AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of South Carolina

United States of America
v.

JAMES BENJAMIN GOSNELL, JR.

Defendant(s)

Case No. 2:25-mj-68

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of September 16, 2025 in the county of Charleston in the _____ District of South Carolina, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. Section 2252A	Possession of Materials Containing Child Pornography

This criminal complaint is based on these facts:

See Affidavit of Homeland Security Investigations (HSI) Special Agent Kyle Tallio, dated September 16, 2025

☑ Continued on the attached sheet.

KR

Complainant's signature

Kyle Tallio, HSI Special Agent

Printed name and title

Sworn to me via telephone or other reliable electronic means and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: 09/16/2025

Molly H. Cherry

Judge's signature

City and state: Charleston, South Carolina Hon. Molly H. Cherry, U.S. Magistrate Judge

Printed name and title

Print Save As... Attach Reset

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
CHARLESTON DIVISION

UNITED STATES OF AMERICA	)	
	)	Criminal No.: 2:25-mj-68
	)	
vs.	)	
	)	
	)	
JAMES BENJAMIN GOSNELL, JR.	)	
	)	

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Special Agent ("SA") Kyle Tallio, hereinafter "Affiant," being first duly sworn, hereby depose and state as follows:

A. Introduction

1. I am an SA with the Department of Homeland Security Investigations ("HSI") and have been since 2018. Affiant knows it is a violation of federal law for a person to knowingly, receive, access, or possess any child pornography using any means or facility of interstate or foreign commerce, including by computer. I also have personally participated in multiple investigations related to child exploitation and Child Sexual Abuse Material ("CSAM").

2. This affidavit is submitted in support of a criminal complaint against **James Benjamin Gosnell, Jr.** (DOB: [redacted]) for violations of Title 18, United States Code, Section 2252A(a)(5)(B) (Certain activities relating to material constituting or containing child pornography). I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probably cause to issue the requested arrest warrant.

B. Target Offense

3. I respectfully submit there is probable cause to believe GOSNELL violated 18 2252A(a)(5)(B), which prohibits an individual from knowingly possessing any child pornography using any means or facility of interstate or foreign commerce, including by computer. Based on my training and experience, I know that § 2252A(a)(5)(B) is violated when the following elements are satisfied:

a. First, that the defendant possessed or accessed with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contained an image of child pornography;

b. Second, that had been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or was produced using materials that had been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

c. Third, that the defendant acted knowingly.

4. "Child Pornography" (as defined in 18 U.S.C. § 2256(8)) as is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

5. "Computer" is defined as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

C. Facts and Circumstances Supporting Probable Cause

National Center for Missing and Exploited Children CyberTipline Report #203155592

6. In December 2024, a financial technology company that facilitates peer to peer online money transfers ("Financial Technology Company 1"), filed a National Center for Missing and Exploited Children (NCMEC) CyberTipline Report #203155592 ("the NCMEC CyberTip"), identifying concerns that transactions to a collection of approximately fifty United Kingdom based accounts associated to one person ("the suspected CSAM vendor") were for the purchase of CSAM. The NCMEC CyberTip identified more than one hundred accounts ("the suspected CSAM purchaser") which sent money to the suspected CSAM vendor's accounts, which was believed to be for the purchase of CSAM based on Financial Technology Company 1's review of transaction comments, messages, and publicly available criminal history information regarding the suspected CSAM purchasers.

7. A review of additional law enforcement records identified an additional portion of the suspected CSAM purchaser accounts had criminal history relating to prior possession of CSAM. Open-source reporting that the suspected CSAM vendor was arrested by foreign law enforcement after they were identified as having "made and distributed thousands of indecent images of children." The suspected CSAM vendor was identified as funding his lifestyle by selling "indecent material" "of children on the internet using various social media and storage platforms." The suspected CSAM vendor

"set up a large number online payment accounts through which he had received thousands of pounds for the indecent material."

The James GOSNELL Accounts

8. Law enforcement conducted a review of a Financial Technology Company 1 account held in the name "James GOSNELL" with account number ending in 9731 ("the GOSNELL account ending in 9731"), which was identified as a the suspected CSAM purchaser in the NCMEC CyberTip.

9. The GOSNELL account ending in 9731 was created on November 4, 2024, and lists a primary street address of [redacted] Charleston, SC 29407, the email address [redacted]@aol.com, and the phone number "1 843[redacted]". The GOSNELL account was created from IP address "45.22.6.151" on November 4, 2024.

10. The suspected CSAM purchaser account was identified as James Gosnell, a Charleston County Magistrate.

11. The GOSNELL account ending in 9731 was the payor on two November 4, 2024, transactions to a single account held by the suspected CSAM vendor for approximately $100. The transactions occurred on November 4, 2024, between 4:38pm EST and 4:44pm EST. Both transactions had a transaction note "vid". There were no additional transactions conducted by the GOSNELL account ending in 9731. On December 20, 2024, the GOSNELL account ending in 9731 placed a hold on both transactions,[1] reporting that it was unauthorized. Based on this Agent's training, experience, and conversation with other law enforcement officers, it is understood that individuals who purchase CSAM online often are purchasing login credentials to a file sharing site. As a result, CSAM vendors have little recourse in instances where the CSAM buyer reports the transaction as fraudulent, even if the exchange

[1] As discussed below in paragraph 16, there was also correspondence from the suspected CSAM vendor account to the GOSNELL account ending in 9731 on November 5, 2024, regarding the processing of refunds.

of the login information actually occurred. I am also aware of a report that collectors of child pornography sometimes reverse payments made to child pornography vendors if the product the collector receives is unsatisfactory.

12. November 4, 2024, falls within the timeframe that the suspected CSAM vendor accounts were accepting payments linked to the suspected sale and distribution of child pornography.

13. Law enforcement databases identified IP address "45.22.6.151" as resolving back to the net range of AT&T. A Customs Summons was served on AT&T. AT&T provided subscriber information indicating IP address "45.22.6.151" was associated with "JAMES Gosnell" with service and billing addresses of [redacted] Charleston, SC 29407, the email address [redacted]@AOL.COM, and the phone number "843[redacted]".

14. James Gosnell has no other known connection to the suspected CSAM vendor.

15. The suspected CSAM vendor account which GOSNELL conducted transactions with had transactions with five additional accounts which were identified as suspects of the NCMEC CyberTip. Two of these accounts had specific indicators of CSAM distribution:

a. One of the suspected CSAM purchaser accounts was associated with notes on a separate transaction which indicated it likely related to CSAM distribution.

b. An additional suspected CSAM purchaser account was arrested in June 2025 for CSAM related offenses.

Investigative Steps regarding the suspected CSAM vendor's accounts at Financial Technology Company 1

16. On September 8, 2025, in District of South Carolina case number 2:25-cr-1063, a search warrant was obtained for information, including but not limited to, the content of messages and/or transaction comments of the suspected CSAM vendor accounts. The following was identified through a review of the search warrant return:

a. Portions of the return, including messages and transactions comments, identified that the transactions may be based on communications through encrypted messaging applications and supported the belief that transactions to the suspected CSAM vendor accounts related to the purchase of CSAM.

b. On November 5, 2024, (the day following the aforementioned transaction from GOSNELL to the suspected CSAM vendor account) a CSAM vendor account sent a message to the GOSNELL account ending in 9731, "Hi i have finally sorted refunds but because you sent 2 identical payments have delayed it by 72hrs so will just havr to wait. least they are on the way back now :)". As was previously discussed, the GOSNELL account later identified these transactions as unauthorized.

c. On November 4, 2024, a second account in the name "james Gosnell" with an account number ending in 4954 ("the GOSNELL account ending in 4954") was identified as having attempted three transactions with an additional CSAM vendor account. The transactions occurred on November 4, 2024, between 5:32 pm EST and 5:34 pm EST (shortly after the transactions with the GOSNELL Account ending in 9731, which were previously discussed in paragraph 11). The transactions were for $50, $80, and $103.45. All three transactions listed the subject "Games". All three attempted transactions had the status "Denied_Cancelled"[2]. The GOSNELL account ending in 4954 was not previously identified as a suspect account in the NCMEC CyberTip. The second CSAM vendor account was previously identified as a suspect account in the NCMEC CyberTip. A review was

[2] Based on my review of Financial Technology Company 1's Help Center, I understand that transactions can be denied for a variety of reasons, including but not limited to, because the source financial institution declines a transaction, an account is limited while under a review by Financial Technology Company 1, or because details have not been confirmed.

conducted of the GOSNELL account ending in 4954, which indicated the account was created on October 11, 2021, and lists a primary street address of [redacted] Charleston, SC 29407 (i.e., the PREMISES), a secondary email address of [redacted]@aol.com, and no phone number. The GOSNELL account ending in 4954 does not list a login IP address. The account is sourced from the same credit/debit card number as the GOSNELL account ending in 9731.

17. For the reasons articulated above, affiant believed there was probable cause that GOSNELL is the individual who conducted transactions with a child pornography vendor.

Identification of the Residence

18. A search of a commercial database that provides names, dates of birth, addresses, associates, telephone numbers, email addresses, and other information was conducted for GOSNELL. These public records indicated that GOSNELL's current address is [redacted] Charleston, SC 29407 ("PREMISES).

19. A check with the South Carolina Department of Motor Vehicles on or about July 31, 2025, revealed that an individual named James Benjamin GOSNELL Jr with a date of birth of [redacted], resides at the PREMISES.

20. On or about March 10, 2016, GOSNELL applied for a United States passport, where he listed a home address of [redacted] Charleston, SC ("PREMISES"), and listed a phone number of 843[redacted].

21. On or about July 25, 2025, GOSNELL departed the United States on an American Airlines flight from Philadelphia, PA to Amsterdam, Netherlands. A review of records relating to GOSNELL's reservation indicates that email address [redacted]@AOL.COM" and phone number 843-[redacted] are associated with the reservation.

22. On August 7, 2025, I conducted surveillance of the PREMISES. I observed a white Kia sports utility vehicle with South Carolina registration [redacted] parked in the driveway. A review of South Carolina Department of Motor Vehicles records relating to South Carolina registration [redacted] indicates the vehicle is registered to James Benjamin GOSNELL Jr at the PREMISES. I also saw a male walking a dog on the lawn of the PREMISES and then on the street in the vicinity of the PREMISES who appeared to be GOSNELL based on a review of photos of GOSNELL in law enforcement photos.

23. On September 15, 2025, in District of South Carolina case number 2:25-cr-1101, the Honorable Molly H. Cherry authorized the search of the property located at [redacted], Charleston, SC 29407, and electronic devices within.

24. On September 16, 2025, members of law enforcement and I executed the federal search warrant based on probable cause presented in the affidavit in support of the search warrant. GOSNELL answered the door in response to law enforcement's knock. I advised GOSNELL that law enforcement was executing a search warrant in furtherance of an investigation of CSAM. After advising GOSNELL of his Miranda rights in writing and verbally, GOSNELL advised that CSAM could be found on a thumb drive connected to a laptop in his front bedroom. GOSNELL believed he received the thumb drive from "a guy in Charleston" he met online approximately six or seven years ago. According to GOSNELL, the thumb drive contained "100s" of "videos" of "child porn."

25. GOSNELL advised that he used email addresses [redacted]@aol.com and [redacted]@aol.com. GOSNELL advised that he recalled his account at Financial Technology Company 1 was "hacked" on a particular occasion. GOSNELL indicated that he was "hacked" after attempting to send money for the purchase of CSAM and adult pornography, and that his credit card

was used in the United Kingdom and the Netherlands. GOSNELL advised that he did not receive CSAM on this occasion.

26. Numerous electronic devices were located during the execution of the search warrant. A particular USB Flash Drive titled "dropper" was located plugged into a laptop within the residence. During a preview of the USB Flash Drive titled "dropper", numerous files containing CSAM were located. Three particular files contained USB Flash Drive titled "dropper" are described as:

a. Image "y (22).jpg": This file was last written April 24, 2018, and was last accessed August 12, 2025. This image depicts the vaginal penetration of an infant less than one year old by an explicitly phallic device. A pacifier is visible in the infant's mouth. There appear to be ropes tied around the infant's wrist and ankles.

b. Image "HAEO3124.jpg": This file was last written June 4, 2018, and was last accessed September 6, 2025. This image depicts a male less than three years old with his legs tied to a protruding piece of furniture in a manner to further expose the anus and genitals. The anus and genitals are the focal point of the photo.

c. Image "bl (684).jpg": This file was last written April 24, 2018, and was last accessed September 10, 2025. This image depicts a prepubescent male performing oral sex on an adult male's erect penis.

27. The USB Flash Drive is a Sandisk Cruzer Glide model with a 16GM capacity. Sandisk is a California corporation, and the specific USB Flash Drive containing the images described above in Paragraph 26 was manufactured in China.

D. Conclusion and Requested Authority

28. Based on the above, I respectfully submit that there is probable cause to believe that **James GOSNELL** did commit violations of Title 18, United States Code, § 2252A(a)(5)(B) (Certain activities relating to material constituting or containing child pornography). In consideration of the foregoing, I respectfully request that this Court issue an arrest warrant for **James GOSNELL**.

Further your Affiant sayeth not.

Affidavit Reviewed by Assistant United States Attorneys Whit Sowards and Emily Limehouse.

KTR

Special Agent Kyle Tallio
Homeland Security Investigations

SWORN TO ME VIA TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS AND SIGNED BY ME PURSUANT TO FED. R. CRIM. P. 4.1 AND 4(d) OR 41(d)(3), AS APPLICABLE

Subscribed and sworn before me on

September 16, 2025

Molly H. Cherry

The Honorable H. Molly Cherry
United States Magistrate Judge