

No.

IN THE SUPREME COURT OF THE UNITED STATES

---

---

MARK TODD MINOR, PETITIONER,

v.

STATE OF FLORIDA, RESPONDENT.

---

*ON PETITION FOR A WRIT OF CERTIORARI TO  
THE FOURTH DISTRICT COURT OF APPEAL OF FLORIDA*

---

**APPENDIX TO PETITION FOR A WRIT OF CERTIORARI**

---

---

DANIEL EISINGER  
*Public Defender*

Gary Lee Caldwell  
*Assistant Public Defender*  
*Counsel of Record*

Office of the Public Defender  
Fifteenth Judicial Circuit of Florida  
421 Third Street  
West Palm Beach, FL 33401  
(561) 355-7600

gcaldwel@pd15.org  
jcwalsh@pd15.org  
appeals@pd15.org

DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA  
FOURTH DISTRICT

**MARK TODD MINOR,**  
Appellant,

v.

**STATE OF FLORIDA,**  
Appellee.

No. 4D2023-3142

[March 6, 2025]

Appeal from the Circuit Court for the Fifteenth Judicial Circuit, Palm Beach County; Sherri Collins, Judge; L.T. Case No. 502021CF001670AXXX.

Daniel Eisinger, Public Defender, and Gary Lee Caldwell, Assistant Public Defender, West Palm Beach, for appellant.

James Uthmeier, Attorney General, Tallahassee, and Melynda L. Melear, Senior Assistant Attorney General, West Palm Beach, for appellee.

PER CURIAM.

*Affirmed.*

KLINGENSMITH, C.J., FORST and ARTAU, JJ., concur.

\* \* \*

***Not final until disposition of timely filed motion for rehearing.***

IN THE DISTRICT COURT OF APPEAL OF THE STATE OF FLORIDA  
FOURTH DISTRICT, 110 SOUTH TAMARIND AVENUE, WEST PALM BEACH, FL 33401

March 24, 2025

MARK MINOR,  
Appellant(s)  
v.

STATE OF FLORIDA,  
Appellee(s).

**CASE NO. - 4D2023-3142**  
L.T. No. - 502021CF001670AXXX

**BY ORDER OF THE COURT:**

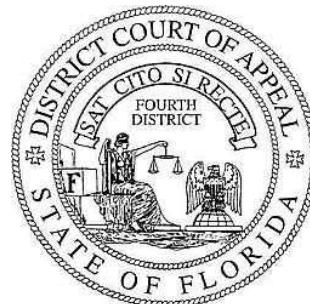
ORDERED that Appellant's March 19, 2025 motion for rehearing, issuance of written opinion and certification is denied.

Served:  
Crim App WPB Attorney General  
Gary Lee Caldwell  
Palm Beach Clerk  
Sherri Collins  
15th Circuit Court Reporting Services  
Mattie S Fore  
Christine C. Geraghty  
Jaclyn Marie Lopez  
Melynda Layne Melear  
Palm Beach Public Defender  
Palm Beach State Attorney

RA

I HEREBY CERTIFY that the foregoing is a true copy of the court's order.

*Lonn Weissblum*  
LONN WEISSBLUM, Clerk  
Fourth District Court of Appeal  
4D2023-3142 March 24, 2025



IN THE CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT,  
IN AND FOR PALM BEACH COUNTY, FLORIDA  
CRIMINAL DIVISION "R"

STATE OF FLORIDA

CASE NO. 2021CF001670AMB

vs.

MARK TODD MINOR,

Defendant.

/

**ORDER DENYING DEFENDANT MARK MINOR'S  
MOTION TO SUPPRESS EVIDENCE AND STATEMENTS**

THIS CAUSE came before the Court by way of the Defendant's Amended Motion to Suppress Search and Statements (DE # 322) filed on November 30, 2022, by Defense Attorney Devin Johnson, Esq., and the State's Response to the Defendant's Motion to Suppress Search and Statements (DE #328) filed on February 27, 2023, by Assistant State Attorney Mathri Thannikkotu, and the Court having reviewed the Defendant's Amended Motion, the State's Response, the pertinent Rule and applicable case law, and considered all the submitted exhibits and the court file, being advised in the premises, the Court finds as follows:

**Factual Findings**

**A. Search Warrant and Execution**

The Court finds that the Defendant is charged with 23 counts of Possess, Control or Intentionally View Sexual Performance by Child while in Possession of 10 or more Images of Child Pornography, in violation of Florida Statutes Sections 827.071(5) (a) and 775.0847, a second degree felonies punishable by a maximum period of incarceration in the Department of Corrections of fifteen (15) years' each.

The State alleges that between September 7, 2020 and February 16, 2021, an investigation revealed that Defendant Minor possessed, controlled or intentionally viewed child pornography. The following facts are contained within the four corners of the affidavit and application for search warrants at issue and therefore are relevant to the legal analysis:

November 2, 2020, Special Investigations Division Detective Brian Pherson received a CyberTip (#79268159) from the National Center for Missing and Exploited Children (“NCMEC”) involving images and videos of child pornography. Detective Pherson is a certified law enforcement officer assigned to the Special Investigations Division (“SID”) since 2018 and investigates, in pertinent part, crimes against children, child deaths, sex crimes, and CyberTips (internet crimes against children). The source of the CyberTip was Facebook, which reported the use of child pornography or suspected child pornography by one of its users.

September 7, 2020, Facebook reported that they discovered that one of their users, Mark Minor, with a verified phone number of (561) 723-2719, email address Mark minor 69@gmail.com, profile URL <http://www.facebook.com/mark.minor.566>, and screen/user name mark.minor.566, date of birth of February 23, 1969, ESP user ID 100002370285337 head uploaded nine images of a parent child pornography to their messenger application in chat room, name, Mark T Minor, to recipient, Mark T Minor, verify the email address mtminor69@yahoo.com, date of birth, February 23, 1969 at 13:23:03 UTC with the Internet protocol (IP) address of 2600:1700:a180:c1c0:b540:a99c:3c65:f0d5.

Facebook also provided the publicly available profile picture for the account and indicated that the same user uploaded seven messages with images in a string of messages, proceeding in following the identified child exploitation images (“CEI”). Facebook provided the images from those seven messages to law enforcement. The profile picture provided by Facebook for the user

depicts, a photo in memory of the 9/11 terrorist attacks, showing the Statue of Liberty, twin towers and the American flag.

Detective Pherson defined the unique hash value that accompanies every file as being similar to the individuality of a person's DNA. He is like in debt to "digital DNA." Detective Pherson reviewed nine files of child pornography. He confirmed, after viewing them, that the files in the entire cyber tipped report, each met the elements of a crime for possession and intentional viewing of child pornography.

The first file is described as "image depicting, a closed, prepubescent, female, conducting oral sex, with her mouth on a naked male's penis. The female subject appears to be approximately 3-5 years of age."

The second image is described as "image depicts, a closed, female prepubescent, kneeling on the floor in front of an unknown subject. There appears to be ejaculate on her face. The female subject appears to be 3-5 years of age."

The third file is described as "image depicts a group of three frames. Each frame shows the same prepubescent female with her breasts and vagina exposed. The first frame depicts a male's penis covering the female subject's vagina. The second frame depicts the male's penis, penetrating the female's anus. The third frame depicts what appears to be ejaculate on the female's vagina. The female subject appears to be approximately 3-5 years of age."

Several additional files are listed with descriptions of images that depict child pornography.

On November 2, 2020, Detective person received a second cyber tip (#79442777) from NCMEC regarding five images of suspected child pornography reported by Facebook. The cyber tip contained the same suspect upload and recipient information related to mark minor as the prior cyber tip, including the same IP address. The date and time of the upload was September 7, 2020,

at 13:22:28 UTC. The tip contains the same verified email, phone numbers and other Facebook user information. The first file was reviewed and is described as one of the prior files.

Detective Pherson reviewed all of the files contained in the cyber tip report and confirmed that they all met the elements of possession, control, and intentional viewing of child pornography.

On November 11, 2020, Detective Pherson served a subpoena upon sprint to obtain subscriber information for the verified phone number at (561) 723-2719 from September 1, 2020 through November 10, 2020. Sprint responded on November 24, 2020 with subpoena results, identifying the subscriber of the phone number as mark minor, account number 345233783 being active and operable since April 25, 2008. The address listed on the account is 3098 Perry Avenue, Greenacres, FL 33463.

On November 24, 2020, Detective person served a subpoena upon Google to obtain basic subscriber information for the email address of markminor69@gmail.com for the same date range. Google responded on December 8, 2020 with results identifying mark minor as the account holder of account ID number 917452264649. Detective person noted that the results showed logins made from the same IP address reported by Facebook for the requested date range.

On November 10, 2020, Detective Pherson served a subpoena upon Oath Holdings, Inc., for subscriber information for the email address of mtminor69@yahoo.com for the same date range. Oath Holdings, Inc. responded that the subscriber was identified as Mark Minor with the verified phone number of (561) 723-2719.

Detective Pherson conducted surveillance on a green Ford F Dash 250 truck in front of the listed address, utilizing the Florida driver, vehicle information database (DAVID). The license plate and vehicle were registered to Mark Minor by Florida's DHSMV. There was also a boat at the address with a VIN number registered in DAVID to Mark Minor.

Detective Pherson also confirmed through DAVID the current address for Mark Minor of 3098 Perry Avenue, Greenacres, FL 33463. Detective Pherson asked the reviewing magistrate to find probable cause existed to believe that the Premises (3098 Perry Avenue, Greenacres, Florida) were being used to store or possess images, movies or visual depictions of sexual conduct or sexual performance by a child or children, in violation of Florida Statutes section 827.071(5).

On February 16, 2021, based on the foregoing, a residential search warrant was issued for the premises located at 3098 Perry Avenue, Greenacres, Florida 33463.

At the hearing, Detective Pherson testified that he personally confirmed the Perry Avenue address 2-3 times. He observed Defendant Minor outside the residence on numerous occasions feeding the cats and taking out the garbage. He stated that there was no other person under suspicion nor any other address. Detective Pherson testified that he made a mistake in the search warrant from editing a prior residential warrant (cutting and pasting error). He correctly stated the address in the affidavit and application, but misstated it in the search warrant in the property description on page two. He listed the correct address on the first page. He also testified that the Cybercrimes Unit, SWAT Team, Digital Forensics Team all were present for the Operations Plan briefing just prior to the execution of the search warrant. He states that all law enforcement personnel knew the correct Perry Avenue address. Further, the team members had a physical copy of the search warrant and affidavit as well as both aerial and street view maps of the correct property. Law enforcement personnel did not go to the wrong address. The search warrant stated the correct address and the photograph depicting the target address was of the correct address.

## **B. Defendant's Statement to Law Enforcement**

Defendant seeks to suppress statements he made on February 16, 2021, to Palm Beach County Sheriff's Office detectives while seated in the detective's vehicle in front of Minor's home, arguing that those statements were obtained as the result of implied promises of leniency. In violation of his Fifth Amendment rights and in violation of Article I, section 9 of the Florida Constitution.

Defendant Minor and his wife were both home during the execution of the search warrant. Detective Pherson testified that he interviewed Defendant Minor in Detective Grimaldi's vehicle with her present. Detective Pherson read Minor *Miranda* rights, which Minor waived. Detective Pherson asked Defendant Minor after each individual right if he understood to which Minor said yes. Defendant Minor signed the *Miranda* rights card. Detective Pherson confirmed that Defendant Minor was not taking any medication and was not cold. Detective Pherson neither promised to let Defendant Minor go if he confessed, nor did he promise to ask the prosecutor for leniency if Defendant Minor confessed. The interview began at 6:22 a.m. and continued for roughly 36 minutes. Defendant Minor was either handcuffed in front or not handcuffed during the interview. The conversation was relaxed and not threatening. When Detective Pherson confronted Defendant Minor with the individual images, he did not change his tone. He asked Defendant Minor to be honest and tell him if Minor had some underlying issues for which Minor could get help.

## **ANALYSIS**

### **A. Search Warrant and Execution**

The United States Supreme Court held in *Franks v. Delaware*, 438 U.S. 154 (1978) that challengers to probable cause affidavits based on ***misstatements*** have the burden to show that (1) the misstatement was material to the question of probable cause and (2) there was a requisite level

of intent of police to deceive. *Johnson v. State*, 660 So. 2d 648, 655 (Fla. 1995) citing *Franks*, 438 U.S. at 171-72. The analysis outlined in *Franks* dealt solely with misstatements rather than **omissions** to a probable cause affidavit. The Florida Supreme Court articulated in *Johnson*, that,

“. . . misstatements are fundamentally a different problem than omissions. Some omissions may be ‘intentional’ but also reasonable in the sense that they exclude material police in good faith believes to be marginal, extraneous or cumulative. Moreover, some omitted information is simply overlooked in the exigencies of the moment without the intent to deceive or recklessness with respect to the truth.”

*Id.* at 656. The Florida Supreme Court in *Johnson* cited to *United States v. Coakley*, 899 F.2d 297 (4<sup>th</sup> Cir. 1990) as the authority on challenges based on omissions. *Id.* Omissions are different than misstatements in that they must do more than “affect the outcome” of the probable cause determination. *Coakley*, 899 F.2d at 301. To be material under a *Franks* analysis, an omission must be such that the inclusion of the information in the affidavit would defeat probable cause all together. *Id.* See *United States v. Reivich*, 793 F.2d 957 (8<sup>th</sup> Cir. 1986). In determining whether the affidavit with the omitted information would be supported by probable cause, the Court must look to the **totality of the circumstances** test articulated in *Illinois v. Gates*, 462 U.S. 213 (Fla. 1983). *Id.* at 302. This requires a commonsense decision whether all the circumstances set forth in the affidavit establish probable cause that the suspect committed the crime. *Id.*

After a thorough review of the “four corners” of the search warrant, the purpose of the description of the property to ensure that law enforcement empowered to effectuate the search warrant actually entered the correct location, unanimous understanding of the search warrant execution team that the property at issue was 3098 Perry Avenue in Greenacres, Florida, and the proper execution at that address, the Court finds no deliberate falsity or reckless disregard for the truth in the search warrant affidavit.

The Fourth Amendment of the United States Constitution and Article I, Section 12 of the Florida Constitution require a warrant to “particularly describe the place or places to be searched. Historically, the purpose of this requirement was to prevent the use of general warrants and wide-ranging exploratory searches.” *Bennett v. State*, 150 So. 3d 842, 844 (Fla. 4th DCA 2014) (citing *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)). *See also State v. Leveque*, 530 So. 2d 512, 513 (Fla. 4th DCA 1988). The incorrect address and description on page two of the search warrant in the premises description was not sufficient to invalidate the warrant. “Independent knowledge of the premises by an officer executing a search warrant, where that knowledge was obtained from prior surveillance of the premises, may be considered in assessing whether the warrant’s description of the premises is sufficiently particular.” *Bennett*, at 846. *See State v. Houser*, 364 So. 2d 823, 824 (Fla. 2d DCA 1978) (citing *State v. Gallo*, 279 So. 2d 71 (Fla. 2d DCA 1973)) in which the address was incorrect however, the District Court held “that this mistake did not render the search warrant invalid. The description of the residence was sufficient to lead and indeed did lead the officers directly to the house to be searched.”)) Further, “[a] residence may be described with reference to its occupants, *see State v. Gallo*, 279 So. 2d 71 (Fla. 2d DCA 1973); *see also, United States v. Hassell*, 427 F.2d 348 (6th Cir. 1970), and a prior or continuing surveillance of the premises may be considered in connection with the warrant description of the place to be searched.” *Carr v. State*, 529 So. 2d 805, 806 (Fla. 1st DCA 1988). “An inaccuracy in the warrant, such as an incorrect address or apartment number, does not invalidate the warrant if the place to be searched is otherwise sufficiently identified in the warrant.” Id.

#### **B. Defendant’s Statement to Law Enforcement**

For reasons discussed below, the Court finds that Defendant’s statement to law enforcement was not obtained as the result of impermissible tactics to obtain a confession, namely,

detectives did not promise Defendant Minor anything to induce him to make a statement. There was no violation of Daniels' constitutional rights. "The test of voluntariness of a confession is whether, examining the totality of the circumstances, the confession was the product of coercive police conduct." *Green v. State*, 878 So. 2d 382, 383 (Fla. Dist. Ct. App. 2003) (citing *Colorado v. Connelly*, 479 U.S. 157 (1986)). "[I]n judging whether a confession should be suppressed as involuntary, promises to bring a defendant's cooperation to the attention of the judge and prosecutor are not per se objectionable, accurately representing the defendant's situation is not coercive, urging a defendant to tell the truth is not objectionable, and engaging in a discussion with the defendant about the realistic penalties that may be imposed after cooperation or non-cooperation is not coercive." *Id.*

The Court in assessing the totality of the circumstances considers the defendant's ability to overcome pressure brought against him and courts examine such factors as "youth, lack of education, low intelligence, explanation of constitutional rights and length of interrogation ...," *State v. Moore*, 530 So. 2d 349 (Fla. 2d DCA 1988). Defendant Daniels was fifty-three years old at the time of the interview. There was no evidence presented to suggest that he has low intelligence, on the contrary, his speech suggests otherwise. Detective Pherson read *Miranda* warnings to Defendant Minor. Minor signed the *Miranda* form. The interrogation was roughly 36 minutes long. The atmosphere in the interview was relaxed, informal, cordial and non-adversarial. The detectives never raised their voices. There was no deception or aggression by law enforcement. Instead, multiple time during the interview detectives told Minor that he should tell the truth. They encouraged him to tell the truth. Detective Pherson told Minor about the physical evidence they had in their possession and that those items were being examined for evidence of child pornography, and that deleted files could be recovered. The detectives presented these facts and

the images to Minor calmly and without hostility. The comments here never rose to the level of an express *quid pro quo* bargain in return for Defendant's statement. In giving answers, Minor's voice sounded calm and deliberate. He also seemed rational and his answers were responsive to the detectives' questions and consistent with his story that he didn't remember downloading or transferring images of child pornography, or by implication, that he hadn't done it since the first time. In this setting and with these facts, detectives did not mislead, promise or imply that Minor would not be arrested or prosecuted if he cooperated by providing an explanation or statement.

It is hereby **ORDERED AND ADJUDGED** that the Defendant's Amended Motion to Suppress Search and Statements is **DENIED**.

**DONE AND ORDERED** at West Palm Beach, Palm Beach County, Florida.



502021CF001670AXXXMB 05/18/2023  
Caroline C. Shepherd Circuit Judge  
ADMINISTRATIVE OFFICE OF THE COURT

502021CF001670AXXXMB 05/18/2023  
Caroline C. Shepherd  
Circuit Judge

copies furnished to:

Mathri Thannikotu, Assistant State Attorney, 401 N. Dixie Highway, FL 33401,  
[mthannikotu@sa15.org](mailto:mthannikotu@sa15.org)

Mattie Fore, Esq., Defense Counsel, 631 Lucerne Avenue, Lake Worth Beach, FL 33460,  
[mattie@mattieforelaw.com](mailto:mattie@mattieforelaw.com)

IN THE CIRCUIT/COUNTY COURT  
OF THE 15TH JUDICIAL CIRCUIT  
IN AND FOR PALM BEACH COUNTY, FLORIDA

AFFIDAVIT AND APPLICATION FOR SEARCH WARRANT

THE STATE OF FLORIDA  
COUNTY OF PALM BEACH

COMES NOW, Affiant, a Detective, Brian Pherson with the Palm Beach County Sheriff's Office in and for Palm Beach County, Florida, herein after referred to as "Affiant," being first duly sworn, deposes and says that they have probable cause to believe that a certain premises located in Palm Beach County, Florida, described as:

3098 Perry Ave. Greenacres, FL 33463



To reach the premises desired to be searched, start at Palm Beach County Sheriff's Office District 16 substation located at 2995 Jog Road, Greenacres, FL 33467. Travel south on Jog Road for 0.1 miles and then turn left (east) onto 10<sup>th</sup> Ave N. Travel approximately 1.2 miles then

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

turn left (north) onto Perry Ave. Travel 340 ft. and the residence will be located on the east side of the street. The building is light green in color with a gray shingle roof. The front door is white and the numerical "3098" is posted in white lettering affixed to the concrete facing the driveway. There is an open concrete paved driveway and a sidewalk adjacent to the residence. Beyond the sidewalk near the roadway is a standalone mailbox in front of the residence. The numeric "3098" is affixed in black lettering with white background onto a black mailbox. This is a complete description of the premises desired to be searched.

Being the premises of, or occupied by, or under the control of **The Minor Family**, as verified through Intelligence gathered from various Law Enforcement Database(s), Sprint, DAVID, Florida's DHSMV, and your Affiant's Surveillance.

And there is now being kept, in the above described premises, certain property contained therein that has been used to commit any crime, or constitutes evidence relevant to proving that a crime has been committed, to wit:

1. Images, movies, or visual depictions of sexual conduct or sexual performance by a child or children, in violation of Florida Statute 827.071.
2. All data, content, files, and information contained on any electronic devices, storage devices, software, or hardware.
3. Any and all digital device(s) and all data, content, files, and information contained on them; including but not limited to any device capable of capturing and/or storing digital data, sub-compact computers, cell phones, and "smart" cell phones, desktop computers, laptop computers, cameras, personal assistants, iPods, portable media players, tablet computers like iPad, gaming consoles, video cameras, DVRs (digital video records), web cams or other video capture devices, modems, routers, firewalls, wireless access points, printers, cellular telephones, GPS navigation devices, etc.
4. Digital device hardware and all data, files, content, and information contained in them, including but not limited to, any and all digital device equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar digital device impulses or data. Hardware includes (but is not limited to) any data processing devices (such as such as central processing units, personal computers to include "laptop" or "notebook" or "pocket" computers or mobile "smart" phones); internal and peripheral storage devices (such as Universal Serial Bus ("USB") memory sticks or thumb drives, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

5. Digital device input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing digital device storage media.
6. Digital device storage media and the digital content to include but not limited to USB memory sticks or flash or thumb drives, floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography. Additionally, any digital data storage media ("media"), solid state drives (SSD's), hard disk drives (HDD's), Blu-Ray discs, flash media, Secure Digital (SD) cards, Micro Secure Digital (Micro SD) cards, backup drives.
7. Digital device software and application software installation and operation media.
8. Digital device software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.
9. Manuals and other documents (whether digital or written) that describe operation of items or software seized.
10. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.
11. Within the digital device(s): data maintained on the device; in particular, text messages, chats, data in the form of images, videos, and/or log files recording the transmission of files as they relate to violations of Florida law cited herein related to the possession, transmission or sexual conduct of minors.
12. Within the digital device(s): all relevant contents and data, including but not limited to, Subscriber and equipment identifiers, Date/time, language and other settings, contact information, appointment calendar information, dialed, incoming, and missed call logs, electronic mail, photos, audio and video recordings, multi-media messages, instant messaging and web browsing activities, electronic documents, location information, SMS and MMS messages, Any messages
13. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the exploitation of children. Correspondence or other documents (whether digital or written) exhibiting an interest in the exploitation of children.
14. Items that would tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain child pornography including but

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

not limited to receipts, credit card bills, telephone bills, correspondence and other identification documents.

15. Items that would tend to show dominion, control and ownership of the premises and property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

16. Data maintained on the digital devices, or digital device related storage devices such as USB memory sticks or thumb drives/flash drives, floppy diskettes, tape backups, computer printouts, and "zip" drive diskettes. In particular, data in the form of images, and/or log files recording the transmission of images as they relate to violations of Florida law cited herein related to the possession and/or distribution of child pornography.

17. Preservation of data maintained in any online remote storage devices/programs that are linked to the digital device or digital device related storage device through folders or internet access.

All of which items detailed in 1-17 above are hereinafter referred to as "The Property" that constitutes evidence relevant to proving that a felony has been committed, to wit:

**F.S.S. 827.071(5) Possession of Child Pornography**

and that the grounds for issuance are, to wit:

**F.S.S. 933.18(6): (Dwelling)**

- A weapon, instrumentality, or means by which a felony has been committed is contained therein.
- Evidence relevant to proving a felony has been committed is contained therein.

The facts establishing Affiant's basis for probable cause that the aforementioned violations of Florida law are being committed in, or on, the afore described premises, and that the afore described property is located in or on the above described premises are as follows:

Your Affiant, Detective Brian Pherson, is a duly appointed Deputy Sheriff for Palm Beach County, and has all the powers of a law enforcement officer in and for Palm Beach County, Florida. Your Affiant has been employed with the Palm Beach County Sheriff's Office continuously since October 27, 2011. Your Affiant is currently registered with and certified by the Florida Department of Law Enforcement, Criminal Justice Standards and Training Commission. Your Affiant is a graduate of Florida State University with a Bachelor of Science degree in Criminology. Your Affiant has been assigned to the Special Investigation Divisions (SID) since October 27, 2018. These investigations include but are not limited to: Crimes against Children such as Child Abuse, Child Neglect, Child Death and Homicides, Sex Crimes, Crimes against the Elderly and Missing Persons, Cybertip

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

**Investigations (Internet Crimes Against Children).** Your Affiant has completed numerous hours of training related to law enforcement including the investigation of sexual type crimes, crimes against children, physical abuse, investigation interviews, and the collection and preservation of evidence. Your Affiant is also currently a member of the South Florida Internet Crimes Against Children Task Force.

As a result of your Affiant's training and experience as set forth above, your Affiant has probable cause to believe the following:

1. On November 2<sup>nd</sup> 2020, Your Affiant was assigned to further investigate Cyber Tip report number 79268159 from the National Center of Missing and Exploited Children (NCMEC) concerning images and videos of child pornography. The Cyber Tip was forwarded from the Broward County Sheriff's Office Internet Crimes Against Children (ICAC) Task Force.
2. Cyber tips are investigative leads generated by NCMEC. NCMEC is a non-profit organization that provides services nationwide for families and professionals in the prevention of abducted, endangered, and sexually exploited children. Pursuant to its mission and its congressional authorization (34 USC 11293) NCMEC operates the Cyber Tip line and Child Victim Identification Programs to assist law enforcement in identifying victims of child pornography and child sexual exploitation. NCMEC works with law enforcement, Internet Service Providers, electronic payment service providers, and others to reduce the distribution of child sexual exploitation images and videos over the Internet. NCMEC forwards reports of child sexual exploitation to law enforcement for the purposes of investigation and disposition.
3. The source of the cyber tip comes from Facebook reporting the upload of child pornography by one of their users to NCMEC. Your Affiant knows from training and experience that Facebook refers to an online social media and social networking service company. Registered users must be 13 years of age or older. Facebook can be accessed from any device with internet connectivity such as computers, tablets and smartphones. Users create customized profiles revealing information about themselves. Users can post messages, photos or multimedia and share it with others. Various embedded applications such as Messenger and Marketplace can be used with Facebook. Users can also join common interest groups which may require Facebook login.
4. Facebook reported that on September 7th, 2020 they discovered that one of their users, Mark Minor, verified phone number +15617232719, verified email address markminor69@gmail.com, profile URL <http://www.facebook.com/mark.minor.566>, screen/user name mark.minor.566, DOB 02/23/1969, ESP user ID 100002370285337 had uploaded 9 images of apparent child pornography to their Messenger application, in Chat Room name Mark T Minor, to recipient Mark T Minor, verified email address mtminor69@yahoo.com, DOB 2-23-1969, on September 7<sup>th</sup>, 2020 at 13:23:03 UTC, with the internet protocol (IP) address of 2600:1700:a180:c1e0:b540:a99c:3c65:f0d5.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

5. Your Affiant knows from training and experience that people possessing or transmitting child pornography will send files to other accounts they control on the internet as a means to store the files online and also to make sure that if one account gets flagged and taken down they will have access to the files through another source.

6. To "verify" account information, an Electronic Service Provider (ESP), like Facebook, will send a verification method such as a link or a code to the user provided contact information, such as the email address, to ensure accurate contact information has been entered by the user. The ESP will also send a code or link to the email address to verify actions like changes in security settings, account preferences, billing information, log in from new devices, etc. The user needs to enter the verification code or click the link when prompted to confirm the account or changes. This ensures that the user/subscriber information verified is accurate.

7. In addition to providing the user's publicly available profile picture, Facebook also reported that the same user uploaded seven messages with images in a string of messages preceding and following the identified child exploitation images ("CEI"). Facebook provided those images to NCMEC as well. NCMEC reported that those files had NCMEC and ESP identifier numbers.

8. The profile picture provided by Facebook for the user is a picture commemorating the 9/11 terrorist attacks, and shows the Statue of Liberty, the twin towers, and the American flag as well as a city scape.

9. Many Electronic Service Providers, such as Facebook, created a categorization system for reporting child pornography to NCMEC. This system is displayed in the following chart, which can be included in the Cyber tip.

Content Ranking		1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lewd Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office Agency Case No.: 20-250140	Warrant No.: PBSO_2021_000448 Reviewing Prosecutor: Eric Baum
---	--

001112

10. This chart is primarily used when the provider detects child pornography by an automated system, like Microsoft's PhotoDNA, to confirm known child pornography. In such a case, the system keeps a database of hash values that correspond to images previously identified as child pornography by the criteria listed in the chart above.

11.. In the same way that the characteristics of every person's DNA are different, the signature or "hash value" for every file is different, enabling the creation of a hash value that can identify a file based on its unique characteristics or its "digital DNA." Although a photo's hash cannot be used to re-create an image or identify people or items within an image, it can be compared with hashes of other files as a reliable way to match two different copies of the same image. When the automated system detects such a hash value, it automatically forwards the information to NCMEC. For example, if the image is classified as A1, it means that an employee of that provider has previously viewed the image and rendered an opinion that the image involved a sex act involving a prepubescent minor.

12.. With respect to the portion of this CyberTip containing the heading: "Was File Reviewed by Company?", when Facebook responds "Yes" it means the contents of the file reported were viewed by a person concurrently to or immediately preceding the sending of the CyberTip.

13. Based on information Facebook provides in the Cybertip and your Affiant's training and experience, when Facebook responds "No", or does not advise NCMEC if they viewed the contents, it means that while the contents of the file were not reviewed concurrently to making the report, historically a person, one of their employees, or law enforcement has reviewed the file whose hash (or digital fingerprint) matched the hash of the reported file and determined it contained apparent child pornography. Facebook may also provide a categorization (e.g. A1, A2, B1, B2) for the file.

14. Facebook and NCMEC reported 9 files of child pornography. Your Affiant viewed the files upon downloading the entire Cybertip report and confirmed they all met the elements of a crime for the possession and intentional viewing or sexual conduct of a child pursuant to Florida Statute 827.071. A description of some of the reported files are as follows:

**Filename:**  
BHWPCrovHeHOHHzd118953246\_790053731534992\_65500699886022  
22811\_o.jpg

**MD5:** 7a2c9c1154e072bb0254b26a176767c3

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001113

**Image Categorization by ESP: A1**

**Original Binary Hash of File (pdna):**  
2401200169028d092d10b3450b2e9c24093967011606180180033d00455  
a313d307f0af2b00d0bb02b3d4f10052e42005b1b692316da2d5917701e4  
dda052164a02521530a46192648221f6942b083261690861bea09732171  
72573c4b2c32374a2140373564288312a82e48c808344960291f7029123e  
2302373641084c2ba81a402e733c0626803c05028a4f000786

- Image depicting a clothed prepubescent female conducting oral sex, with her mouth on a naked male's penis. The female subject appears to be approximately 3 – 5 years of age.

**Filename:**  
eqcfkQbzrPpddLTN118919188\_601828467179833\_27689896946812563  
85\_n.jpg

**MD5:** 480229ab7a77089f2ce3b1b14a7de05e

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Original Binary Hash of File (pdna):**  
42015000512b610f124312693040234c03ff550b0025040e4c04312433be2  
b6629aa25eab12823be38ff5d240150230a601f296044d244591992ac27bc  
22953f2dff2b680178171d18550569602f0fa01f5e3b482f49267b04db0c74  
0328190b144a5f12242b22370f4b0a700d3e0969044e16300b163b024e45  
58210385640400331c0901232a04161b4b03401f6e02

- Image depicts a clothed female prepubescent kneeling on the floor in front of an unknown subject.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

There appears to be ejaculate on her face. The female subject appears to be 3 – 5 years of age.

- Your Affiant knows from training and experience that when NCMEC advises, as in this cybertip, that there was a hash value match for this file, and it is classified as apparent child pornography, it means that an employee of NCMEC, the ESP, or a law enforcement agency, (all of whom have a statutory duty to report child abuse) previously had an employee or officer open the file and confirm that this exact same file was apparent child pornography.

**Filename:**  
tDqm9HNeChTybG6k118953246\_790053731534992\_655006998860222  
2811\_o.jpg

**MD5:** 7a2c9c1154e072bb0254b26a176767c3

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent two messages before Child Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 790053724868326

Relation to CEI: Sent two messages before the CEI was uploaded

CEI's NCMEC ID: 8eba91606f1109416143be1e49427359

- Your Affiant viewed this file and it is the same image depicted in filename  
“BHwPCRovHeHOHHzd118953246\_790053731534992\_6550069988602222811\_o.jpg”.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor: Eric Baum

001115

**Filename:**  
1JtWLy5InO5KA6yK118949765\_1254488434895564\_764207251014952  
2485\_o.jpg

**MD5:** eb19193de90d4d2a9fccf6ad5456bfde

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent three messages before Child Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 1254488431562231

Relation to CEI: Sent three messages before the CEI was uploaded

CEI's NCMEC ID: 8eba91606f1109416143be1e49427359

- Image depicts a group of three frames. Each frame shows the same prepubescent female with her breasts and vagina exposed. The first frame depicts a male's penis covering the female subject's vagina. The second frame depicts the male's penis penetrating the female's anus. The third frame depicts what appears to be ejaculate on the female's vagina. The female subject appears to be approximately 3-5 years of age.

**Filename:**  
Ed6HLNj5kxnKJF19118919188\_601828467179833\_2768989694681256  
385\_n.jpg

**MD5:** 480229ab7a77089f2ce3b1b14a7de05e

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001116

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent two messages after Child Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 601828463846500

Relation to CEI: Sent two messages after the CEI was uploaded

CEI's NCMEC ID: 95336d3861f799d3795d519cf34e65ec

- Your Affiant viewed this file and it is the same image depicted in filename  
"eqcfkQbzrPpddLTN118919188\_601828467179833\_2768989 694681256385\_n.jpg".

**Filename:**

UV33pmJtymNUtpEV118928038\_348179093216552\_509294293187979 4432\_o.jpg

**MD5:** 2b324f6731c8808f93312323ed82bc48

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent immediately before Child

Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 348179086549886

Relation to CEI: Sent immediately before the CEI was uploaded

CEI's NCMEC ID: 8eba91606f1109416143be1e49427359

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001117

- Image depicts a prepubescent female engaged in oral copulation with a male's penis. The female subject appears to be approximately 5-7 years of age.

**Filename:**

OnUGOQgkXM5uluqo118894192\_1067822087055534\_84385312408092

11016\_o.jpg

**MD5:** 77e09644a5fc70dc1633cd96ecc07a26

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent two messages before Child Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 1067822080388868

Relation to CEI: Sent two messages before the CEI was uploaded

CEI's NCMEC ID: 95336d3861f799d3795d519cf34e65ec

- Image depicts a prepubescent female with what appears to be ejaculate on her face. There is an adult female subject licking the prepubescent female's face. The prepubescent's female appears to be approximately 6 – 9 years of age.

**Filename:**

64bMhEhyW9xsysuz118928038\_348179093216552\_5092942931879794

432\_o.jpg

**MD5:** 2b324f6731c8808f93312323ed82bc48

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office Agency Case No.: 20-250140	Warrant No.: PBSO_2021_000448 Reviewing Prosecutor:Eric Baum
---	---

001118

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent immediately after Child Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 348179086549886

Relation to CEI: Sent immediately after the CEI was uploaded

CEI's NCMEC ID: 95336d3861f799d3795d519cf34e65ec

- Your Affiant viewed this file and it is the same image depicted in filename  
"UV33pmJtymNUtpEV118928038\_348179093216552\_5092942931879794432\_o.jpg".

**Filename:**

RUbdk1ogv8L16nXY118949765\_1254488434895564\_764207251014952

2485\_o.jpg

**MD5:** eb19193de90d4d2a9fccf6ad5456bfde

**Did Reporting ESP view entire contents of uploaded file? (Information Not Provided by Company)**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Additional Information:** This image was uploaded because it was sent immediately before Child Exploitation Imagery (CEI):

Uploaded by: 100002370285337

Image's unique ESP identifier: 1254488431562231

Relation to CEI: Sent immediately before the CEI was uploaded

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001119

CEI's NCMEC ID: 95336d3861f799d3795d519cf34e65ec

- Your Affiant viewed this file and it is the same image  
depicted in filename  
“1JtWLy5lnOSKA6yK118949765\_1254488434895564\_7642072510149522485\_o.jpg”

15. Also on November 2<sup>nd</sup>, 2020, your Affiant was also assigned to further investigate a related Cybertip report number 79442777 from NCMEC concerning five images of child pornography reported by Facebook. NCMEC and ESP also provided the profile picture for this account which matches picture from the related cybertip. This Cybertip contained the same suspect upload and recipient information pertaining to Mark Minor as in Cybertip 79268159, including the upload IP address, 2600:1700:a180:c1c0:b540:a99c:3c65:f0d5, with date and time of upload with date 9/7/20 13:22:28 UTC, as well as the verified email and phone numbers, and the other Facebook user information.

16. Facebook, through NCMEC reported the following file of CEI was uploaded by the suspect user described above

**Filename:**  
04jS75e1XYa7Wyy118949765\_1254488434895564\_7642072510149522485\_o.jpg

**MD5:** eb19193de90d4d2a9fccf6ad5456bfde

**Did Reporting ESP view entire contents of uploaded file? Yes**

**Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)**

**Source Information:**

**Were entire contents of uploaded file publicly available? (Information Not Provided by Company)**

**Original Binary Hash of File (pdna):**

372a3e22205b53116d4f3d1f31a83614be25523832443c23673e3c587937  
5e1f46948c2752b77b1eaa727360634835685d8951109c46193b60992234  
52755d1f35644e163068362b44663c245b8c145db14a43723586273c4d68  
29220f770c362255143e4470592170333d5f536c2a479498401a086f300c1

**Source information**

**Type Value Event Date/Time**

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001120

IP Address 2600:1700:a180:c1c0:b540:a99c:3c65:f0d5 Upload 09-07-2020 13:22:28  
UTC

- Image depicts a group of three frames. Each frame shows the same prepubescent female with her breasts and vagina exposed. The first frame depicts a male's penis covering the female subject's vagina. The second frame depicts the male's penis penetrating the female's anus. The third frame depicts what appears to be ejaculate on the female's vagina. The female subject appears to be approximately 3-5 years of age.

1. Much like Cybertip 79268159, in this Cybertip, Facebook flagged and provided the files that the suspect user uploaded and transmitted before and after the CEI. They are identified as having NCMEC and ESP identifier ID's. There were 4 such files. Those files appear to be files which depict the same CEI contents as the files in the first Cybertip.
2. Your Affiant viewed the files upon downloading the entire Cybertip report and confirmed they all met the elements of a crime for the possession and intentional viewing or sexual conduct of a child pursuant to Florida Statute 827.071.
3. On November 11<sup>th</sup>, 2020, a subpoena was served to Sprint to obtain basic subscriber information for the verified phone number of 561-723-2719 for the date range of September 1<sup>st</sup>, 2020 through November 10<sup>th</sup>, 2020.
4. On November 24<sup>th</sup>, 2020, Sprint returned the subpoena results identifying the subscriber of aforementioned phone number to be Mark Minor. Sprint account #345233783 is active and opened on April 25<sup>th</sup>, 2008. The address listed on the account is 3098 Perry Ave. Greenacres FL 33463.
5. On November 24<sup>th</sup>, 2020, a subpoena was served to Google to obtain basic subscriber information for the email address of markminor69@gmail.com for the date range of September 1<sup>st</sup>, 2020 through November 10<sup>th</sup>, 2020.
6. On December 8<sup>th</sup>, 2020, Google returned the subpoena results identifying the subscriber of the aforementioned email address to be Mark Minor with account ID #917452264649. The results also show logins made from IP address 2600:1700:a180:c1c0:b540:a99c:3c65:f0d5 matching the upload IP address reported by Facebook for the requested date range.
7. Your Affiant used the Internet Protocol address (also known as an IP address) provided by the reporting company to track the source of the child pornography. An IP address is a set of numbers which identify an electronic device on the Internet. IP addresses follow the format of ###.###.###.###, wherein each of the numbers are between

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

0 and 255<sup>1</sup>, or #####:#####:#####:#####:#####:#####.#####, wherein each digit is between 0 and 'f' in hexadecimal form<sup>2</sup>. Computers use IP addresses to identify each other on the Internet. Internet Protocol addresses, both V4 and V6, are registered to specific individuals, or entities such as an Internet service provider.

<sup>1</sup>As specified in the protocol TCP/IP v4 which is a common, but legacy usage today.

<sup>2</sup>As specified in the protocol TCP/IP v6, which is slowly becoming standard usage.

8. When a subscriber of an Internet service provider wishes to access the Internet via their service, the Internet service provider will assign that account an IP address which identifies that account holder on the Internet. By providing the Internet service provider with the dates, times and IP addresses which a suspect used to access the Internet, the Internet service provider is able to provide the identifying information for the account holder who was assigned that specific IP address at that date/time, if the records still exist on their system.

9. On November 10<sup>th</sup>, 2020 a subpoena was served to Oath Holdings Inc. to obtain basic subscriber information for the email address of mtminor69@yahoo.com for the date range of September 7<sup>th</sup>, 2020 through November 10<sup>th</sup>, 2020.

10. On November 11<sup>th</sup>, 2020 Oath Holdings Inc returned the subpoena results identifying the subscriber of the aforementioned email address to be Mark Minor, with the verified phone number of 561-723-2719.

11. Additionally, your Affiant conducted surveillance and observed a green Ford F-250 vehicle in front of the residence which utilizing Florida's Driver Vehicle and Information Database (DAVID), the license plate was registered to Mark Minor, that vehicle was also registered to Mark Minor in Florida's Department of Highway Safety and Motor Vehicles.

12. Your Affiant also observed a boat, and the VIN number of the boat is registered in DAVID to Mark Minor.

13. Additionally, through DAVID your Affiant confirmed that the address of 3098 Perry Ave. in Greenacres, FL, 33463 to be current for the Minor family including Mark Minor.

14. The above information leads your Affiant to believe and to have probable cause to believe that the Premises and the curtilage thereof are being used for the purpose of storing or possessing images, movies, or visual depictions of sexual conduct or sexual performance by a child or children, in violation of section 827.071(5) Florida Statutes.

#### SPECIFICS OF THE FACEBOOK SOCIAL MEDIA NETWORK

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

1. Your Affiant knows that Facebook.com is a social networking site that allows individuals on the Internet to communicate with one another. The Facebook.com website specifically describes itself with the following language located on their website:

*Mission: Founded in 2004, Facebook's mission is to give people the power to share and make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them.*

2. After registering to use the site, users can create a user profile, add other users as "friends", exchange messages, post status updates and photos, share videos and receive notifications when others update their profiles. Additionally, users may join common-interest user groups, organized by workplace, school or college, or other characteristics, and categorize their friends into lists such as "People From Work" or "Close Friends" or describe relationships that include "Married", "In Relationship", and "widowed".

3. Through training and experience, I know that Facebook allows its users to access their accounts through various means. This includes directly through their website ([www.Facebook.com](http://www.Facebook.com)) using a web browser as well as their mobile application that can be used through laptops and Android or iOS-based systems. I also know – through training and experience – that Facebook allows their users to use their social media site to send text, video, and audio clips through their other mobile application called "*Facebook Messenger*". This application is supported by Facebook, Inc. and utilizes the user's account profile for monitoring and tracking purposes. In addition to sending clips and messages, this application will also allow the user to conduct voice calls between other Facebook users or cellular phone numbers utilizing 'voice over internet protocol' (VOIP) technology and even video calls. This is content that is separate from cellular phone data and is maintained by Facebook, Inc.

4. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

5. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

6. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by any user that have that user tagged in them.

7. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

8. Facebook also retains Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

#### **SPECIFICS OF DIGITAL DEVICES**

1. Your Affiant requests permission to search and seize any digital device, software or hardware found at the scene.

2. Digital devices are akin to a filing cabinet or a vault. More germane to this investigation, images and videos of child pornography are hoarded by those who possess it. People who possess these images, rarely, if ever, dispose of them as the sexually explicit material is treated as a prize possession. It acts as a sexual stimulus and provides sexual gratification. Great lengths will be taken to conceal and protect from discovery, theft, and damage their collections of illicit materials. The images and videos of child pornography may be moved around to different parts of the digital device or moved to different external media, but it is maintained as a collection for months and years.

3. Since child pornography materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to quickly destroy them. Because of their illegality and the severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

4. Alternatively, those who download and possess child pornography either feel guilty because of the actions they have committed or are afraid they will be caught, and thus will delete the images of child pornography after viewing them. However, digital devices maintain deleted material or in some instances files and records of the child pornography that was downloaded and viewed. Thus, the information, if once on the digital device, can usually be retrieved from that digital device.

5. Digital device technology has revolutionized the way in which child pornography is produced, distributed, and utilized. Digital devices have also revolutionized the way in which a person possessing child pornography interacts with each other. Child pornography formerly was produced using cameras and film (either still photography or movies). The photographs required darkroom facilities and a significant amount of skill in order to develop and reproduce images. There were significant costs involved with the production of pornographic images. To distribute these on any scale required significant resources. The photographs themselves were somewhat bulky and required secure storage to prevent their exposure to the public. The distribution of these wares was accomplished through a combination of personal contact, mailings and telephone calls. Any reimbursement would follow these same paths.

6. The development of digital devices and computers has changed all of this, serving four functions in connection with child pornography: production, communication, distribution, & storage.

7. Pornographers can now produce both still photographs (commonly referred to as "pics") and movie images directly from a common cell phone or video camera. A video camera can be attached, using a cable, directly to the computer using a device called a video capture board. This device turns the video output into a form that is usable by computer program. The output of the video camera can be stored, manipulated, transferred or printed out directly from the computer. The captured image can be edited like a photograph. The image can be lightened, darkened, cropped, and manipulated in a wide variety of ways. 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. There is the added benefit to the pornographer that this method of production does not leave as large a trail for law enforcement to follow as have methods used in the past.

8. Previously, a person possessing child pornography had to rely on personal contact, U.S. mail, and telephonic communications in order to sell, trade, or market child pornography. The development of digital devices has changed that. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable television lines or satellite connection. By connection to a host computer, electronic contact can be

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

made to literally millions of computers around the world. A host computer is one that is attached to a dedicated network and serves many users. These host computers are sometimes commercial concerns, such as Yahoo.com or Google.com mail or GMAIL, which allow subscribers to connect to a network which is in turn connected to their host systems. These service providers allow electronic mail service between subscribers and sometimes between their own subscribers and those of other networks.

9. This communication structure is ideal for the person possessing child pornography. The communication allows the user to locate others of similar inclination and still maintain their anonymity. Once contact is established, it is then possible to send text messages and graphic images/movies to a trusted conspirator. In addition to the use of large service providers, a person possessing child pornography and pornographers can use standard Internet connections, such as those provided by businesses, universities, and government agencies to communicate with each other and to distribute pornography. These communication links allow contacts around the world.

10. These communications can be quick, relatively secure, and anonymous. These advantages are well known and are the foundation of commerce and communication between persons possessing child pornography on the Internet.

11. Your Affiant used the Internet Protocol address (also known as an IP address) provided by the reporting company to track the source of the child pornography. An IP address is a set of numbers which identify an electronic device on the Internet. IP addresses follow the format of ####.####.####.####, wherein each of the numbers are between 0 and 255<sup>3</sup>, or #####:#####:#####:#####:#####:#####:#####:#####, wherein each digit is between 0 and 'F' in hexadecimal form<sup>4</sup>. Computers use IP addresses to identify each other on the Internet. Internet Protocol addresses, both V4 and V6, are registered to specific individuals, or entities such as an Internet service provider.

<sup>3</sup>As specified in the protocol TCP/IP v4 which is a common, but legacy usage today.

<sup>4</sup>As specified in the protocol TCP/IP v6, which is slowly becoming standard usage.

12. When a subscriber of an Internet service provider wishes to access the Internet via their service, the Internet service provider will assign that account an IP address which identifies that account holder on the Internet. By providing the Internet service provider with the dates, times and IP addresses which a suspect used to access the Internet, the Internet service provider is able to provide the identifying information for the account holder who was assigned that specific IP address at that date/time, if the records still exist on their system.

13. Your Affiant thus believes there is probable cause that evidence relevant to the possession of child pornography still exists at the above stated residence.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

## SPECIFICS OF SEARCHING DIGITAL DEVICES

1. Your Affiant requests permission to search and seize any digital device found at the premises.
2. Your Affiant knows from training and experience that current electronic devices consist of central processing units (CPU's), other types of processing units, display screens, SIM cards, modems, RAM, NAND Flash memory, hard disks, hard disk drives, display screens, keyboards, and memory cards (i.e. scan disk, micro scan disk) containing information. These items are necessary evidence to establish a particular person was able to, and has the ability to commit the acts alleged.
3. Your Affiant knows from training and experience that electronic devices and magnetic media are used to store information. That information often includes data files of the evidence believed to exist in this case as well as of other persons engaged in similar activities with juveniles, and lists of other exploited juveniles, as well as records of correspondence (printed or electronic) with such persons, and pictures and/or videos of juveniles.
4. Your Affiant knows from training and experience that searches and seizures of evidence from electronic devices must be processed later by a qualified person in a laboratory or other controlled environment. Devices include but are not limited to such as fixed disks, memory cards (i.e. scan disk, micro scan disk) used by laptops and computers to store or retrieve data or images of solicitation can store the equivalent of thousands of pages of information. Users may store information or images or videos in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can be accomplished by the Palm Beach County Sheriff's Office.
5. Your Affiant knows from training and experience that searching electronic devices for criminal evidence requires experience in the computer field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Evidence can also be embedded into unlikely files for the type of evidence, such as a photo hidden within a document or vice versa, or files stored on an external device in an effort to conceal their existence. Information stored in digital devices and on media can be stored in random order; with deceptive file names; can be hidden from normal view; can be encrypted or password protected; Since digital evidence is extremely vulnerable to tampering or destruction (both from external sources and from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.
6. Your Affiant knows from training and experience that files related to the exploitation of children found on electronic devices are usually transmitted using the Internet or telephone connection using application software which often leaves files, logs or file remnants which would

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

tend to show the exchange, transfer, distribution, possession or origin of the files. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

7. Your Affiant knows from training and experience that electronic devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the laptop as well as ownership and use of Internet service accounts used for the Internet access.

8. Your Affiant knows from training and experience that searching for a particular piece of evidence can be a painstaking and complicated process. A suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. File extensions can be intentionally altered to make graphic files appear to be text files and text files appear to be graphic files. Such difficulties can also arise even when the user is not intentionally trying to conceal the nature of his or her files. For example, documents are frequently stored on digital devices after having been scanned and converted into digital format. When stored in this manner, such documentary evidence is converted to a graphical image format much like a photograph. Therefore, it is necessary for the forensic examiner to inspect files stored in graphical format to see if the relevant documents have been so stored. Graphical images or pictures can be stored on a digital device with either the standard graphical extensions such as jpg, .bmp, gif, etc... or they can be embedded in other file types, such as word processing documents, spreadsheets and other usable programs. The forensic examiner, therefore, will need to view such other programs to see if the relevant graphical images are stored in such a manner. It is thus essential to search files of all types in the "PROPERTY" order to ensure that any and all evidence or instrumentalities of crime are discovered. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime.

9. Apart from user-generated files and data, digital devices and media typically store, often without any conscious action by the user, electronic evidence pertaining to virtually all actions taken on the digital device. This includes, for example, information regarding the identity of the device user(s) (the actual or assumed identity used by the person or persons using the digital device or media (user profile)). Additional examples of the type of data that analysis of digital devices and media can reveal include the date, time, and geographic location at which the device or media were used; evidence regarding the purpose of and actual use of the device and media; and evidence related to devices that have been connected, via wire or wirelessly, to the device being searched, which can include evidence of remote storage, syncing of devices to one another, uploading or saving data to other devices, pointers to, and/or information pertaining to evidence that was transferred to and/or is stored at other locations such as web-based email accounts, network accessible services, social networking websites, and cloud storage. Digital device users typically do not erase or delete this evidence, because special software is typically required for the task. However, it is technically possible to delete this information. The data can be found in numerous locations, and formats. These types of information will be important to the forensic examiner's ability to piece together and recognize evidence of the above-listed crimes, when it is found in the digital device(s) or digital storage media.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

10. Based on my training and experience, your Affiant knows that digital devices and digital storage media can store the above-referenced information for long periods of time, and that the information can often be retrieved by a trained forensic examiner months or even years after the data was stored on the digital device(s), even when it purportedly has been erased or deleted from the device(s). Deleted data remains accessible to a forensic examiner until the memory space at which it is stored is needed for new data. Thus, the ability to retrieve residue of a deleted electronic file from a hard drive depends less on when the file was created, downloaded, viewed, or deleted, than on a particular user's operating system, storage capacity, and computer habits. A forensic examiner can usually retrieve the above referenced evidentiary material from digital devices and media.

11. Your Affiant knows from training and experience that various software applications may contain relevant saved digital data, and requests this be searched as well. In the search for child exploitation material, it is possible to locate the source of the images by analyzing software applications that are used to access the Internet. Graphical imaging programs may contain data that shows the relevant images were actually viewed by someone after being downloaded to the digital device. Since it is important to determine whether any of the relevant images were actually viewed while on the subject digital device, a forensic analyst will need to examine the file properties of any images found and determine whether any of these images were manipulated or viewed by any of the software resident on the digital device.

12. Your Affiant is aware that search warrants involved in digital devices related to criminal activity usually produces items that would tend to establish ownership, control, or use of digital devices to include receipts, credit card bills, telephone bills, correspondence and other identification documents.

#### **NECESSITY TO SEIZE DIGITAL DEVICES AND SEARCH ON SCENE**

1. Your Affiant requests permission to search and seize any digital device found at the scene.

2. Your Affiant knows from training and experience that computer systems commonly consist of central processing units (CPU's), hard disks, hard disk drives, floppy disk drives, tape drives, display screens, keyboards, printers, modems (used to communicate with other computers), electronic cables, cassette tapes, floppy disks, and other forms of magnetic media containing computer information. In addition, the specific transmission of computerized imagery indicates the possible use of CD-ROM drives and their compact laser disks, image scanning devices, still cameras and lighting equipment, video cameras or camcorders, VCRs, digital-analogue translation devices, and the software (computer programming) necessary to operate them. Other storage devices such as, but are not limited to MP3 music players, digital cameras, Personal Digital Assistants (PDAs), laptop computers, sub-notebook computers, handheld computers, USB storage devices, external

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

hard drives, console gaming systems, and wireless hard drives are marketed for use as storage devices, albeit for legitimate purposes. These items are necessary evidence to establish a particular person was able to, and has the ability to commit the acts alleged.

3. Your Affiant knows from training and experience that one form in which evidence of or pertaining to the above-listed crimes might be found is digital -- stored on a digital device or digital storage media. The terms "digital device" and "device" include devices capable of capturing and/or storing digital data, such as computers, cell phones, cameras, personal assistants, iPods, portable media players, tablet computers like iPad, gaming consoles, video cameras, DVRs (digital video recorders), web cams or other video capture devices, modems, routers, firewalls, wireless access points, printers, GPS navigation devices, etc. Digital data storage media (hereafter "media") include solid state drives (SSDs), hard disk drives (HDDs), compact discs, DVDs, Blu-Ray discs, flash media such as USB memory sticks, thumb drives, flash drives, Secure Digital (SD) cards, Micro Secure Digital (MicroSD) cards, backup drives, and the like. Data stored on digital devices and media can be easily transferred from one device or storage media to another. These items are necessary evidence to establish a particular person was able to, and has the ability to commit the acts alleged.

4. Your Affiant knows from training and experience that such digital devices are used to store information. In addition to the above mentioned image files, that information often includes data files of other persons engaged in similar activities with juveniles, and lists of other exploited juveniles, as well as records of correspondence (printed or electronic) with such persons.

5. Your Affiant knows from training and experience that searches and seizures of evidence from computers require agents to seize most or all computer items (hardware, software, passwords and instructions) to be processed later by a qualified person in a laboratory or other controlled environment. This includes computer storage media to include but not limited to floppy disks, hard drives, tapes, DVD discs, CD-ROM discs, external storage devices, internal hard drives and/or storage devices, or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography can store the equivalent of thousands of pages of information. Users may store information or images in random order with deceptive file names, which requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process renders it impractical to attempt this kind of data search on site and will be processed later by a qualified person in a laboratory or other controlled environment.

6. Your Affiant knows that if the computer or other device is "on" when the search is conducted, that searching said device at the residence is imperative before it is shut down so that data in the short term memory of the computer (or RAM) is not lost. Said information will contain the most recent actions performed on the device including the access or use of child pornography.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

## NECESSITY TO REMOVE DIGITAL DEVICES FROM PREMISES AND CONDUCT THOROUGH SEARCH OFF-SIGHT

7. Your Affiant knows from training and experience that searching digital devices for criminal evidence requires experience in the field and a properly controlled environment in order to protect the integrity of the evidence and recover even "hidden", erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (both: from external sources and/or from destructive code imbedded in the system as a "booby trap"), the controlled environment of a laboratory is essential to its complete and accurate analysis.

8. Wholly apart from user-generated files and data, digital devices and media typically store, often without any conscious action by the user, electronic evidence pertaining to virtually all actions taken on the digital device. This includes, for example, information regarding the identity of the device user(s) (the actual or assumed identity used by the person or persons using the digital device or media (user profile)). Additional examples of the type of data that analysis of digital devices and media can reveal include the date, time, and geographic location at which the device or media were used; evidence regarding the purpose of and actual use of the device and media; and evidence related to devices that have been connected, via wire or wirelessly, to the device being searched, which can include evidence of remote storage, synching of devices to one another, uploading or saving data to other devices, pointers to, and/or information pertaining to evidence that was transferred to and/or is stored at other locations such as web-based email accounts, network accessible services, social networking websites, and cloud storage. Digital device users typically do not erase or delete this evidence, because special software is typically required for the task. However, it is technically possible to delete this information. The data can be found in numerous locations, and formats. These types of information will be important to the forensic examiner's ability to piece together and recognize evidence of the above-listed crimes, when it is found in the digital device(s) or digital storage media.

9. Evidence can also be embedded into unlikely files for the type of evidence, such as a photo hidden within a document or vice versa, or files stored on an external device in an effort to conceal their existence. Information stored in digital devices and on media can be stored in random order; with deceptive file names; can be hidden from normal view; can be encrypted or password protected; and can be stored on unusual devices for the type of data, such as routers, printers, scanners, game consoles, or other devices that are similarly capable of storing digital data. Additionally, a computer router may store information about a user's internet access and could reveal unknown connected digital or remote storage devices or capability; a scanner or printer may store information that would identify the digital device with which it was used. Whether some data on the digital device(s) or media is evidence may depend on other information stored on the

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County  
Sheriff's Office

Warrant No.: PBSO\_2021\_000448

Agency Case No.: 20-250140

Reviewing Prosecutor:Eric Baum

digital device(s) and media, and the application of an examiner's knowledge about how digital device(s) and media behave. A person, who has appropriate familiarity with how a digital device works, and relevant contextual information from a particular device, can draw conclusions about how the devices and media were used, by whom, where, and when. This information is sometimes necessary to identify and understand the other evidence that falls within the scope of the warrant. Further, in finding evidence of how a digital device or media was used, the purpose of its use, who used it, where, and when, it is sometimes necessary to establish that a particular thing is not present on the device or media.

10. Based on training and experience, your Affiant knows that digital device(s) and digital storage media can store the above-referenced information for long periods of time, and that the information can often be retrieved by a trained forensic examiner months or even years after the data was stored on the digital device(s), even when it purportedly has been erased or deleted from the device(s). Deleted data remains accessible to a forensic examiner until the memory space at which it is stored is needed for new data. Thus, the ability to retrieve residue of a deleted electronic file from a hard drive depends less on when the file was created, downloaded, viewed, or deleted, than on a particular user's operating system, storage capacity, and computer habits. A forensic examiner can usually retrieve the above referenced evidentiary material from digital devices and media.

11. Digital device programs frequently require passwords, user names, and/or pass phrases to operate. Those may be kept inside a device, or outside the device in some other area known to the user. So, in addition to searching a digital device for evidence of the above-listed crime(s), investigators will need to search both the premises searched, and the digital device for evidence identifying the user(s) of the device and for passwords, user names, and/or pass phrases needed to operate the device. Further, due to the wide variety of digital devices and their operating systems, the forensic examiner may also need the following items in order to conduct a thorough and accurate search of the devices: computer hardware, software, peripherals, internal or external storage devices, power supplies, cables; internet connection and use information; security devices; software; manuals; and related material.

12. Your Affiant knows from training and experience that persons trading in, receiving, distributing or possessing images involving the exploitation of children or those interested in the actual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child exploitation.

13. Your Affiant knows from training and experience that searching for a particular piece of evidence can be a painstaking and complicated process. A suspect may try to conceal criminal evidence by storing it in random order with deceptive file names. File extensions can be intentionally altered to make graphic files appear to be text files and

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

text files appear to be graphic files. Such difficulties can also arise even when the user is not intentionally trying to conceal the nature of his or her files. For example, documents are frequently stored on digital devices after having been scanned and converted into digital format. When stored in this manner, such documentary evidence is converted to a graphical image format much like a photograph. Therefore, it is necessary for the forensic examiner to inspect files stored in graphical format to see if the relevant documents have been so stored. Graphical images or pictures can be stored on a digital device with either the standard graphical extensions such as .jpg, .bmp, gif, etc... or they can be embedded in other file types, such as word processing documents, spreadsheets and database and PowerPoint programs. For instance, a slide show consisting of hundreds of images can be imbedded in a Power Point presentation program and it would not be apparent to the examiner until opening and viewing that program. The forensic examiner, therefore, will need to view such other programs to see if the relevant graphical images are stored in such a manner. It is thus essential to search files of all types in order to ensure that the requested "Property" is discovered. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crime.

14. Your Affiant knows from training and experience that various software applications may contain the evidence sought, and requests them to be searched as well. In the search for child exploitation material, it is possible to locate the source of the data and whether they were received or distributed via the Internet by analyzing software applications that are used to access the Internet. Examination of the applications and the files within them, makes it possible to locate the source of any images/videos. Graphical imaging programs may contain data that shows the relevant data were actually viewed by someone after being downloaded to the digital device. Since it is important to determine whether any of the relevant data were actually viewed while on the subject digital device, a forensic analyst will need to examine the file properties of any data found and determine whether any of the data were manipulated or viewed by any of the software resident on the digital device.

15. Your Affiant knows from training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files. Also that computer software or hardware exists that allows persons to share Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

16. Your Affiant knows from training and experience that computers used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of internet service accounts used for the internet access.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor: Eric Baum

17. Your Affiant knows search warrants of residences involved in digital device or computer related criminal activity usually produces items that would tend to establish ownership, control, dominion, or use of digital devices, the Premises, or of any Internet service accounts accessed to obtain child pornography to include but not limited to credit card bills, receipts, telephone bills, correspondence, rental agreements, and other identification documents.

18. Your Affiant knows from training and experience that in order to fully retrieve data from a digital device, the analyst needs all magnetic storage devices as well as the digital devices. In cases like this one where the evidence consists partly of graphics files, the input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing computer storage media and the storage media are also essential to show the nature and quality of the graphic images which the system could produce. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media) as well as documentation, items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized or to activate specific equipment or software. Your Affiant knows that digital files can be easily transferred from one digital device to another through a number of different means.

19. Your Affiant knows that digital data, such as images, screenshots, messages, etc., can easily be transferred from one device to another for storage or sharing purposes. This transfer can occur through many means, such as data transfer cable, Bluetooth, email, text message, WiFi sharing, AirDrop, etc.

20. Your Affiant knows from training and experience that files related to the exploitation of children found on computers are usually obtained from the Internet using application software which often leaves files, logs or file remnants which would tend to show the exchange, transfer, distribution, possession or origin of the files. Also that computer software or hardware exists that allows persons to share Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address. Examination of these items can reveal information about the authorized or unauthorized use of Internet connection at the residence.

21. Your Affiant knows from training and experience that digital devices used to access the Internet usually contain files, logs or file remnants which would tend to show ownership and use of the computer as well as ownership and use of internet service accounts used for the internet access. Your Affiant is aware that search warrants of residences involved in digital device related criminal activity usually produces items that would tend to establish ownership or use of computers and ownership or use of any Internet service accounts accessed to obtain child pornography including but not limited

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

to credit cards, credit card bills, telephone bills, correspondence and other identification documents.

#### **GLOSSARY OF TERMS APPLICABLE TO THIS AFFIDAVIT**

22. **INTERNET SERVICE PROVIDER (ISP):** company that provides its customers with access to the Internet, usually over telephone or cable connections. Typically, the customer pays a monthly fee, and the ISP supplies software that enables the customer to connect to the Internet by a modem or similar device attached to/installed in a digital device.
23. **IP ADDRESS (Internet Protocol Address):** the unique numeric address of a machine or digital device attached to and using the Internet. IPv6 addresses are represented in 8 groups of 16 bits each. Each group is written as four hexadecimal digits and the groups are separated by colons (:). An example of this representation is `2001:0db8:0000:0000:ff00:0042:8329`. Each number can only be used by one digital device or machine over the Internet at a time.
24. **MINOR** means any person under the age of 18 years. Florida Statute 847.001(8).
25. **CHILD PORNOGRAPHY** means any image depicting a minor engaged in sexual conduct. Florida Statute 847.001(3).
26. **SEXUAL CONDUCT** means actual or simulated sexual intercourse, deviate sexual intercourse, sexual bestiality, masturbation, or sadomasochistic abuse; actual lewd exhibition of the genitals; actual physical contact with a person's clothed or unclothed genitals, pubic area, buttocks, or, if such person is a female, breast with the intent to arouse or gratify the sexual desire of either party; or any act or conduct which constitutes sexual battery or simulates that sexual battery is being/will be committed. F.S. §847.001
27. **STATIC IP** remains constant without changing for a particular user.
28. **DYNAMIC IP** - assigns a different IP address each time the ISP customer logs on to the Internet, but this is dependent upon the Internet Service Provider (ISP) because some ISP's only change the IP address as they deem it necessary. However, only one user account can be assigned a particular IP address at any given time.

The above information leads your Affiants to believe and to have probable cause to believe that the Premises and the curtilage thereof are being used for the purpose of storing and/or distributing images, movies, or visual depictions of sexual conduct or sexual performance by a child or children, in violation of sections 827.071, Florida Statutes, related the possession of images of child pornography. It is also your Affiant's belief that the premises and the curtilage

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

thereof are being used to upload images of child pornography, in violation of section 827.071(5), Florida Statutes relating to Possession of child pornography.

WHEREFORE, Your Affiants make this affidavit and prays that a search warrant be issued commanding the Sheriff of Palm Beach County, Florida, and the Sheriff's deputies and/or any police officer in Palm Beach County within whose jurisdiction the aforesaid property to be searched is found, or the Commissioner of the Florida Department of Law Enforcement, or any of his duly constituted Agents, and any Investigators or Special Investigators of the Office of the State Attorney, 15<sup>th</sup> Judicial Circuit, with proper and necessary assistance, to search the Premises and property and all of its spaces and its curtilage where the property might be kept for the property specified, including all vehicles, vessels, outbuildings and containers within the curtilage and any person thereon reasonably believed to be connected with the illegal activity, certain property contained therein that has been used to commit any crime, or constitutes evidence relevant to proving that a crime has been committed reasonably believed to be connected with the illegal activity making the search in the daytime or the nighttime, as the exigencies may demand or require, or on Sunday, and to bring the property and any person arrested before a court having jurisdiction of the offense.

*Brian Pherson*  
Palm Beach County Sheriff's Office  
February 16, 2021 04:05:52 PM

Detective Brian Pherson (I.D.#13024)  
February 16 2021 04:05:52 PM

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001136

The foregoing Affidavit and Application for Search Warrant was sworn to (or affirmed) and subscribed before me this 16 day of February, 2021.

Search Warrant  
Jason L'Etoile  
Sergeant 6489  
04:10:00 PM  
2021\_000448

Sergeant Jason W L'Etoile (I.D.# 6489)  
February 16 2021 04:10:00 PM  
Law Enforcement Officer Authorized to Administer Oaths under F.S. 117.10.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

001137

IN THE COUNTY/CIRCUIT COURT  
OF THE 15TH JUDICIAL CIRCUIT  
IN AND FOR PALM BEACH COUNTY, FLORIDA

SEARCH WARRANT

THE STATE OF FLORIDA  
COUNTY OF PALM BEACH

IN THE NAME OF THE STATE OF FLORIDA, TO ALL AND SINGULAR:

The Sheriff of Palm Beach County, Florida, and the Sheriff's deputies, any police officer in Palm Beach County, Florida, within whose jurisdiction the Property to be searched is found, the Commissioner of the Florida Department of Law Enforcement and any of his duly constituted Agents, Investigators and Special Investigators from the Office of the State Attorney.

WHEREAS, a complaint on oath and in writing, supported by affidavit of a credible witness has this day been presented to me, and upon examination of the affidavit and application for this search warrant, I am satisfied that probable cause exists that the Premises located in Palm Beach County, Florida described as:

3098 Perry Ave. Greenacres FL 33463



Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor: Eric Baum

001139

To reach the premises desired to be searched, start at the Palm Beach County Sheriff's Office District 16 Substation located at 2995 Jog Road in Greenacres, FL 33467. Travel south on Jog Road for 2.6 miles then turn east (left) on Brentwood Blvd. Travel 0.4 miles on Brentwood Blvd. then turn left onto Gillette Drive. In 0.5 miles turn left onto Plains Drive. Travel 0.2 miles on Plains Drive and turn left into the cul-de-sac of Angola Circle. The residence is approximately 108 feet on the left side of the street, 3<sup>rd</sup> house on the left. The building is grey stone and tan with a shingle roof. The numerical "5037" is posted in black lettering affixed above the front screen door to the residence. This is a complete description of the premises desired to be searched.

Being the premises of, or occupied by, or under the control of The Minor Family, as verified through Intelligence gathered from various Law Enforcement Database(s), Sprint, DAVID, Florida's DHSMV, and your Affiant's Surveillance.

And there is now being kept, in the above described premises, certain property contained therein that has been used to commit any crime, or constitutes evidence relevant to proving that a crime has been committed; to wit:

1. Images, movies, or visual depictions of sexual conduct or sexual performance by a child or children, in violation of Florida Statute 827.071.
2. All data, content, files, and information contained on any electronic devices, storage devices, software, or hardware.
3. Any and all digital device(s) and all data, content, files, and information contained on them; including but not limited to any device capable of capturing and/or storing digital data, sub-compact computers, cell phones, and "smart" cell phones, desktop computers, laptop computers, cameras, personal assistants, iPods, portable media players, tablet computers like iPad, gaming consoles, video cameras, DVRs (digital video records), web cams or other video capture devices, modems, routers, firewalls, wireless access points, printers, cellular telephones, GPS navigation devices, etc.
4. Digital device hardware and all data, files, content, and information contained in them, including but not limited to, any and all digital device equipment used to collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar digital device impulses or data. Hardware includes (but is not limited to) any data processing devices (such as such as central processing units, personal computers to include "laptop" or "notebook" or "pocket" computers or mobile "smart" phones); internal and peripheral storage devices (such as Universal Serial Bus ("USB") memory sticks or thumb

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor: Eric Baum

drives, fixed disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, and other electronic media devices).

5. Digital device input and output devices to include but not limited to keyboards, mice, scanners, printers, monitors, network communication devices, modems and external or connected devices used for accessing digital device storage media.

6. Digital device storage media and the digital content to include but not limited to USB memory sticks or flash or thumb drives, floppy disks, hard drives, tapes, DVD disks, CD-ROM disks or other magnetic, optical or mechanical storage which can be accessed by computers to store or retrieve data or images of child pornography. Additionally, any digital data storage media ("media"), solid state drives (SSD's), hard disk drives (HDD's), Blu-Ray discs, flash media, Secure Digital (SD) cards, Micro Secure Digital (Micro SD) cards, backup drives.

7. Digital device software and application software installation and operation media.

8. Digital device software, hardware or digital contents related to the sharing of Internet access over wired or wireless networks allowing multiple persons to appear on the Internet from the same IP address.

9. Manuals and other documents (whether digital or written) that describe operation of items or software seized.

10. Items containing or displaying passwords, access codes, usernames or other identifiers necessary to examine or operate items, software or information seized.

11. Within the digital device(s): data maintained on the device; in particular, text messages, chats, data in the form of images, videos, and/or log files recording the transmission of files as they relate to violations of Florida law cited herein related to the possession, transmission or sexual conduct of minors.

12. Within the digital device(s): all relevant contents and data, including but not limited to, Subscriber and equipment identifiers, Date/time, language and other settings, contact information, appointment calendar information, dialed, incoming, and missed call logs, electronic mail, photos, audio and video recordings, multi-media messages, instant messaging and web browsing activities, electronic documents, location information, SMS and MMS messages, Any messages

13. Correspondence or other documents (whether digital or written) pertaining to the possession, receipt, origin or distribution of images involving the exploitation of children. Correspondence or other documents (whether digital or written) exhibiting an interest in the exploitation of children.

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

14. Items that would tend to establish ownership or use of digital devices and ownership or use of any Internet service accounts accessed to obtain child pornography including but not limited to receipts, credit card bills, telephone bills, correspondence and other identification documents.

15. Items that would tend to show dominion, control and ownership of the premises and property searched, to include utility bills, telephone bills, correspondence, rental agreements and other identification documents.

16. Data maintained on the digital devices, or digital device related storage devices such as USB memory sticks or thumb drives/flash drives, floppy diskettes, tape backups, computer printouts, and "zip" drive diskettes. In particular, data in the form of images, and/or log files recording the transmission of images as they relate to violations of Florida law cited herein related to the possession and/or distribution of child pornography.

17. Preservation of data maintained in any online remote storage devices/programs that are linked to the digital device or digital device related storage device through folders or internet access.

All of which items detailed in 1-17 above are hereinafter referred to as "The Property" that constitutes evidence relevant to proving that a felony has been committed, to wit:

**F.S.S. 827.071(5) Possession of Child Pornography**

and that the grounds for issuance are, to wit:

**F.S.S. 933.18(6): (Dwelling)**

- A weapon, instrumentality, or means by which a felony has been committed is contained therein.
- Evidence relevant to proving a felony has been committed is contained therein.

NOW THEREFORE, the Sheriff of Palm Beach County, Florida, and all of his deputies, any police officer in Palm Beach County, Florida within whose jurisdiction the aforesaid Property to be searched is found, the Commissioner of the Florida Department of Law Enforcement, and any of his duly constituted Agents, Enforcement and any of his duly constituted Agents, and Investigators and Special Investigators from the Office of the State Attorney are hereby commanded with lawful and proper assistance as may be necessary in the name of the State of Florida, to enter and search the Premises hereinbefore specified and all of its spaces and its curtilage, where the Property might be kept, including all vehicles, vessels and containers within the curtilage, and any person thereon reasonably believed to be connected with the illegal activity; making the search in the daytime or the nighttime, as the exigencies may demand or

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

require, or on Sunday, and if the Property is found there, to seize it, search it, arrest all persons unlawfully possessing it, and to bring the same before a court of competent jurisdiction.

You are further commanded, in the event that you seize any of the said Property hereinbefore described, to make up, at the time and place of seizure, a full, true and itemized list and inventory of all things seized and taken, in duplicate, signed by you, and to then and there give and deliver the said duplicate copy thereof to the person from whom possession shall be taken, if taken from the possession of anyone, together with a duplicate copy of this warrant, and if not taken from the possession of anyone, then to any person in charge of said Premises and in the absence of any such person, to leave the same on or in the Premises.

PURTHER, this court directs that the Affiant keep the original Affidavit and Application in support of this Search Warrant, in the custody of the executing agency until further Order of the Court or until release by the executing agency.

The original of the warrant, together with the original inventory, shall be returned and filed with the Clerk of the Court as stated above within ten (10) days of the issuance of this warrant. Further, any Property seized or taken shall be impounded for use as evidence at any trial of any criminal or penal cause growing out of the having or possession of said Property.

WITNESS MY HAND AND SEAL this 16 of February in the year 2021.

*Sandra Bosso Pardo*  
Sandra Bosso Pardo  
15TH Judicial Circuit  
In and for PALM BEACH County, Florida  
February 16 2021 04:24:19 PM

Sandra Bosso Pardo  
15TH Judicial Circuit  
In and for PALM BEACH County, Florida  
February 16 2021 04:24:19 PM

Tuesday, February 16, 2021 16:24:19

Agency Name: Palm Beach County Sheriff's Office	Warrant No.: PBSO_2021_000448
Agency Case No.: 20-250140	Reviewing Prosecutor:Eric Baum

IN THE CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT,  
IN AND FOR PALM BEACH COUNTY, FLORIDA  
CRIMINAL DIVISION "R"

STATE OF FLORIDA

CASE NO.: 2021CF001670AMB

vs.

MARK MINOR,  
Defendant

**Motion for Twelve-Member Jury**

The defendant objects to trial by a jury of six and moves that he be tried by a jury of twelve members. He is charged with 53 counts of possession of child pornography. Although each of those offenses is only individually punishable by 15 years, if convicted as charged, his sentence points under the Criminal Punishment Code (972 points) far exceed 363 points. As such, he is subject to a sentence of life imprisonment pursuant to § 921.0024(2), Fla. Stat.

The defendant recognizes that the state constitution provides:

SECTION 22. Trial by jury.—The right of trial by jury shall be secure to all and remain inviolate. The qualifications and the number of jurors, not fewer than six, shall be fixed by law.

Art. I, § 22, Fla. Const.

No other state allows for a jury of six members for a crime punishable by up to life imprisonment, and only one allows for a jury of less than twelve members for such a crime: Utah law provide for a jury of eight for noncapital crimes punishable by more than one year. Utah Code, § 78B-1-104.

Florida's provision for a jury of six stems from the dawn of the Jim Crow era, one month after federal troops were withdrawn from the state.

The historical background is as follows:

In 1875, the Jury Clause of the 1868 constitution was amended to provide that the number of jurors “for the trial of causes in any court may be fixed by law.” *See Florida Fertilizer & Mfg. Co. v. Boswell*, 34 So. 241, 241 (Fla. 1903).

The common law rule of a jury of twelve was still kept in Florida while federal troops remained in the state. There was no provision for a jury of less than twelve until the Legislature enacted a provision specifying a jury of six in Chapter 3010, section 6. *See Gibson v. State*, 16 Fla. 291, 297–98 (1877) (quoting and discussing Chapter 3010, section 6, Laws of Florida (1877)); *Florida Fertilizer*, 34 So. 15 241 (noting that previously all juries had twelve members).

The Legislature enacted chapter 3010 with the jury-of-six provision on February 17, 1877. *Gibson*, 16 Fla. 294. This was less than a month after the last federal troops were withdrawn from Florida in January 1877. *See* Jerrell H. Shofner, *Reconstruction and Renewal, 1865-1877*, in *The History of Florida* 273 (Michael Gannon, ed., first paperback edition 2018) (“there were [no federal troops] in Florida after 23 January 1877”). *See also* <https://dos.myflorida.com/florida-facts/florida-history/a-brief-history/civil-war-and-reconstruction/>.

The jury-of-six thus first saw light at the birth of the Jim Crow era as former Confederates regained power in southern states and state prosecutors made a concerted effort to prevent blacks from serving on jurors.

On its face the 1868 constitution extended the franchise to black men. But the historical context shows that it was part of the overall resistance to Reconstruction efforts to protect the rights of black citizens. The constitution was the product of a remarkable series of events including a coup in which leaders of the white southern (or native) faction took possession of the assembly hall in the middle of the night, excluding Radical Republican delegates from the

proceedings. *See* Richard L. Hume, *Membership of the Florida Constitutional Convention of 1868: A Case Study of Republican Factionalism in the Reconstruction South*, 51 Fla. Hist. Q. 1, 5-6 (1972); Shofner at 266. A reconciliation was effected as the “outside” whites “united with the majority of the body’s native whites to frame a constitution designed to continue white dominance.” Hume at 15.

The racist purpose of the resulting constitution was spelled out by Harrison Reed, a leader of the prevailing faction and the first governor elected under the 1868 constitution, who wrote to Senator Yulee that the new constitution was constructed to bar blacks from legislative office:

Under our Constitution the Judiciary & State officers will be appointed & the apportionment will prevent a negro legislature.

Hume, 15-16. *See also* Shofner 266 and Adam Wasserman, *A People’s History of Florida* 530 (4th ed. 2009).

The Supreme Court held in *Patton v. United States*, 281 U.S. 276 (1930), that the Sixth Amendment right to trial by jury means “a trial by jury as understood and applied at common law, and includes all the essential elements as they were recognized in this country and England when the Constitution was adopted, is not open to question. Those elements were: (1) That the jury should consist of twelve men, neither more nor less; (2) that the trial should be in the presence and under the superintendence of a judge having power to instruct them as to the law and advise them in respect of the facts; and (3) that the verdict should be unanimous.” *Id.* at 288 (emphasis added).

The Defendant recognizes that in *Williams v. Florida*, 399 U.S. 78 (1970), the Supreme Court departed from the historical discussion in *Patton*, and held that a jury of twelve is not required by the Sixth Amendment as applied to the states by the Fourteenth Amendments. The

Defendant submits, however, that the *Williams* decision failed to take into account the history of Florida's six-member jury system and was based on an erroneous view of incorporation under the Fourteenth Amendment which has since been abandoned by the Court.

Fifty years after *Williams*, the Supreme Court abandoned the view of Fourteenth Amendment incorporation set out in *Apodaca v. Oregon*, 406 U. S. 464 (1972), and a companion case, *Johnson v. Louisiana*, 406 U. S. 356 (1972), and held that a non-unanimous verdict of a jury of twelve violates the Sixth Amendment. As Justice Alito noted in his dissent in *Ramos*, Justice White's plurality opinion in *Apodaca* was based on the view of the Sixth Amendment incorporation set out in *Williams*.

In *Ramos*, the plurality opinion of [REDACTED] repeatedly pointed out that the common law required a jury of twelve. *Id.* at 1395, 1396-97, 1400 n. 38. Justice Gorsuch noted that the Louisiana non-unanimity arose from Jim Crow era efforts to enforce white supremacy. *Id.* at 1394. *See also id.* at 1417 (Kavanaugh, J., concurring) (non-unanimity was enacted “as one pillar of a comprehensive and brutal program of racist Jim Crow measures against African-Americans, especially in voting and jury service.”). The history of Florida’s jury of six arises from the same historical context.

In view of the foregoing, a jury of six at a criminal trial for a crime punishable by up to life imprisonment is unconstitutional under the Sixth and Fourteenth Amendments of the United States Constitution. The defendant demands that he be tried by a jury of twelve.

WHEREFORE, this Court should try the defendant with a jury of twelve members.

**Certificate of Service**

I HEREBY CERTIFY that a true and correct copy of the foregoing was sent by E-service this 17th day of September, 2023 to:

Office of the State Attorney, Division R  
Alexandra Dorman, ASA  
401 N. Dixie Highway  
West Palm Beach, FL 33401  
Service address: [adorman@sa15.org](mailto:adorman@sa15.org)

Respectfully submitted,



---

MATTIE FORE, Esquire  
Bar No.: 0068777  
Mattie Fore Law, LLC  
631 Lucerne Avenue  
Lake Worth Beach, FL 33460  
Phone: (561)-203-0912  
Fax: (561)-228-0094  
Email: mattie@mattieforelaw.com

## ARGUMENT

### I. THE COURT ERRED IN DENYING THE MOTION TO SUPPRESS.

#### Standard of Review

“The standard of review for motions to suppress is that the appellate court affords a presumption of correctness to a trial courts findings of fact but reviews *de novo* the mixed questions of law and fact that arise in the application of the historical facts to the protections of the Fourth Amendment.” *Wyche v. State*, 987 So. 2d 23, 25 (Fla. 2008) (reviewing *de novo* question of whether “defendant’s motion to suppress must be granted because the police investigator told the defendant that his DNA was needed in the investigation of a fictitious burglary”). Here, the question is the legal sufficiency of the description of the place to be searched, a question of law.

#### Discussion

Officers obtained the state’s evidence by execution of a search warrant on Appellant’s house on Perry Avenue.

The warrant said there was probable cause to search Appellant’s Perry Avenue address, and it contained a photograph of a building. R 1139.

But it then gave directions to a house on a cul-de-sac on Angola Circle. R 1140. It was undisputed that this house was miles away from Appellant's Perry Avenue house, as shown by Google Maps. R 1145, 1148.

After giving detailed directions to the Angola Circle house, the warrant described it as follows: "The building is grey stone and tan with a shingle roof. The numerical '[four digit number different from Appellant's house number]' is posted in black lettering affixed above the front screen door to the residence. This is a complete description of the premises desired to be searched." R 1140.

One equipped with the warrant would not be led unerringly to Appellant's house on Perry Avenue to the exclusion of all others. Appellant's house was "light green in color with a gray shingle roof," with a white front door and a specific four-digit house number on the concrete facing the driveway and on a black mailbox. R 1108. This four-digit number was completely different from the number of the Angola Circle house.

In denying the motion to suppress as to this issue, the court relied mainly on its reading of *Bennett v. State*, 150 So. 3d 842 (Fla. 4th DCA 2014) (opinion on rehearing).

As noted in *Bennett*, the Constitution requires a high level of care in the issuance of a search warrant. *Id.* at 844. The Fourth Amendment provides: “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Amend. IV, U.S. Const. (emphasis added). Article I, Section 12 of our constitution contains a longer version of the same requirement.

“Any designation or description known to the locality that points out the place to the exclusion of all others, and on inquiry leads the officer unerringly to it, satisfies the constitutional requirement.” *Bennett*, 150 So. 3d at 844 (emphasis added; quoting *Jackson v. State*, 87 Fla. 262, 267, 99 So. 548 (1924); *State v. Brooker*, 449 So. 2d 386, 387 (Fla. 1st DCA 1984) (“the description of the place to be searched must identify the place to be searched to the exclusion of all others and on inquiry lead the searching officers unerringly to it. *Shedd v. State*, 358 So.2d 1117 (Fla. 1st DCA 1978).”) (emphasis added); *Clapsaddle v. State*, 545 So. 2d 946, 947–48 (Fla. 2d DCA 1989) (“The description must be sufficient to point out the place to be searched to the exclusion of all others, and

on inquiry, lead officers unerringly to it.”).

In *Bennett*, the warrant erred as to the specific street address of a building in an apartment complex, but it correctly identified the building and apartment in the apartment complex, and the officer who prepared the application led the search team to the place. The warrant was for a search of apartment 302 at building Q of an apartment complex on Brooks Street. Although the warrant accurately described the place, the complex’s street address was actually on Petals Road; further, the directions in the warrant were impossible to literally follow. In the same complex was an apartment at the Brooks Street address, but it was building F. Nonetheless, officers searched the right place because “[t]he officer who applied for the warrant, and who had surveilled the premises during a controlled drug buy, accompanied them and directed them to the correct apartment.” *Id.* at 843–44 (emphasis added).

This Court held that the independent knowledge of an officer executing the warrant may be considered in assessing whether the warrant is sufficient, although this principle has limits:

We hold that independent knowledge of the premises by an officer executing a search warrant, where that knowledge was obtained from prior surveillance of the

premises, may be considered in assessing whether the warrant's description of the premises is sufficiently particular. *See Carr*, 529 So. 2d at 806–07; *Burke*, 784 F.2d at 1092–93. This principle has limits, grounded in the need to protect the public from general searches or seizures by officers with unfettered discretion. *See Leveque*, 530 So. 2d at 513; *Garrison*, 480 U.S. at 84, 107 S.Ct. 1013. If the warrant's description is so manifestly defective that the executing officer's independent knowledge is essentially the only way the executing officers could have found the property, the warrant description is not sufficiently particular. *See Williamson*, 1 F.3d at 1136.

Here, the warrant's description is not so manifestly deficient. The description was correct as to the letter of the building and the apartment number. Moreover, there was only one Building Q in the apartment complex.

*Id.* at 846 (emphasis added).

The present case is unlike *Bennett*. The warrant provided a manifestly deficient description, and authorized the search of the Angola Circle house. The description was grossly dissimilar to Appellant's light green house on Perry Avenue, and one following the directions would wind up miles away on Angola Circle, where one was directed to search a gray and tan house with a different street number.

Thus, unlike the description in *Bennett*, an officer following the warrants would not have unerringly come to the house to the exclusion of all others. Moreover, Pherson did not go to the house

with the SWAT team, and was at another location when the warrant was served.

Further, even if Pherson had accompanied the officers, the description of the place to be searched was so dissimilar to Appellant's house that the search of Appellant's house was not authorized by the warrant.

The court also relied on *State v. Houser*, 364 So. 2d 823 (Fla. 2d DCA 1978). There, the warrant gave a very precise description of the place to be searched, but misidentified the place as 6815 Wall Street rather than 6813 Wall Street. *Id.* at 823–24. Thus, the officers were confronted with two buildings side-by-side and the correct one had a very precise description.

The present case is far different from *Houser*. The Perry Avenue and Angola Circles houses were not side-by-side, they were miles apart and the warrant authorized the search of a gray and tan house with a completely different street number than Appellant's light green house.

In these circumstances, the court erred in denying the motion to suppress. The search violated the Fourth Amendment and Article I, Section 12 of our state constitution. The evidence obtained by this

unconstitutional search must be suppressed as the fruit of the poisonous tree.

Because the prosecution case depended entirely on evidence resulting from the search, the convictions should be reversed, and the case should be remanded with instructions to discharge him.

*See Manuel v. State*, 932 So. 2d 1120 (Fla. 3d DCA 2006) (reversing conviction for possession of cocaine and ordering discharge upon finding that trial court erred in denying motion to suppress, and prosecution's trial evidence was result of illegal seizure).

## II. THE COURT ERRED IN DENYING THE MOTION TO SUPPRESS BECAUSE THE WARRANT AND AFFIDAVIT WERE BASED ON AN ILLEGAL SEARCH.

Appellant contended below that Det. Pherson conducted a warrantless search when, without a warrant, he opened the attachments in order to determine whether they contained child pornography. R 320-21. At the hearing, counsel pointed out to the court that the motion had been amended to include this issue. R 780. By denying suppression, the court necessarily denied this issue, although its order did not directly address it.

The prosecution bears the burden to prove the lawfulness of warrantless searches. *State v. K.C.*, 207 So. 3d 951, 953 (Fla. 4th DCA 2016) (holding warrantless search of defendant's cellphone was illegal).

Det. Pherson received two cyber tips from NCMEC that child pornography had been downloaded via Appellant's online accounts. R 1111, 1113, 1120. Such cyber tips are routinely generated through an automated system generated via a hashtag indicating that an automated system, like Microsoft's PhotoDNA has detected that it contains child pornography. R 1112-13.

Pherson testified that the cyber tips did not tick the box show-

ing whether anyone at Facebook or NCMEC had actually viewed the suspect files. R 813.

His belief was that the tips were forwarded to him without anyone at Facebook or NCMEC looking at the images:

Q Okay. So as far as you know, between you, Facebook, and NCMEC, you're the first person that actually looked at the images?

A Again, I don't know whether or not they did or didn't because of the information I'm provided (unintelligible). But again, my suspect is that they flagged — since the hash values were identified, they forwarded it straight to NCMEC, then to me.

Q Okay. And you can't give us any better information than that they would at least be able to flag them. You can't tell us that they confirmed them the way you did by looking at them.

A Correct.

Q Is that fair?

A Yes.

R 813.

He opened the attachments in order to confirm that they were child pornography. R 796-97. He did this before obtaining the warrant — in fact the warrant was based on his observation of the attachments.

By opening the attachments, Pherson conducted a warrantless

search under the Fourth Amendment. *See United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) (opinion of then-Judge Gorsuch for the court) (finding that NCMEC's act of viewing email attachments is a search for Fourth Amendment purposes); *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021). (holding that detective's act of viewing email attachments was a warrantless search in violation of Fourth Amendment).

Appellant relied on *Wilson*, below. R 320-21. In that case, as in the present case, a cyber tip was forwarded to a law enforcement officer. The tip had been sent by Google to NCMEC based on, as at bar, a hash tag match with previously identified child pornography. *Id.* 13 F.4th at 964-65. The record showed that no Google employee viewed the images concurrently with submitting the tip to NCMEC. *Id.* at 965. NCMEC then forwarded the tip to a law enforcement officer, who looked at the images without a warrant. *Id.* at 965. The officer then obtained a warrant for Appellant's email account and found extensive further incriminating evidence. *Id.* at 965-66.

The prosecution did not dispute that the officer's inspection of the images constituted a warrantless search. It relied, however, on the "private search exception" — the doctrine that suppression is

not required where the government may use evidence discovered by a private party even if the private party's search would violate the Fourth Amendment if conducted by a government agent. *Id.* at 967.

The Ninth Circuit held that that exception could not benefit the prosecution in Wilson's case. It noted that the government had the burden to prove the application of the private search exception. *Id.* at 971. It noted further that the record showed that the officer went beyond any search conducted by Google when he opened the attachments, so that the exception could not apply, writing:

The government's argument to the contrary mischaracterizes the record, by representing that Google's scan "equates to a full-color, high-definition view" of Wilson's images. It does not. The critical fact is that no Google employee viewed Wilson's files before Agent Thompson did. When the government views anything other than the specific materials that a private party saw during the course of a private search, the government search exceeds the scope of the private search. That is the clear holding of *Jacobsen*. In that case, "[t]he field test ... had not been conducted by the Federal Express agents and therefore exceeded the scope of the private search." 466 U.S. at 122, 104 S.Ct. 1652 (emphasis added); *see supra* Part II.B.1.

*Id.* at 974. It noted further that there was a split among the federal circuits about application of the doctrine, but that Eleventh Circuit had reached a similar conclusion:

Further, in *United States v. Sparks*, 806 F.3d 1323 (11th Cir. 2015), *overruled on other grounds by United States v. Ross*, 963 F.3d 1056 (11th Cir. 2020), a store employee and her fiancé discovered child pornography on a lost cell phone and showed the phone to the police. The police officer ultimately viewed two videos on the cell phone, one of which the private parties “had not watched.” *Id.* at 1332. Because the government search exposed new information, not seen by the private party, the Eleventh Circuit concluded that the government search exceeded the scope of the private search.

*Id.* at 977 (footnote omitted).

The court held that the officer violated Wilson’s Fourth Amendment rights “when he examined Wilson’s email attachments without a warrant.” *Id.* at 980. Hence, it vacated Wilson’s conviction and reversed the denial of his motion to suppress. *Id.*

In the present case, there was an illegal warrantless search when the officer opened the attached images. The prosecution did not prove the search was lawful. Accordingly, the court erred in denying the motion to suppress and the conviction and sentence should be reversed. Further, because the prosecution case depended entirely on evidence resulting from the search, the convictions should be reversed, and the case should be remanded with instructions to discharge him. *See Manuel v. State*, 932 So. 2d 1120 (Fla. 3d DCA 2006) (reversing conviction for possession of cocaine and

ordering discharge upon finding that trial court erred in denying motion to suppress, and prosecution's trial evidence was result of illegal seizure).

It is true that in *Barnes*, this Court noted that the prosecutor had a history of prior instances of improper conduct. *Id.* But that fact could hardly have been dispositive. The important point is whether the improper argument goes directly to the principle issue in the case, to the heart of the defense.

As in *Barnes*, the evidence was close and the improper argument went to the very core of the case against Appellant. In these circumstances, a new trial should be ordered.

V. THE CONVICTION SHOULD BE REVERSED BECAUSE APPELLANT WAS TRIED BY A SIX-MEMBER JURY IN VIOLATION THE DUE PROCESS AND JURY CLAUSES OF THE FEDERAL CONSTITUTION.

Florida allows trial by a jury of six in non-capital cases. Art. I, § 22, Fla. Const.; § 913.10, Fla. Stat. Accordingly, this case involved a trial by a jury of six rather than twelve members. T 169-70. Appellant contends that the Due Process, Privileges and Immunities, and Jury Clauses of the federal constitution require a jury of twelve, so that structural, fundamental error occurred because he was deprived of this right. Amend. VI, XIV, U.S. Const. He acknowledges contrary authority, as discussed below. He further acknowledges that the Supreme Court recently denied review of this

issue over Justice Gorsuch's dissent. *Cunningham v. State*, 144 S. Ct. 1287–88 (2024) (Gorscuch, J., dissenting from denial of certiorari).

*Williams v. Florida*, 399 U.S. 78 (1970), held that state court juries as small as six were constitutionally permissible, despite the determination in *Thompson v. Utah*, 170 U.S. 343, 349–50 (1898), that the jury guaranteed by the Sixth Amendment consists “of twelve persons, neither more nor less.”

*Thompson* held that the Sixth Amendment enshrined the right to a jury of twelve as provided at common law. *Id.* at 349–50. In addition to the authorities cited there, one may note that Blackstone stated that the right to a jury of twelve is even older, and more firmly established than the unqualified right to counsel in criminal cases. 4 William Blackstone, *Commentaries on the Laws of England*, ch. 27 (“Of Trial and Conviction”).<sup>4</sup> Blackstone traced the right back to ancient feudal right to “a tribunal composed of twelve good men and true,” and wrote that “it is the most transcendent privilege which any subject can be enjoy or wish for, that he cannot

---

<sup>4</sup> Found at <https://lonang.com/wp-content/download/Blackstone-CommentariesBk4.pdf>

be affected in his property, his liberty or his person, but by the unanimous consent of twelve of his neighbours and equals.”<sup>3</sup> Blackstone, ch. 23 (“Of the Trial by Jury”).<sup>5</sup>

Thus, at the time of the amendment’s adoption, the essential elements of a jury included “twelve men, neither more nor less.” *Patton v. United States*, 281 U.S. 276, 288 (1930).

*Williams* itself has now come into question in light of *Ramos v. Louisiana*, 140 S. Ct. 1390 (2020), which concluded that the Sixth Amendment’s jury requirement encompasses what the term “meant at the Sixth Amendment’s adoption.” *Id.* at 1395. (Of course, the requirement that the jury be composed of men has been overturned by a subsequent amendment – the Equal Protection Clause of the Fourteenth Amendment. *See J.E.B. v. Alabama ex rel. T.B.*, 511 U.S. 127, 146 (1994).

In this case, Appellant did not receive a trial by a jury as the term was meant at the Sixth Amendment’s adoption, or at the time of the Fourteenth Amendment’s adoption for that matter, as he was not tried by a jury of twelve. The undersigned acknowledges that

---

<sup>5</sup> Found at <https://lonang.com/wp-content/download/Blackstone-CommentariesBk3.pdf>

this Court has rejected this argument. *Guzman v. State*, 350 So. 3d 72 (Fla. 4th DCA 2022), *rev. denied* SC2022-1597 (Fla. June 6, 2023), *cert. denied* No. 23-5173 (U.S. May 28, 2024). He further acknowledges that section 913.10, Florida Statutes, provides for six person juries in all non-capital criminal cases, and that this provision is authorized by Article I, section 22 of the Florida Constitution.

Appellant raised this issue by written motion arguing he was entitled to a 12-member jury under the Sixth and Fourteenth Amendments. R 498-502. The defense argued the motion when the case came up for trial, and the court denied the motion and said that Appellant was preserving the issue for appeal. ST 6-8. Counsel then again raised the issue, and the court again refused to allow a 12-member jury. T 20-21.

Even if the defense had not raised the issue, the error is fundamental and structural, as the conviction arose from a sheer denial of a fundamental constitutional right. Waiver of the constitutional right of trial by the proper number of jurors must be made personally by the defendant. *See Blair v. State*, 698 So. 2d 1210, 1217 (Fla. 1997) (finding valid defendant's agreement to verdict by five-

member jury valid when made “in a colloquy at issue here, including a personal on-the-record waiver,” and sufficient to pass muster under the federal and state constitutions,” and his decision was made “toward the end of his trial, after having ample time to analyze the jury and assess the prosecution's case against him. He affirmatively chose to proceed with a reduced jury as opposed to a continuance or starting with another jury.”). A new trial should be ordered.

## ARGUMENT

Due to word-count constraints, Appellant's reply is limited to the following:

### I. THE COURT ERRED IN DENYING THE MOTION TO SUPPRESS.

Appellee cites *State v. Leveque*, 530 So. 2d 512 (Fla. 4th DCA 1988). There the only question was whether the warrant extended to suspect premises beyond the door a single unit to an area that was also suspect.

Appellee cites *Clapsaddle v. State*, 545 So. 2d 946 (Fla. 2d DCA 1989), but it involved a minor error in the description. The warrant was for an apartment, but at three points it referred to the place to be searched as a "vehicle." This error was insignificant because the warrant repeatedly made clear that an apartment was to be searched: "The descriptive portion of the warrant uses the terms 'apartment,' 'structure,' 'duplex,' 'complex,' or 'unit' a total of fourteen times. There is no question that a structure, not a vehicle, is to be searched." *Id.* at 948 (emphasis added). Also the officer who obtained the warrant was the one who executed it. *Id.* at 947. The court limited the decision to the facts. *Id.* at 948-49.

Appellee cites *Carr v. State*, 529 So. 2d 805 (Fla. 1st DCA 1988). There, as in *Clapsaddle* — unlike at bar — the apartment to be searched was accurately described except as to an error in the apartment number. *Id.* at 806. Also unlike at bar, the officers executing the warrant had maintained a lengthy surveillance and knew which apartment was to be searched. *Id.* The First District wrote: “An inaccuracy in the warrant, such as an incorrect address or apartment number, does not invalidate the warrant if the place to be searched is otherwise sufficiently identified in the warrant.” *Id.* (emphasis added). At bar, the place to be searched was identified in the warrant as the Angola Circle house, not Appellant’s house.

*Carr* is like *State v. Hauser*, 364 So. 2d 823 (Fla. 2d DCA 1978), which was discussed at page 35 of the initial brief. *Carr* and *Hauser* involve minor errors in the identification of adjacent properties, and have no bearing here where the warrant told the police to search a place miles from Appellant’s home.

Appellee cites *Bennett v. State*, 150 So. 3d 842 (Fla. 4th DCA 2014) (opinion on rehearing). *Bennett* was discussed at pages 31-35 of the initial brief, and there is no need to repeat that discussion here. It is sufficient to say that, like *Carr* and *Hauser*, it involved a

minor discrepancy in the address where the warrant made clear the property to be searched.

Appellee relies on *United States v. Abdalla*, 972 F.3d 838 (6th Cir. 2020), and *United States v. Turner*, 770 F.2d 1508 (9th Cir. 1985). Those cases do not help Appellee. In both—unlike at bar—the warrant would lead an officer unerringly to the right place and the it was executed by an officer who was familiar with the place.

In *Abdalla*, the warrant listed the correct and an incorrect address, but that is where the similarities to the present case end. Unlike at bar, the *Abdalla* warrant accompanied the correct address with detailed “step-by-step directions along with a detailed description of Abdalla’s residence. So the warrant’s singular incorrect address posed almost no chance of a mistaken search.” *Id.* 972 F.3d at 842. Further—unlike at bar—the agent who prepared the affidavit led officers directly to Abdalla’s house, and “an executing officer’s knowledge may be a curing factor.” *Id.* at 843, 846-47. These facts were crucial to the court’s decision:

All in all, the warrant (1) provided detailed directions to Abdalla’s New Hope Road address, (2) described a “white double wide trailer with a green front porch and a black shingle roof,” along with an American flag on the front porch and an “auto detail sign” in the driveway, and (3)

identified the correct address and county, except for one sentence on the final page. (R. 20-1, Search Warrant, Page ID # 57, 59.) It is nearly unfathomable, given those particular identifiers and Agent Gooch's familiarity with the residence, that officers would have arrived at an incorrect address and then found a residence so resembling the warrant's description that they would have performed a mistaken search. So we are unpersuaded by Abdalla's claim that the warrant failed to describe his residence with particularly and granted officers overly broad authority to search multiple residences.

*Id.* at 847.

The present case is not like *Abdalla*. Here, the warrant (1) provided detailed directions to an Angola Circle residence — miles from Appellant's Perry Avenue house, R 1140; (2) gave a detailed description of the Angola Circle residence as the place to be searched, R 1140; and (3) merely cited Appellant's address with a photograph without detailed directions or a detailed description, R 1139; and (4) the detective did not himself execute the warrant. R 828.

In *Turner*, unlike at bar, the warrant described the place to be searched with great particularity, and the warrant was executed by an officer who participated in applying for the warrant and personally knew the premises to be searched. *Id.* 770 F.2d at 1511. As discussed above, the directions and description at bar were for a residence miles from Appellant's home, and the detective who pre-

pared the warrant and conducted the surveillance did not execute the warrant, which was executed by the SWAT team.

Appellee cites *State v. Carson*, 482 So. 2d 405 (Fla. 2d DCA 1985). There “[t]he blank space on the warrant and affidavit for the description of the premises to be searched contained the following: ‘See Exhibit ‘A’ which is attached and made a part hereof.’ Exhibit A described in detail the premises to be searched.” *Id.* at 406. Hence, the warrant was valid because it expressly incorporated the accurate description of the place to be searched and it contained no erroneous description of a different place. The warrant at bar did not incorporate the affidavit, and it contained detailed directions to, and a detailed description, of a place miles from Appellant’s home. It did not order the officers to enter and search Appellant’s home.

Appellee also cites *State v. Kingston*, 617 So. 2d 414 (Fla. 2d DCA 1993). There the warrant did not describe the place to search but referred three times to the affidavit, and it did not describe a completely different place as the place to be searched. The warrant in the present case referred to the affidavit, but it specifically identified the Angola Circle property as the place to be searched.

Further, the Second District wrote that the “good faith” excep-

tion of *United States v. Leon*, 468 U.S. 897 (1984), applied to the facts. Under *Leon*, this exception does not apply if the warrant is “so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.” *Id.* at 923 (emphasis added).

At bar, an executing officer could not reasonably presume that the warrant — which particularly described the Angola Circle house as the place to be searched — would be valid for searching the Perry Avenue house. *Cf. United States v. King*, 227 F.3d 732, 753–54 (6th Cir. 2000) (holding good faith exception did not apply to search of basement of duplex where warrant referenced apartment but did not reference the basement despite officer’s belief that search of basement was allowed).

Moreover, the “good faith” exception cannot apply where the error is caused by the officer rather than in the magistrate’s determination of probable cause. *See Groh v. Ramirez*, 540 U.S. 551, 564 (2004) (“because petitioner himself prepared the invalid warrant, he may not argue that he reasonably relied on the Magistrate’s assurance that the warrant contained an adequate

description of the things to be seized and was therefore valid.”). *See also Finch v. State*, 479 So. 2d 1314, 1319 (Ala. Crim. App. 1985). (“because the error in the identification of the address was due to the police officer’s ‘mental error’, and not an error on the part of the issuing magistrate, the good faith exception does not apply”).

As to good faith, it must also be noted that Det. Pherson admitted at the suppression hearing to omitting from the affidavit the fact that he had subpoenaed AT&T records in Appellant’s name in the effort to confirm uploads reported in the cypertip, R 790, 791, 799-801, 819, and AT&T responded that no information was available. R 791. (Specifically, AT&T responded: “After conducting a thorough search on all identifiers listed in the legal demand, AT&T was unable to identify any information responsive to the Legal Demand.” R 1102.) After receiving AT&T’s negative response, he did no follow-up with AT&T. R 820, 822. He admitted that he intentionally omitted this information from the warrant affidavit. R 822. This fact also negates any claim of good-faith.

Appellee also cites *United States v. Garcia*, 707 F.3d 1190 (10th Cir. 2013). There, an officer applied for a warrant to search Garcia’s residence, which did not have an address. His affidavit

contained a description and photograph of the residence, but incorrectly stated it had a specific address on Mescalero Street. The judge signed a warrant to search the place “described in the Affidavit.” *Id.* at 1193-94. After receiving the warrant but before executing it, Agent Mirabal went to the area with the affidavit’s author, who identified for him the place to be searched. *Id.* The court held that suppression was not required because: “The photograph and description of Garcia’s home in the affidavit, combined with the knowledge of the agents involved, enabled the executing officers to locate the premises without difficulty or confusion and virtually eliminated the possibility of searching the wrong residence.” *Id.* at 1997 (emphasis added). In the present case, the warrant described a completely different place, told the police to search that different place rather than the place in the affidavit, and the author of the affidavit did not go with the executing officers to Appellant’s residence.

The answer brief seeks to use a statement in *Carr* that a residence may be described by its occupants, but that case involved the misidentification of the apartment number in a small three-unit building. It does not affect this case, where the warrant identified

the place to be searched as being on Angola Circle miles from Appellant's home, provided detailed directions to the Angola Circle house, and described the Angola House in detail. The warrant said the Angola Circle house was Appellant's. R 1140.

*State v. Gallo*, 279 So. 2d 71, 72 (Fla. 2d DCA 1973), which is also cited by Appellee, is similar to *Carr* — it involves a minor misidentification of the apartment number.

Finally, the answer brief makes a cursory claim under the good-faith exception, citing *U.S. v. Watson*, 498 F.3d 429 (6th Cir. 2007). *Watson* involved a warrant to search a residence and four persons believed to be in it. The warrant “comprehensively described the residence as well as the four individuals to be searched. Moreover, maps of the area, a tax-assessment printout, and photographs of the residence were all attached to the warrant. The warrant, however, listed only the four individuals in its grant-of-authority section and inexplicably omitted the residence.” *Id.* at 430.

The court “assum[ed] without deciding, that the warrant’s omission of the residence from the grant-of-authority section rendered the warrant invalid as to a search of the residence,” and

then considered whether the good-faith exception applied. *Id.* at 431.

It wrote that, because the “warrant’s introductory paragraph put a reasonable officer on notice that the warrant was issued for the purpose of searching a premises,” the warrant described “the residence in painstaking detail,” and the grant-of-authority section referred to the residence, the omission was “virtually unnoticeable.”

*Id.* at 432.

The present case is totally different. Here, the warrant gave painstaking directions to a completely different residence on Angola Circle miles from Appellant’s home. Further, it described this Angola Circle residence to be searched as a gray and tan house and a different house number in a different location on the property from Appellant’s green house. R 1140 (description of Angola Circle house in warrant); R 1108 (description of Appellant’s house in affidavit).

This case does not involve a “virtually unnoticeable” omission — the error is conspicuous and obvious. *See Leon*, 468 U.S. at 923 (“[A] warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be

valid.”), *Groh*.

The guide here is the Constitution. The Fourth Amendment provides: “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” Amend. IV, U.S. Const. (emphasis added). Article I, Section 12 of our constitution provides: “ No warrant shall be issued except upon probable cause, supported by affidavit, particularly describing the place or places to be searched, the person or persons, thing or things to be seized, the communication to be intercepted, and the nature of evidence to be obtained.” (Emphasis added.)

The Supreme Court has determined that Webster’s 1828 dictionary is a reliable guide as to the meaning of terms in the Bill of Rights. *See Crawford v. Washington*, 541 U.S. 36, 51 (2004).

Webster defined “Particularly” as follows:

**PARTIC'ULARLY**, *adverb* Distinctly; singly.

**1.** In an especial manner.

This exact propriety of Virgil I *particularly* regarded as a great part of his character.

<https://webstersdictionary1828.com/Dictionary/particularly> (underlining added; italics in original);

<https://archive.org/details/in.ernet.dli.2015.83674/page/n242/mode/1up> (facsimile of original).

Here, the warrant did not identify Appellant's Perry Avenue home distinctly and singly. It identified two residences miles apart; it distinctly and singly described the other residence as Appellant's property to be searched.

These constitutional provisions act as a restraint on Appellee. Naturally, Appellee fights to be free of that restraint. In its struggle, Appellee would have the Particularity Clause die by a death of a thousand cuts.

But it is the Constitution that must be heeded, not the wishes of the government straining against the leash. The courts must apply with Constitution as written without fail. "Constant competition between constable and quarry, regulator and regulated, can come as no surprise in our changing world. But neither should the proper role of the judiciary in that process—to apply, not amend, the work of the People's representatives." *Henson v. Santander Consumer USA Inc.*, 582 U.S. 79, 90 (2017). Under the plain terms of the constitutional language, the warrant in this case was invalid.

II. THE COURT ERRED IN DENYING THE MOTION TO SUPPRESS BECAUSE THE WARRANT AND AFFIDAVIT WERE BASED ON AN ILLEGAL SEARCH.

The issue is preserved for appeal

Appellee argues the issue is not preserved. AB 10-11. Appellant must disagree.

The trial court denied the motion to suppress. Hence, it necessarily denied Appellant's arguments on the motion. *See Pagidipati v. Vyas*, 353 So. 3d 1204, 1212 n.3 (Fla. 2d DCA 2022) ("Although it did not expressly address the issue, the trial court appears to have agreed, as it ruled on the merits of the motion despite Mr. Vyas's pending challenge to standing.").

For example, in *Data Lease Fin. Corp. v. Barad*, 291 So. 2d 608 (Fla. 1974), the supreme court held that, although the judge did not expressly rule on the petitioner claim of waiver and estoppel he did generally rule against the petitioner, so that it must be presumed that the judge did reject petitioner's claim. *Id.* at 611.

Citing *Data Lease*, the Second District wrote in *Lopez v. Ernie Haire Ford, Inc.*, 974 So. 2d 517, 518 (Fla. 2d DCA 2008): "Additionally, the Lopezes argue that Ernie Haire waived its right to arbitrate, and that they did not knowingly, intelligently, and voluntarily

waive their jury trial right. The trial court did not elaborate its reasoning on the last two issues and the Lopezes did not seek a more specific ruling. However, the trial court implicitly found no waiver by Ernie Haire and that the Lopezes waived their jury trial right.”

Similarly, when an appellate court affirms without opinion, it necessarily rejects the issues advanced for reversal so that the law of the case rule applies to those issues. *See Chipman v. State*, 310 So. 3d 472, 473 (Fla. 2d DCA 2020).

The cases cited by Appellee are beside in the point. They did not involve a situation like at bar. Unlike in those cases, counsel specifically directed the court’s attention to the present argument at the suppression hearing, which the court acknowledged. R 780.

Thus, counsel preserved the issue by placing the court on notice of the issue and providing it the opportunity to rule on it. *See State v. T.G.*, 800 So. 2d 204, 210 (Fla. 2001), *Daniels v. State*, 121 So. 3d 409, 417 (Fla. 2013). Counsel preserved the issue by bringing the issue to the judge’s attention and “provid[ing] the judge an opportunity to respond to the objection.” *J.B. v. State*, 705 So. 2d 1376, 1378 (Fla. 1998).

The court erred in denying suppression

On the merits, Appellee relies on an unpublished federal trial court opinion from North Carolina. That opinion has no precedential value. Further, in that case — unlike at bar — a Google employee viewed many of the images and determined many of them were child pornography. *United States v. Lowers*, 5:22-CR-00178-M, 2024 WL 418626, at \*1 (E.D.N.C. Feb. 5, 2024). This private-party search triggered the private search doctrine, defeating Lowers' claim. In the present case, there the record does not show a private search before Pherson opened the attachments. Hence, the private search doctrine does not apply. *See United States v. Ackerman*, 831 F.3d 1292, 1308 (10th Cir. 2016) (*Ackerman I*) (opinion of then-Judge Gorsuch for the court), *Walter v. United States*, 447 U.S. 649 (1980) (private search doctrine did not apply where, after company employee opened box containing obvious pornography and unsuccessfully attempted to view films, FBI agents exceeded private search by actually viewing the films).

The answer brief argues Appellant had the burden to show the search was illegal. AB 14-15. The record shows Pherson opened the attachments without a warrant. The prosecution bears the burden

to prove the lawfulness of warrantless searches. *State v. K.C.*, 207 So. 3d 951, 953 (Fla. 4th DCA 2016).; *Miles v. State*, 953 So. 2d 778, 779 (Fla. 4th DCA 2007) (“The initial burden on a motion to suppress an illegal search is on the defendant to make an initial showing that the search was invalid. When that *prima facie* showing is made, however, the burden shifts to the state to prove that the search is valid.”).

The answer brief cites *United States v. Reddick*, 900 F.3d 636 (5th Cir. 2018), but that case’s interpretation of the private search doctrine is contrary to the Supreme Court’s decision in *Walter* and to Justice Gorsuch’s opinion for the Tenth Circuit in *Ackerman*.

Appellee cites *United States v. Simpson*, 904 F.2d 607 (11th Cir. 1990), but there — unlike at bar — the government search did not exceed the scope of the search by FedEx. See *United States v. Sparks*, 806 F.3d 1323, 1336 (11th Cir. 2015) (“Nothing in *Simpson* provides a safe harbor for a governmental search of materials beyond the scope of a private search.”).

Again citing the trial court decision in *Lowers*, Appellee makes a cursory claim of good faith under *Leon*. Appellee’s argument is based on the fact that the providers were statutorily obligated to

make disclosure to the government and that, somehow, Pherson relied on that fact to view the attachments without a warrant.

This argument derives from the unpublished Tenth Circuit opinion after remand in *Ackerman*. *United States v. Ackerman*, 804 Fed. Appx. 900 (10th Cir. 2020) (*Ackerman II*) (opinion of then-Judge Gorsuch for the court). The issue there was whether the search by NCMEC and not the government search —fell within the good faith exception because NCMEC was obligated by statute to receive and review child pornography. *Id.* at 904.

The Tenth Circuit relied on *Illinois v. Krull*, 480 U.S. 340 (1987), which concerned a warrantless administrative search of automobile wrecking yard records as part of “a comprehensive statutory scheme regulating the sale of motor vehicles and vehicular parts.” *Id.* at 342. The Court applied the good faith doctrine even though the statute authorizing the search was found unconstitutional because “this Court has upheld legislative schemes that authorized warrantless administrative searches of heavily regulated industries.” *Id.* at 357. *Krull* did not alter the fact that *Leon*’s good-faith doctrine does not apply to non-administrative searches, such as the investigative search here. “We have held, however, that the

exclusionary rule requires suppression of evidence obtained in searches carried out pursuant to statutes, not yet declared unconstitutional, purporting to authorize searches and seizures without probable cause or search warrants. *See, e.g., Ybarra v. Illinois*, 444 U.S. 85 (1979); *Torres v. Puerto Rico*, 442 U.S. 465 (1979); *Almeida-Sánchez v. United States*, 413 U.S. 266 (1973); *Sibron v. New York*, 392 U.S. 40 (1968); *Berger v. New York*, 388 U.S. 41 (1967).” *Leon*, 468 U.S. at 913 n.8. The cases cited at that point in *Leon* applied the exclusionary rule to statutory non-administrative searches. The case here involves an investigatory search, not an administrative search, so that *Krull* does not apply.

Finally, the record does not show NCMEC personnel opened the attachments, so there can be no claim of good faith reliance on any search by NCMEC.

### III. THE COURT ERRED IN DENYING APPELLANT’S MOTION FOR JUDGMENT OF ACQUITTAL.

As to the fact that there were multiple possible suspects at the house with access to the computer, Appellee says this fact “goes to the weight of the evidence and that the jury was free to consider the credibility and reasonableness of this. *See S.M. v. State*, 150 So. 3d