described. *United States v. Beckett*, 544 F.Supp. at 1351.

The *Beckett* court found that the search warrant called for the search and seizure of computers and storage devices, as constituting evidence of enumerated computer crimes. *Id*. The district court also found that the challenged evidence was otherwise described in the warrant, and the affidavit went through the forensic computer examination process utilized during the search. *Id*. As such, the district court determined that any lack of precision in the description of the computer search did not mean that the warrant was defective. *Id*.

The Eleventh Circuit affirmed the district court's ruling in *United States v. Beckett*, 369 Fed.Appx. 52, 56 (11th Cir. 2010), noting:

> '[T]he particularity requirement must be applied with a practical margin of flexibility, depending on the type of property to be seized, and that a description of property will be acceptable if it is as specific as the circumstances and nature of activity under investigation permit.' *United States v. Wuagneux,* 683 F.2d 1343, 1349 (11th Cir.1982). "A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized." *Id.* at 1348. **Furthermore, 'an affidavit incorporated into a warrant by express reference and attached to and accompanying the warrant can cure ambiguity in the warrant itself.'** *United States v. Weinstein,* 762 F.2d 1522, 1531 (11th Cir.1985) (emphasis supplied).

The Eleventh Circuit found that the affidavit attached to the application for a search warrant of the defendant's house and computers adequately described the purpose of the search. *Id*. at 57. The allegations centered on the fact that Beckett had contacted minors through the use of the Internet and a home computer soliciting nude

photographs of the minors. *Id*. The search warrant affidavit explained that the computer and its drives can store numerous pages of information and the pertinent information can be found therein. *Id*. Further, the warrant described with specificity the items to be searched and the objectives of the search. *Id*. Thus, the Court found that the search of the defendant's computer did not exceed the scope of the warrant. *Id*.

Just like in the above-mentioned case, in this case, the warrant authorized the search of the defendant's residence (the PREMISES), to include computer media found therein, for evidence related to child specific child pornography offenses, because SA Kaufman believed that a computer located at the residence was involved in the distribution and possession of child pornography. The term "PREMISES" as explained in the affidavit at paragraph 6, included computer, computer media, or electronic devices located therein, where the items specified in Attachment B may be found.

Attachment B of the search warrant allowed for the seizure of all "records, documents, programs, applications, files or materials created, modified or stored in any form, including by computer hard drives, external hard drives, thumb drives, cell-phones," etc., that may contain evidence of the child pornography offenses specified in the warrant. *See* Exhibit 1, Attachment B. Attachment B was also incorporated by express reference to the search warrant. Therefore, that the warrant authorized the search and seizure of computer media, and the same was not overbroad.

The *Leon* good faith exception applies to claims that a warrant is not sufficiently particularized or overbroad. *United States v. Leon*, 486 U.S. 897 (1984); *United States v. Travers*, 233 F.3d 1327, 1329-30 (11th Cir. 2000). In order for the evidence to be suppressed in spite of the warrant, the defendant must show that it was "so facially deficient - *i.e.*, failing to particularize the place to be searched or the things to be seized - that the executing officers could not have reasonably presumed it to be valid." *Travers*, 233 F.3d at 1330 (citing *United States v. Accardo*, 749 F.2d 1477, 1481 (11th Cir. 1985) (citing *Leon*, 468 U.S. at 923)).

The search warrant in this case was not overbroad because it listed the place to be searched and items to be seized with sufficient particularity. The search was limited to the instrumentalities and evidence of the enumerated offenses:

> As set forth in more detail below, I have probable cause to believe that a crime has taken place, that is, the knowing possession and distribution of child pornography in interstate commerce, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B). Furthermore, I have probable cause to believe that the PREMISES to be searched contains instrumentalities, contraband, and evidence of these crimes, as set forth in Attachment B.
>
> I am requesting authority to search the entire PREMISES—including the curtilage, residential dwelling(s), and any computer, computer media, or electronic storage devices located therein, where the items specified in Attachment B may be found. I also request to seize all items listed in Attachment B as instrumentalities, contraband, and evidence of criminal activity.

See Warden v. Hayden, 387 U.S. 294, 307 (1967) (describing instrumentalities of crime as object of warrant). The scope of the items to be seized was particularly described in Attachment B of the affidavit, with reference to the enumerated offenses. In essence, the items authorized by the Court for search and seizure in the warrant were

each limited to those items (including computer media) providing evidence of enumerated child pornography offenses; evidence indicating attempts to thwart law enforcement detection efforts; and evidence showing possession, ownership, occupancy, or control of the premises and electronic devices. *See* Attachment B to Search Warrant. Regardless, the touchstone for the Court's consideration is the officer's reasonableness, not whether the warrant was itself valid. *Accardo*, 749 F.2d at 1481. In this case, the officers were reasonable in relying on the warrant, which is similar to electronic device warrants authorizing the search for child pornography evidence that have been approved in this district. SA Kaufman relied on the CCIPS approved premises computer search warrant affidavit to obtain a valid and enforceable search warrant.

Further, the items to be searched and seized were narrowly linked to the factual basis for the probable cause finding. Therefore, the search warrant left "nothing … to the discretion of the officer executing the warrant." *Marron*, 275 U.S. at 196. Accordingly, the search warrant for defendant's residence was not overbroad, and the evidence obtained therefrom should not be suppressed.

IV. *The Exclusionary Rule Does Not Apply*

Evidence obtained in violation of an individual's rights under the Fourth Amendment ordinarily must be excluded from the prosecution's case. *United States v. Martin*, 297 F.3d 1308, 1312 (11th Cir. 2002). The exclusionary rule, as it is known, is a judicially created remedy designed to deter future Fourth Amendment violations. *Id.* But the fact that a Fourth Amendment violation occurred does not automatically

mean that the exclusionary rule applies. *Herring v. United States*, 555 U.S. 135, 141 (2009).

The application of the exclusionary rule depends on a cost-benefit analysis that takes into account the deterrent value served by suppression and "the substantial social costs generated by the rule." *Davis v. United States*, 564 U.S. 229, 237 (2011) (internal quotation marks omitted). "For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs." *Id.*

The Fourth Amendment exclusionary rule should not be applied as to bar the use of evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate, but ultimately found to be invalid. *United States v. Leon*, 486 U.S. at 922-23. "'If the purpose of the exclusionary rule is to deter unlawful police conduct, then evidence obtained from a search should be suppressed only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.'" *Id*. at 919.

> This is particularly true, we believe, when an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope. In most such cases, there is no police illegality and thus nothing to deter. It is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment. In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient. "[O]nce the warrant issues, there is literally nothing more the policeman can do in seeking to comply with the law." Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations. *Id*. at 920-921.

Leon, supra, outlined four situations in which suppression would still be appropriate. These situations are (1) "if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth," (2) "where the issuing magistrate wholly abandoned his judicial role," (3) where the "warrant [is] based on an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable,'" and (4) where "a warrant [is] so facially deficient ... that the executing officers cannot reasonably presume it to be valid." *Id*. at 923.

In judging whether the good faith exception to the exclusionary rule applies, the question is whether the police officer's belief in the existence of probable cause underlying a search warrant was objectively reasonable from the viewpoint of a reasonable officer, not a reasonable jurist. *United States v. Taxacher*, 902 F.2d 867, 872-73 (11th Cir. 1990). In *Taxacher, supra*, the Eleventh Circuit considered the fact that the officer had consulted with the District Attorney and facts testified by the officer that were not included in the affidavit in reaching its conclusion, that the officer acted in good faith and that the warrant was not so lacking in indicia of probable cause as to render official belief in the existence of probable cause entirely unreasonable.

Thus, in determining whether an officer acted in good faith when relying upon an invalid warrant the reviewing court may look outside the four corners of the affidavit. *United States v. Martin*, 297 F.3d 1308 (11th Cir. 2002). Furthermore, the government is properly allowed to question an officer in court about the other information that he had in order to show he relied on the warrant in good faith.

In the instant case, SA Kaufman's search warrant affidavit contained sufficient information from which a detached Magistrate Judge inferred that probable cause existed to search the premises for any records, including computer media containing child pornography. SA Kaufman's affidavit was based on a template issued by CCIPS, reviewed by the undersigned Assistant United States Attorney (AUSA), approved by a supervising AUSA, and authorized by a neutral Magistrate Judge. Thus, the search warrant was valid and in executing it, SA Kaufman acted under the good faith belief that he had probable cause to search the target premises. Further, the societal interest at issue here is the protection of vulnerable children in our communities from sexual predators. The deterrent value served by suppression in this case cannot outweigh the substantial social costs generated by the exclusionary rule, because "[c]hild sex crimes are among the most egregious and despicable of societal and criminal offenses." *United States v. Sarras,* 575 F.3d 1191, 1220 (11th Cir. 2009). As such, the exclusionary rule does not apply.

Therefore, the government respectfully requests from the Honorable Court to deny the defendant's motion to suppress evidence. Because the search warrant authorized the seizure and search of computer media and the defendant's motion is clearly frivolous, the United States submits that an evidentiary hearing is unwarranted.

As such, the Court should deny the defendant's request for an evidentiary hearing on this issue.

Respectfully submitted,

MARIA CHAPA LOPEZ
United States Attorney

By: */s/ Ilianys Rivera Miranda*
ILIANYS RIVERA MIRANDA
Assistant United States Attorney
USA No. 150
400 W. Washington Street, Suite 3100
Orlando, Florida 32801
Telephone: (407) 648-7500
Facsimile: (407) 648-7643
E-mail: ilianys.rivera@usdoj.gov

U.S. v. RONALD HILL **Case No. 6:19-cr-1-Orl-40LRH**

CERTIFICATE OF SERVICE

I hereby certify that on June 7, 2019, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to the following:

Joshua R. Lukman
Assistant Federal Defender

/s/ Ilianys Rivera Miranda
ILIANYS RIVERA MIRANDA
Assistant United States Attorney
USA No. 150
400 W. Washington Street, Suite 3100
Orlando, Florida 32801
Telephone: (407) 648-7500
Facsimile: (407) 648-7643
E-mail: ilianys.rivera@usdoj.gov