23SW-22-218

FILED
DATE 12/7/22 @ 11:24
Crystal Taylor, Clerk
By _____ DC

IN THE CIRCUIT COURT OF THE STATE OF ARKANSAS
FOR THE COUNTY OF FAULKNER

STATE OF ARKANSAS	)	
	)	SEARCH WARRANT
COUNTY OF FAULKNER	)	Google Account Records

To any Police Officer in the State of ARKANSAS Greetings;

You are hereby commanded to search the following in the County of Faulkner, State of Arkansas for evidence of the crimes of **A.C.A. 5-27-603 Computer child pornography.**

The location to be searched and the items to be sized are under the control of **Google, Inc.** in the Matter of the Search of information associated with Google account bwilliams@mvewarhawks.org that is stored at premises owned, maintained, controlled, or operated by Google, Inc.

That, in as much as **Google, Inc.** will furnish all information, records, and any technical assistance necessary to release records associated with the User Account **bwilliams@mvewarhawks.org**. It is hereby ordered that **Google, Inc.** be provided with a copy of this search warrant.

This search warrant allows Law Enforcement Officers to search: Google, Inc., an on-line services provider located in California with a physical address that includes 1600 Amphitheater Parkway, Mountain View, CA 94043, www.google.com. The records to be searched for and seized are more particularly described as;

Google Records to be Searched and Seized:

The specific account is associated with the account records currently under the control of **Google, Inc.** The specific account is associated with the account **bwilliams@mvewarhawks.org.**

Evidence to be Searched and Seized:

1. **Account Information - User name, primary e-mail address, secondary e-mail addresses, connected applications and sites, and account activity from 01/01/2014 to 7/1/2022, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;**

2. **Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;**
3. **Evidence of user attribution - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).**
4. **Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, from 01/01/2014 to 07/01/2022, calendar entries, notes, alerts, invites, and invitees;**
5. **Contacts - All contacts stored by Google including name, all contact phone numbers, e-mails, social network links, and images;**
6. **Documents – All user created documents stored by Google;**
7. **Gmail - All e-mail messages from 01/01/2014 to 07/01/2022, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and e-mails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;**
8. **Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service;**
9. **Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period 01/01/2014 to 07/01/2022;**

10. **Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device;**
11. **Search History - All search history and queries from 01/01/2014 to 07/01/2022, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;**
12. **Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voice-mail messages sent by or from the Google Voice account associated with the target account/device from 01/01/2014 to 07/01/2022;**
13. **Google Home (Smart Speaker & Home Assistant) - All information related to Google Home, including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times from 01/01/2014 to 07/01/2022;**
14. **Android Auto – All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs, text messages (SMS), voice actions, and all location data with dates and times from 01/01/2014 to 07/01/2022.**

IT IS ALSO FURTHER ORDERED, that Google, Inc. will deliver these records in an electronic format by electronic mail (e-mail) to **Inv. Steve Sumner** at steve.sumner@fcso.ar.gov. If sending the records by e-mail is not possible, the records shall be reduced to a compact disk (CD) or DVD and sent by common carrier to: Inv. Steve Sumner 801 Locust Ave, Conway, AR 72032

You are further directed to execute the search warrant within five (5) days of issuance between the hours of 7 am and 10 pm, and make return of this search warrant to me within five (5) days after execution, except as otherwise provided herein:

____ This warrant may be executed at any time of the day or night

____ This warrant may be executed more than five (5) days, but not more than ten (10) days from its date of issuance.

Dated this 27 day of July 2022, at 1:50 am/pm

Honorable Judge David Clark
20th Judicial District
4th Division

23SW-22-218

IN THE CIRCUIT COURT OF THE STATE OF ARKANSAS
FOR THE COUNTY OF FAULKNER

STATE OF ARKANSAS	)	
	)	AFFIDAVIT FOR ORDER OF NON-DISCLOSURE
COUNTY OF FAULKNER	)	Google Inc.

APPLICATION FOR ORDER COMMANDING META INC., NOT TO NOTIFY ANY PERSON OF THE EXISTENCE OF SEARCH WARRANT

The Faulkner County Sheriff's Office requests that the Court order Google, Inc., not to notify any person (including the subscribers or customers of the account **bwilliams@mvewarhawks.org)** listed in the subpoena of the existence of the attached subpoena until further order of the Court.

In this case, such an order would be appropriate because the attached subpoena relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the attached subpoena will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates.

WHEREFORE, the Faulkner County Sheriff's Office respectfully requests that the Court grant the attached Order directing Google, Inc., not to disclose the existence or content of the attached subpoena, except that Google, Inc., may disclose the attached subpoena to an attorney

for Google, Inc., for the purpose of receiving legal advice.

The Faulkner County Sheriff's Office further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Signed this 27 day of July, 2022

Inv. Steve Sumner

23CV-22-218

IN THE CIRCUIT COURT OF THE STATE OF ARKANSAS

FOR THE COUNTY OF FAULKNER

STATE OF ARKANSAS)
) AFFIDAVIT FOR SEARCH WARRANT
COUNTY OF FAULKNER) Google Account Records

Introduction and Investigator Background

I, Stephen Sumner, after being first duly sworn upon oath, depose and say:

I am an Investigator with the Faulkner County Sheriff's Office Major Crime Unit located in the County of Faulkner State of Arkansas, and that I have been so employed for more than three years. My training and experience includes the investigation of numerous criminal cases including, but not limited to, sex crimes.

I have more than eight hundred hours of official law enforcement related training recorded with the Criminal Justice Institute.

I am currently assigned as a full-time Investigator with the Faulkner County Sheriff's Office Major Crime Unit. I have been assigned to investigate several instances of possible child sexual assaults and possession of child pornography. The child pornography possession occurred in Faulkner County, Arkansas between 2014 and 2022.

I have reason to believe that a particular Google, Inc. account may contain evidence identifying and linking, victim(s), suspect(s), and possible witness(es) to the crime(s) of Child Pornography.

The facts set forth in this affidavit are based on the following: My investigation of a Mt. Vernon-Enola (MVE) School District employee, Mr. Blair Williams, who was brought to my attention by the staff at MVE High School in relation to possible child pornography discovered on a Google account, owned by MVE, and used by Mr. Williams in his capacity as an employee.

Therefore, the affiant is requesting a search warrant allowing them and/or Law Enforcement Officers to search: Google, Inc., an on-line service provider located in California with a physical address that includes 1600 Amphitheater Parkway, Mountain View, CA 94043, www.google.com.

Evidence to be Searched and Seized

This application seeks permission to search for and seize evidence of the crimes described above, that are associated with records currently under the control of **Google, Inc.**

The specific account is associated with the account **bwilliams@mvewarhwaks.org**.

Statement of Probable Cause

On 5/23/2022, I was assigned to a case involving possible child pornography. The superintendent of Mt. Vernon-Enola High school (MVE) told me they had recently terminated an employee, Mr. Blair Williams, for school policy violations that included inappropriate conduct between staff and students. As part of their normal procedures, the school district conducted an audit of the school issued accounts (bwilliams@mvewarhawks.org) and equipment given to Mr. Williams. The audit revealed suspected possible child pornography stored on the Google account used my Mr. Williams and possibly accessed using the school issued account and equipment.

I reviewed the photographs and videos stored on the Google account with the permission and consent of the MVE superintendent. I discovered many images and videos that depicted suspected juveniles engaged in various sexual acts and exhibitions, both alone and with Mr. Williams. I also discovered many photographs (screenshots) of conversations, using various mobile applications, including Facebook, Instagran and Snapchat, with suspected juveniles discussing possible sexual contact and sharing of sexually explicit content. I was able to extract metadata from the photographs and videos that indicated they were produced between 2014 and 2021. Mr. Williams was an employee of at least two different school districts during that time.

Historical Google Account Records

Based on my prior training and experience and after reviewing Google's privacy policy (https://policies.google.com/privacy), I am aware users of Android operating system mobile devices and other devices that access Google resources, such as cellular telephones, commonly have an associated account with Google, Inc.

When a user purchases and activates a mobile device one of the initial prompts during the set-up phase is to associate a Google Gmail e-mail account with the device. The purposes of this account are to facilitate a password reset in the event the consumer forgets their passcode, pattern unlock, or password. If the consumer does not have an existing Gmail account, the operating system prompts the user to create a new account. Whether the Gmail account is new or existing, the association of the account with the device allows Google to collect and store information relevant to this criminal investigation. This information includes, by way of example and not

limitation;

1. **Account Information - User name, primary e-mail address, secondary e-mail addresses, connected applications and sites, and account activity for the dates between 01/01/2014 through 7/1/2022, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;**

Google maintains information about their customers including primary e-mail addresses, secondary e-mail addresses for account password recovery, applications, websites, and services that are allowed to access the user's Google account or use the user's Google account as a password login, and account login activity such as the geographic area the user logged into the account, what type of internet browser and device they were using, and the internet protocol (IP) address they logged in from. The IP address is roughly analogous to a telephone number assigned to a computer by an internet service provider. The IP can be resolved back to a physical address such as a residence or business with Wi-Fi access or residential cable internet. I believe this information will assist in the investigation by identifying previously unknown e-mail accounts and location history information tending to show the movements of the suspect, his mobile device, and/or computers;

2. **Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device.**

Google stores information about mobile devices associated with the user's Google account. This includes the make, model, and unique serial numbers of all linked devices. I believe this information will identify any previously unknown cell phones or other mobile devices associated with the suspect's account and/or known device(s);

3. **User attribution data – accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s);**

I know that Google may not verify the true identity of an account creator, account user or any other person who accesses a user's account using login credentials. For these reason's it is necessary to examine particularly unique identifying information that can be used to attribute the account data to a certain user. This is often accomplished by analyzing associated account data,

usage, and activity through communication, connected devices, locations, associates, and other accounts. For these reasons it may be necessary to search and analyze data from when the Google account was initially created to the most current activity;

4. **Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, calendar entries, notes, alerts, invites, and invitees;**

Google offers a calendar feature that allows users to schedule events. This calendar function is the default option in the Android operating system and remains so unless the user adds a third party application. Calendar events may include dates, times, notes and descriptions, others invited to the event, and invitations to events from others. I believe this information will identify dates and appointments relevant to this investigation, as well as, identify previously unknown co-conspirators and/or witnesses, and any potential corroborative evidence;

5. **Contacts - All contacts stored by Google including name, all contact phone numbers, e-mails, social network links, and images;**

When a user links the Android device to their Google account the names, addresses, phone numbers, e-mail addresses, notes, and pictures associated with the account are transferred to the phone and vice versa. This process is continuously updates so when a contact is added, deleted, or modified using either the Google account or the mobile device the other is simultaneously updated. I believe this information is pertinent to the investigation, as it will assist with identifying previously unknown coconspirators and/or witnesses. Docs (Documents)- All Google documents including by way of example and not limitation, Docs (a web based word processing application), Sheets (a web-based spreadsheet program), and Slides (a web based presentation program.) Documents will include all files whether created, shared, or downloaded.

6. **Documents - All user created documents stored by Google;**

Google offers their users access to free, web-based alternatives to existing word processing, spreadsheet, and presentation software. These documents are stored in the user's account and are accessible from any device or platform as long as the user knows the password. These documents can include those created by the user, modified or edited by the user, or shared by the user and others. I believe this information may contain notes, files, and spreadsheets containing information relevant to this investigation including recordation of sales, communications with unknown co-conspirators and/or witnesses, and other information concerning the ongoing investigation;

7. **Gmail - All e-mail messages, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and e-mails in the trash folder. Such messages will include all information such as**

the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;

As noted previously, when user of an Android device first activates the device they are prompted to associate the device with a Google mail, commonly referred to as Gmail, account.

The purpose of this account is to facilitate password recovery in the event the user forgets their password or pattern lock. If the user does not have an existing Gmail account, they are prompted to create one. The Gmail account may be used to send and receive electronic mail messages and chat histories. These messages include incoming mail, sent mail, and draft messages. Messages deleted from Gmail are not actually deleted. They are moved to a folder labelled Trash and are stored there until the user empties the Trash file. Additionally, users can send and receive files as attachments. These files may include documents, videos, and other media files. I believe these messages would reveal motivations, plans and intentions, associates, and other co-conspirators;

8. **Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service;**

Google users have the option to store, upload, and share digital images, graphic files, video files, and other media files. These images may be downloaded from the internet, sent from other users, or uploaded from the user's mobile device. In many cases, an Android user may configure their device to automatically upload pictures taken with a mobile device to their Google account. I believe a review of these images would provide evidence depicting the suspect, his/her associates and others performing incriminating acts, and victims. I also believe these image files may assist investigators with determining geographic locations such as residences, businesses, and other places relevant to the ongoing criminal investigation;

9. **Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period** 01/01/2014 **to** [07/01/2022]**;**

Google collects and retains location data from Android enabled mobile devices. The company uses this information for location-based advertising and location based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, and Wi-Fi access points. While the specific parameters of when this data is

collected are not entirely clear, it appears that Google collects this data whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or e-mail access. I believe this data will show the movements of the suspect's mobile device and assist investigators with establishing patterns of movement, identifying residences, work locations, and other areas that may contain further evidence relevant to the ongoing criminal investigation;

10. Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device;

Google operates an online marketplace whereby Google and other third party vendors offer for sale applications such as games, productivity tools, and social media portals. Many of these applications can be used to communicate outside the cellular service of a mobile device by accessing the internet via Wi-Fi.

These various applications facilitate communication via voice using voice over internet protocol (VOIP) technology, short message system (SMS) text messages, multi-media message system (MMS) text messages, audio transmission of recorded messages, and recorded or live video messages. As these services operate independently of the cellular service network there is no corresponding information regarding communications from the cellular provider. Identifying communications applications purchased, downloaded, and/or installed on the mobile device would assist investigators by determining what application provider should be served with additional search warrants. Furthermore, identifying the user's applications would assist investigators with determining banking and other financial institution information and social media sites used. Identifying the purchased or installed applications would assist locating those with potentially criminal implications such as applications that appear to the observer to be a calculator or other innocuous appearing program but in actuality are used to conceal pictures, videos, and other files. These concealment applications are commonly missed during manual and forensic examinations of mobile devices as existing technologies are not designed to detect and locate them and the information they conceal;

11. Search History - All search history and queries, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;

Google retains a user's search history whether it is done from a mobile device or from a traditional computer. This history includes the searched for terms, the date and time of the search, and the user-selected results. Furthermore, the specific type of search a user performed into categories differentiates these searches. These categories include a general web search and

specialty searches where the results are focused in a particular group such as images, news, videos, and shopping.

I believe a review of the suspect's search history would reveal information relevant to the ongoing criminal investigation by revealing what information the suspect sought and when he sought it;

12. Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voice-mail messages sent by or from the Google Voice account associated with the target account/device;

Google offers users access to a free voice over internet protocol (VOIP) communications system called Google Voice or simply Voice. This system is layered on top of any existing cellular service. Users are provided with a phone number they select from a pool of available numbers. These numbers can be from whatever area code and prefix they desire and have no correlation with the user's actual location when the number is selected. Google allows users to access this system to make and receive phone calls and text messages. The service also has a voice-mail feature where incoming phone calls are permitted to leave a message that is subsequently transcribed by Google and delivered by electronic mail and/or text message. Google maintains call detail records similar to those of a traditional cellular or wireline telephone company. Additionally, they also store the text message content of sent and received text messages, as well as, any saved voice-mail messages and the associated transcriptions;

13. Google Home (Smart Speaker & Home Assistant) - All information related to Google Home including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times;

Google Home is a brand of smart speaker developed by Google, Inc. Google Home Speakers have microphones that are always listening that enable users to speak voice commands to interact with services through Google's intelligent personal assistant called Google Assistant. A large number of services, both in-house and third-party, are integrated, allowing users to listen to music, control playback of videos and photos, and receive news updates entirely by voice. Google Home devices also have integrated support for home automation, letting users control smart home appliances with their voice. Multiple Google Home devices can be placed in different rooms in a home for synchronized connectivity. The data collected by Google Home devices are stored remotely on Google's servers. Users can access their Google Home account and associated data by way of a connected smart phone application or through their Google account. I believe the Google Home related data, including the archived audio recordings may be

used to refute and corroborate statements, and may be important in identifying potential witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing a timeline and provide context and intent.

14. **Android Auto - All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs and text messages, voice actions, and all location data;**

Android Auto is a mobile device application developed by Google that allows enhanced use of an Android device within a vehicle equipped with a compatible head unit. Once the Android device is connected to the head unit, the system enables it to broadcast applications (apps) with a simple, driver-friendly user interface onto the vehicle's dash display, including GPS mapping/navigation, music playback, text messages (SMS), voice calls, and web search. The system supports both touchscreen and button-controlled head unit displays, although hands-free operation through voice commands is encouraged. Once the user's Android device is connected to the vehicle, the Android mobile device will have access to several of the vehicle's sensors and inputs, such as GPS, steering-wheel mounted buttons, the sound system, directional microphones, wheel speed, compass, and other vehicle data.

I believe the Android Auto related data, including the historical geo-location data (GPS, compass, speed, direction) may be important in establishing locations and activities of possible witnesses, victims, co-conspirators, and suspects. This information may also be important in establishing the driver and occupants of a particular vehicle, refute and corroborate statements, and can be used to establish a timeline and provide context and intent.

For the reasons outlined above, I believe probable cause exists to seize and examine the specified records held by Google, Inc. associated with the account **bwilliams@mvewarhawks.org**. The records to be searched for and seized are more particularly described as;

Records to be Searched and/or Seized

1. **Account Information - User name, primary e-mail address, secondary e-mail addresses, connected applications and sites, and account activity from** -1/01/2014 **to** 07/01/2022**, including account sign in locations, browser information, platform information, and internet protocol (IP) addresses;**

2. **Android Information - Device make, model, and International Mobile Equipment Identifier (IMEI) or Mobile Equipment Identifier (MEID) of all associated devices linked to the Google accounts of the target device;**
3. **Evidence of user attribution - accounts, e-mail accounts, passwords, PIN codes, account names, user names, screen names, remote data storage accounts, credit card number or other payment methods, contact lists, calendar entries, text messages, voice mail messages, pictures, videos, telephone numbers, mobile devices, physical addresses, historical GPS locations, two-step verification information, or any other data that may demonstrate attribution to a particular user or users of the account(s).**
4. **Calendar - All calendars, including shared calendars and the identities of those with whom they are shared, from 01/01/2014 to 07/01/2022, calendar entries, notes, alerts, invites, and invitees;**
5. **Contacts - All contacts stored by Google including name, all contact phone numbers, e-mails, social network links, and images;**
6. **Documents – All user created documents stored by Google;**
7. **Gmail - All e-mail messages from 01/01/2014 to 07/01/2022, including by way of example and not limitation, such as inbox messages whether read or unread, sent mail, saved drafts, chat histories, and e-mails in the trash folder. Such messages will include all information such as the date, time, internet protocol (IP) address routing information, sender, receiver, subject line, any other parties sent the same electronic mail through the 'cc' (carbon copy) or the 'bcc' (blind carbon copy), the message content or body, and all attached files;**
8. **Google Photos - All images, graphic files, video files, and other media files stored in the Google Photos service;**
9. **Location History - All location data whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location. Such data shall include the GPS coordinates and the dates and times of all location recordings from the period 01/01/2014 to 07/01/2022;**
10. **Play Store - All applications downloaded, installed, and/or purchased by the associated account and/or device;**

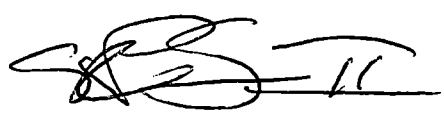
11. **Search History - All search history and queries from 01/01/2014 to 07/01/2022, including by way of example and not limitation, such as World Wide Web (web), images, news, shopping, ads, videos, maps, travel, and finance;**
12. **Voice - All call detail records, connection records, short message system (SMS) or multimedia message system (MMS) messages, and voice-mail messages sent by or from the Google Voice account associated with the target account/device from 01/01/2014 to 07/01/2022;**
13. **Google Home (Smart Speaker & Home Assistant) - All information related to Google Home, including device names, serial numbers, Wi-Fi networks, addresses, media services, linked devices, video services, voice and audio activity, and voice recordings with dates and times from 01/01/2014 to 07/01/2022;**
14. **Android Auto – All information related to Android Auto including device names, serial numbers and identification numbers, device names, maps and map data, communications including call logs, text messages (SMS), voice actions, and all location data with dates and times from 01/01/2014 to 07/01/2022.**

Authorization for Electronic Service

I also request authorization to execute the search warrant for the requested records via electronic means including facsimile or other electronic transmission.

Conclusion

Based on the foregoing information, I have probable cause to believe that evidence of the crime(s) **A.C.A. 5-27-603 Computer Child Pornagrpahy,** as set forth herein are currently within the records described above. I therefore respectfully request that a search warrant be issued authorizing the search for, seizure of and examination of the records set forth in herein.



Investigator Steve Sumner
Faulkner County Sheriff's Office

Subscribed and sworn to before me this 21 day of May, 2022.

Honorable Judge David Clark

20th Judicial District

4th Division

23SW-22-218

IN THE CIRCUIT COURT OF FAULKNER COUNTY, ARKANSAS

FILED
DATE 12/7/2022 11:24
Crystal Taylor, Clerk
By _____ DC

STATE OF ARKANSAS
VS.
OWNER/USER OF: Google enterprise account

REPORT OF RETURN OF A SEARCH WARRANT

The undersigned has **NOT** executed a Search Warrant issued by this Court on the 28th day of July, 2022, for the search of the account of:

Screen/user Name – Blair Williams
Google User Alias – bwilliams@mvewarhawks.org

The undersigned reports to this Court the following facts and circumstances surrounding the execution of this Warrant and attaches the returned Warrant and the Inventory of any and all evidence/information seized:

Digital files

WHEREFORE, the undersigned prays that this report be filed with this Court and with any other Court who may have jurisdiction over the offense alleged concerning which said Warrant be issued.

_____
Signature of Affiant

INVESTIGATOR
Official Title

SUBSCRIBED AND SWORN to before me, a Notary Public, on this 7th **day of**

December, **2022.**

_____ **Notary Public**

My Commission Expires: Nov 8, 2029

NICOLE SPILLER
Comm. Exp. 11-08-2029
NOTARY PUBLIC
Comm. No. 12709254
FAULKNER COUNTY, ARKANSAS