

AO 91 (Rev. 08/09) Criminal Complaint

**FILED****UNITED STATES DISTRICT COURT**

JUL 25 2025

for the

Northern District of Oklahoma

Heidi D. Campbell, Clerk  
U.S. DISTRICT COURT

United States of America

v.

Case No.

*25-mj-637-MTS*Austin Sewell*Defendant(s)***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 March 22, 2025 to on or about July 24, 2025 in the county of Tulsa in the  
Northern District of Oklahoma, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. §§ 2252(a)(2) and (b)(1)	Receipt and Distribution of Child Pornography
18 U.S.C. §§ 2252(a)(4)(B) and (b)(2)	Possession of Child Pornography in Indian Country

This criminal complaint is based on these facts:

See Attached Affidavit

☒ Continued on the attached sheet.*Complainant's signature**TFO Matt Gray, HSI*  
*Printed name and title*

Sworn to before me and signed in my presence.

Date:

*7-25-2025*Mark T. Steele*Judge's signature*

City and state:

Tulsa, OKUnited States Magistrate Judge*Printed name and title*

**Affidavit in Support of an Arrest Warrant  
in the Northern District of Oklahoma**

I, Matt Gray, being duly sworn under oath, do hereby depose and state:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Federal Taskforce Officer as defined under Rule 41(a)(2)(C) and am authorized to request these search warrants because I am a government taskforce agent who is engaged in enforcing federal criminal laws and I am within the category of officers authorized by the Attorney General to request such a warrant.

2. I am a Detective and have been employed with the Tulsa County Sheriff's Office since January 2013. I am also a Task Force Officer (TFO) with the Department of Homeland Security Investigations (HSI), currently assigned to investigate crimes involving child exploitation. While so employed, I have investigated federal criminal violations related to child exploitation, attempted enticement and coercion and child pornography. I have received training in the area of child pornography and child exploitation and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I received training in the investigation of crimes involving the use of computers and the recovery of evidence from computers and computer-related storage devices. I have received focused child exploitation training covering topics such as interview techniques, undercover investigations, capturing digital evidence, correlations between child pornography and hands-on offenses, psychological and behavioral characteristics of sex offenders, and mobile

messaging platforms utilized by these types of offenders. Moreover, I am a Task Force Officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252, and 2422.

3. As part of my duties as a TFO, I investigate criminal violations relating to crime in Indian Country, to include Notice or Advertisement Seeking Child Pornography in violation of 18 U.S.C. §§ 2251(d)(1)(A) & 2251(e); Attempted Coercion and Enticement in violation of 18 U.S.C. § 2422(b); Receipt and Distribution of Child Pornography in violation of 18 U.S.C. §§ 2252(a)(2) and (b)(1); and Possession of Child Pornography in Indian Country in violation of 18 U.S.C. §§ 2252(a)(4)(A) and (b)(2).

4. I am familiar with the facts and circumstances of this investigation. The facts set forth in this affidavit are based on my personal observations, knowledge obtained from other law enforcement officers, my review of documents related to this investigation, conversations with others who have personal knowledge of the events and circumstances described herein, and a review of open-source information including information available on the Internet. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact I or others have learned during the course of this investigation.

5. It is my belief that **Austin SEWELL, DOB xx-xx-2000**, a United States citizen,, has violated 18, United States Code, Sections 2252(a)(2) and (b)(1)

(Receipt and Distribution of Child Pornography) and 18 U.S.C. 2252(a)(4)(A) and (b)(2) (Possession of Child Pornography in Indian Country) in that on or about March 22, 2025, through on or about July 24, 2025, he:, received or distributed at least one video of a minor male victim engaging in sexually explicit conduct and possessed files of child pornography within Indian Country.

6. SEWELL resides at 1204 N Garfield Ave., Sand Springs, OK. 74063, within the territorial boundaries of the Muscogee Creek Nation in the Northern District of Oklahoma. SEWELL is an enrolled member of the Muscogee Creek Nation, Citizen ID 64720.

#### **PROBABLE CAUSE**

1. On June 30, 2025, TFO Matt Gray received an Internet Crimes Against Children (ICAC) Cyber Tip (208057216) from the Oklahoma State Bureau of Investigation (OSBI) regarding an Electronic Service Provider (ESP), Kik, that showed a suspect/ subscriber residing in the Northern District of Oklahoma (NDOK) due to an AT&T U-Verse IP Address of "[REDACTED]" that the suspect used when logging into their Kik account on March 14, 2025, @ 06:34:58 UTC. This specific IP address checks back to Sand Springs, Oklahoma in the Northern District of Oklahoma.

2. The account was reported by Kik because the account showed "apparent child pornography". The Cyber Tip (208057216), which was reported by NCMEC on March 22, 2025, included the account holder's email address of [REDACTED] the account holder's Kik username of [REDACTED]

██████████ the account's ESP User ID of ██████████ and an AT&T U-Verse IP Address "██████████" that the account holder used when logging into their Kik account.

3. I was able to view the 9 reported images and videos reported in the Cyber Tip (208057216). One of the videos displayed a prepubescent boy ██████████

██████████  
██████████  
██████████ The other 8 videos in the Cyber Tip display prepubescent children engaged in sexually explicit conduct including a video of an adult male ██████████ a toddler.

4. On March 25, 2025, @ 08:07:43 UTC, Kik reported an additional Cyber Tip (208154411) in reference to the same subject who was using a different Kik username of ██████████ an ESP User ID of "██████████", and the identical AT&T U-Verse IP Address of "██████████". This Cyber Tip stated that the suspect uploaded 30 child sexual abuse material ("CSAM") videos and images. These two Cyber Tips were linked due to the suspect using the same Gmail address of coryindahouseOO@gmail.com and AT&T U-Verse IP Address of "108.254.143.251."

5. I know from my training and experience that when accounts are flagged for possessing CSAM images, the ESP will shut down the account and report said account. This requires the account holders to create a new account where they can be found linked by phone number, email and or IP addresses the suspect used to

create and use the new account.

6. I was able to view the 30 CSAM videos and images of associated with this Cyber Tip **(208154411)**. The reported CSAM consisted of toddlers to prepubescent boys and girls [REDACTED] by adult men and forced [REDACTED]

7. On June 17, 2025 @ 15:57:48 UTC, Kik reported an additional Cyber Tip **(214173556)** in reference to an account user with username [REDACTED] talking about how he sexually assaulted a 9-year-old girl who he was babysitting when he was 17 years old. In the Cyber Tip, Kik reported the basic user info of the suspect including the Kik username of [REDACTED] an ESP User ID of [REDACTED] and an email address of [REDACTED] This Cyber Tip was flagged by OSBI during their initial triage stage due to it being associated with 4 additional reported Kik Cyber Tips **(213171535, 212941369, 212839924, 212823197)**. Kik reported all 5 user accounts as using the same Gmail address of [REDACTED]

8. The first associated Kik Cyber Tip **(213171535)** was reported by Kik due to the account user uploading 1 CSAM video which displayed a prepubescent girl [REDACTED]. The second associated Kik Cyber Tip **(212941369)** was reported by Kik due to the account user uploading 1 CSAM video which displays a prepubescent girl [REDACTED]

9. The third associated Kik Cyber Tip **(212839924)** was reported by Kik due to the account user uploading 9 CSAM videos and 1 image, which displayed newborn babies to prepubescent boys and girls [REDACTED] After



reviewing Cyber Tip **212839924**, I was able to locate the AT&T U-Verse IP Address of "[REDACTED]" which was identical to the IP address associated with the other Cyber Tips (**208057216 & 208154411**) which utilized usernames [REDACTED]

10. The fourth associated Kik Cyber Tip (**212823197**) reported by Kik due to the account user uploading 21 CSAM images displayed prepubescent girls being [REDACTED] by adult men. All 5 Cyber Tips are connected due to the suspect using the same Gmail address of [REDACTED]

11. I was able to connect all 7 of the Cyber Tips reported by Kik by locating the identical AT&T U-Verse IP Address of "[REDACTED]". All 7 reported Cyber Tips, which utilized usernames [REDACTED] and [REDACTED] and email addresses [REDACTED] and [REDACTED], had the same IP address that the suspect used when logging into their Kik account.

12. On 7/ 14/ 25, I received the Kik search warrant return for account usernames of [REDACTED]. During the review of data located in the content folder within the return for username [REDACTED] I discovered multiple anime depicted CSAM images of prepubescent girls. Some of those images [REDACTED]

13. The CSAM videos initially reported in the CyberTip by Kik were

located on this return which included bondage and one video of toddler

[REDACTED] Another video showed a prepubescent girl [REDACTED]

[REDACTED]

14. During the review of the data, the same AT&T U-Verse IP address of [REDACTED] was located and used by the account holder. The messages showed the suspect, [REDACTED] creating groups for individual to join and informing them that the group has no limit, meaning you can post anything and talk about anything without fear of being reported by the users in the group.

15. The suspect goes on to inform the users that he is into [REDACTED] [REDACTED] meaning child sexual abuse material (CSAM).

On March 14, 2025, at approximately 07:11:54 UTC, the suspect tells another user [REDACTED] that he is a 17-year-old girl from Arizona but states the current time is 2:11am. I know from experience that the UTC is approximately 5 hours ahead of Central Standard Time during daylight saving hours which was on March 14, 2025.

16. This would place the suspect residing in Central Standard Time Zone. The state of Arizona is on Mountain Standard Time and would have placed the suspect's current time, 11 minutes after midnight, not 2:11am as he



stated. Also, the AT&T U-Verse IP address of [REDACTED] which was located and used by this suspect, checks back to the Sand Springs area of Oklahoma.

17. I was able to locate another conversation where the suspect talks about being 17 years old and [REDACTED] that he was babysitting. This is precisely the same conversation the suspect had in the reported Kik CyberTip (214173556). However, in that particular CyberTip, he was stating that he was a 17-year-old boy and [REDACTED] with a 9-year-old girl he was babysitting.

18. I know from my training and experience that predators who use online social media to collect CSAM and talk to other like-minded individuals that are interested in CSAM, will often role play and create stories for their audience while disguising their true identity due to their illegal conduct.

19. During the review of data located in the content folder within the return for the suspects account, [REDACTED] I discovered multiple anime CSAM images as well as the 29 reported Kik CyberTip CSAM videos. Those videos consisted of toddlers and prepubescent girls [REDACTED] some with bondage, [REDACTED]

20. During the review of the data from the [REDACTED] account, the

suspect is observed informing other users that he is a 19-year-old female from Louisiana. The suspect is again observed adding individuals to groups he created and informing them that the group doesn't have a limit.

[REDACTED]

[REDACTED]

23. On July 14, 2025, I received the Google search warrant returns for the suspects 2 accounts of [REDACTED] and

[REDACTED] During the review of data from Google return of [REDACTED], I located a name and date of birth for the suspect. The suspect's name being Austin Sewell (SEWELL), and a DOB of \*\*/\*\* /2000. The review of the return also showed a new IP address of

[REDACTED] This IP address checks back to and is owned by Life Covenant Church, otherwise known as Life Church, located in Edmond, OK.

24. Utilizing the search engine, CLEAR, I ran the name of Austin **SEWELL** and the birthdate of \*\*/\*\*/2000, and discovered only 1 match to an Austin **SEWELL** with that DOB. CLEAR also shows **SEWELL** residing at [REDACTED], in Sand Springs, Oklahoma 74063.

25. The AT&T U-Verse IP address, '[REDACTED]', which the suspect used to log into their Kik accounts, checks back to the Sand Springs area. I discovered this by utilizing maxmind.com, which is a website used by law enforcement in order to track the locations of IP addresses and was able to determine that the IP address shows the area of location to be Sand Springs.

26. On July 16, 2025, I received the AT&T U-Verse subpoena for IP address of "[REDACTED]". The return proved the owner of said Wi-Fi to be [REDACTED] Sewell with a residential address of [REDACTED] Sand Springs, Oklahoma 74063.

[REDACTED]

28. Utilizing Facebook searching the name of Austin **SEWELL**, I was able to locate **SEWELL** who shows on Facebook to reside in Sand Springs and works for LIFE CHURCH. Under **SEWELL**'s information page, it

states that **SEWELL** works at Life Church for the Midtown Tulsa location as an Operations Intern. I was able to positively match **SEWELL**'s driver's license photo with his Facebook picture and determined that it was the same. **SEWELL**'s Facebook states that he started working for Life Church Midtown on 1/6/25 and is still presently working there.

29. During the review of data from Google return for

[REDACTED] under the subscriber info, the same Life Church IP address was located. Both Google returns show **SEWELL** used an iPhone to log into his account.

30. On July 24, 2025, I executed federal search warrants on Austin **SEWELL**, his residence and vehicle located at [REDACTED] in Sand Springs.

31. During the search of their residence, I spoke to Austin **SEWELL**. I informed **SEWELL** that I had a search warrant for his residence in order to seize electronics deemed fruitful to my investigation. **SEWELL** was informed that the investigation was in reference to his online activity with Kik. At that time, **SEWELL** took a long pause and then stated, "I think I need an attorney and the interview was concluded.

32. Shortly after, **SEWELL** began to make multiple spontaneous utterances. **SEWELL** stated that he knew why I was there, that he had

been waiting for this for a long time and that every time someone came to his door and knocked, he thought his time was up. SEWELL stated he was glad it was finally over and that he had let everyone down.

33. SEWELL stated that he never did it for any sexual gratification but did it because he was bored due to not having anyone to talk to, but continued even knowing he knew it was doing was bad. SEWELL informed his mother that he was sorry for everything, apologized for his actions and that he has been wanting to “die.”

34. The warrant service was concluded with multiple electronics seized. During the search of SEWELL’s bedroom, located in the basement of his parents’ house, multiple high-power AR-15 Tactical rifles were found to include an AR-15 shotgun.


35. SEWELL was transported to David L. Moss where he was booked in on federal charges for possession of child sexual abuse material.

### **CONCLUSION**

Based on the information set forth in this affidavit, I submit there is probable cause to believe that Austin SEWELL has violated 18, United States Code, Sections

2252(a)(2) and (b)(1) (Receipt and Distribution of Child Pornography) and Title 18, United States Code, Sections 2252(a)(4)(A) and (b)(2) (Possession of Child Pornography in Indian Country).

Respectfully submitted,

  
\_\_\_\_\_  
Matt D. Gray  
Taskforce Officer  
Homeland Security Investigations

Subscribed and sworn via phone on the 25 day of July, 2025.

  
\_\_\_\_\_  
MARK T. STEELE  
UNITED STATES MAGISTRATE JUDGE