|  |  |  |
| --- | --- | --- |
| IN THE CIRCUIT COURT OF {{COUNTY|upper }} COUNTY, MISSOURI | | |
|  | )  )  )  )  ) | Sikeston DPS: {{ CASE }} |
| STATE OF MISSOURI  COUNTY OF {{COUNTY|upper }} |
|  |  |  |
| **AFFIDAVIT AND APPLICATION FOR A SEARCH WARRANT** | | |

**INTRODUCTION AND AGENT BACKGROUND**

1. I, {{ NAME|title }}, knowing that false statements are punishable by law, hereby affirm and state that the facts contained herein are true to the best of my information and belief. Based on the following information, I hereby request the Court find probable cause and make this Affidavit in support of the issuance of a Search Warrant.
2. I am a {{ RANK|title }} with the {{AGENCY }}, located in the County of {{ COUNTY|title }}, State of Missouri. I am a “Peace Officer” as defined in RSMO § 542.261. I have been employed as a peace officer for more than {{ YEARS }} years. I have training pertaining to the investigation of criminal offenses and as part of my regular duties, I have previously participated in the investigation of various criminal offenses, including the offense which is currently under investigation and is the subject of this Affidavit.
3. I have been assigned to investigate a {{CRIME|title}}, a violation of RSMO § {{RSMO}}. The incident occurred in {{COUNTY|title}} County on or about {{MONTH|title}} {{DAY}}, {{YEAR}}.

**PERSON, PLACE, OR THING TO BE SEARCHED**

See Attachment "A"

**ITEMS TO BE SEARCHED AND SEIZED**

See Attachment "B"

**STATEMENT OF PROBABLE CAUSE**

1. {Type your probable cause statement here. Remember that you have to establish probable cause for what you want to search and also establish that it’s probable that the evidence you wish to search for will be at that location.}

{%p **if** FACEBOOK %}

**BACKGROUND AND EXPLANATION OF META**

1. Meta Platforms Inc., commonly referred to as Meta, is the creator and owner of Facebook which is an open-access social networking website that can be currently accessed at www.facebook.com. Because the transition of Facebook to their new name of Meta is not yet complete, core Facebook services can still be accessed as they always have. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public. Facebook requires 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.
2. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust to control, for example, the types of notifications they receive from Facebook.
3. 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.
4. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.
5. 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.
6. 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.
7. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs ("blogs"), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.
8. The Facebook Gifts feature allows users to send virtual "gifts" to their friends that appear as icons on the recipient's profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other "pokes," which are free and simply result in a notification to the recipient that he or she has been "poked" by the sender.
9. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.
10. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that the user's access or use of that application may appear on the user's profile page.
11. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.
12. 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.
13. Social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

{%p endif %}

{%p if FBPING %}

**REQUEST FOR ONGOING LOCATION DATA ORDER**

1. I know that Meta Platforms Inc. (Facebook) has the technical capability to provide nearly real time location information of the Target Account described in the search warrant pursuant to an order from this court. Location data is collected by Meta Platforms Inc. (Facebook) through its App and website and is stored as a normal course of business. This location data is extremely useful in law enforcement investigations in determining peoples locations, routes of travel, residences or business or locations that the person stops at.
2. I also know that Facebook has the technical capability to install and use a technology similar to a Pen Register and a Trap and Trace Device. Pen Registers are used to register numbers that are dialed by a telephone and record the length of the call. A Trap and Trace Device is used in conjunction with a Pen Register to capture and record the telephone numbers of incoming calls. Together, these tools provide investigators with a more complete view of the people and businesses that the suspect is communicating with. It is important to note that Pen Register and Trap and Trace Device only record the telephone numbers and cannot capture call content. Facebook can implement a similar method for Facebook Messenger calls and messages by monitoring based upon Facebook ID instead of telephone number.

{%p endif %}

{%p **if** SNAP %}

**BACKGROUND AND EXPLANATION OF THE SNAPCHAT APPLICATION**

1. Snapchat is both a messaging platform and a social network that enables users to connect with their contacts using both a mobile app and a new browser based interface. Users can "chat" with their friends by sending them photos or short videos up to 10 seconds long, overlaying text on these photos and short videos, by sending plain text to another user, or by audio and video calls. One of the most unique things about Snapchat is the ephemeral components of the content that gets shared on it. Photos, videos, and unsaved text messages are automatically deleted a few seconds after they've been viewed by their recipients. Snapchat also provides a news feed feature where the user can post photos and videos that could be viewed by their friends as a story clip rather than as a private or group message. These clips, called "stories", are posted for 48 hours only before they are automatically deleted.
2. Before a user can use Snapchat they must create an account consisting of personally identifiable information and/or information that may provide additional investigative avenues for which additional search warrants or other legal process may be sought. The initial stage of creating an account is selection of a unique username. This name cannot be changed and remains as the identifiable account name for the profile. A new user can additionally create a 'vanity name' which is capable of being modified and can contain emojis, symbols or other characters that are not allowed for the account username. Both the username and vanity name are visible to other Snapchat users, however, users commonly reference the vanity name when identifying a Snapchatter. Vanity names and usernames can pose investigative challenges and initial confusion when researching Snapchat accounts. It is important to note that Snapchat does not have the technical capability to locate Snapchat accounts based upon vanity names.
3. Snapchat users are immediately notified if the recipients of their Snapchat messages, also known as "snaps", try to take a screenshot of the snaps. Screenshots can indeed be captured if a user does it quickly and the sender is always notified about it right away. Despite this notification feature there exists several methods and apps that are capable to covertly saving snaps and bypassing this feature.

{%p endif %}

{%p **if** INSTA %}

**BACKGROUND AND EXPLANATION OF INSTAGRAM**

1. Instagram is a social networking app, owned by Meta Platforms Inc., made for sharing photos and videos from a smartphone. Similar to Meta or Twitter, everyone who creates an Instagram account has a profile and a news feed. When a user posts a photo or video on Instagram, it will be displayed on their profile. Other users who follow a specific Instagram user will see that specific Instagram user's posts in their own feed. Similar to other social networks, users interact with others on Instagram by following them, being followed by them, commenting, liking, tagging and private messaging.
2. Instagram can be accessed on the web from a computer, but users can only upload and share photos or videos from their devices. Instagram profiles allow the user to provide their name, a photo, a short bio, and a website link. Every user profile has a "Followers" and "Following" count, which represents how many people they follow and how many other users are following them. Every user profile has a button you can tap to follow them. If a user has their profile set to private, they will need to approve your request first. Additionally, users can edit and apply filters to the photos, fill out a caption, tag other users to it, tag it to a geographical location, and post it to some of the user's other social networks.

{%p endif %}

{%p **if** INSTAPING %}

**REQUEST FOR ONGOING LOCATION DATA ORDER**

1. I know that Meta Platforms Inc. (Instagram) has the technical capability to provide nearly real time location information of the Target Account described in the search warrant pursuant to an order from this court. Location data is collected by Meta Platforms Inc. (Instagram) through its App and website and is stored as a normal course of business. This location data is extremely useful in law enforcement investigations in determining peoples locations, routes of travel, residences or business or locations that the person stops at.

{%p endif %}

{%p **if** APPLE %}

**BACKGROUND AND EXPLANATION OF APPLE INC.**

1. Apple Inc. is an American multinational technology company headquartered in Cupertino, California, that designs, develops, and sells consumer electronics, computer software, and online services. Apple's hardware products include the iPhone smartphone, the iPad tablet computer, the Mac computer, the iPod portable media player, the Apple Watch smartwatch, the Apple TV digital media player, the AirPods wireless earbuds and the HomePod smart speaker. Apple's software includes macOS, iOS, iPadOS, watchOS, and tvOS operating systems, the iTunes media player, the Safari web browser, the Shazam music identifier, and the iLife and iWork creativity and productivity suites, as well as professional applications like Final Cut Pro, Logic Pro, and Xcode. Its online services include the iTunes Store, the iOS App Store, Mac App Store, Apple Music, Apple TV+, iMessage, and iCloud. Other services include Apple Store, Genius Bar, AppleCare, Apple Pay, Apple Pay Cash, and Apple Card.
2. Apple Inc. utilizes an online storage system, known as iCloud, for each of it's customers. iCloud is built into every Apple device and is the default way to back-up a user's photos, files, notes, and more. Every user gets 5GB of free iCloud storage to start with paid options for more storage. Because iCloud stores a user's files in the "cloud", these files are accessible to them from any device in the world and can be accessed through their username and password from iCloud.com. Additionally, iCloud is the primary method for storing a user's iOS device backup files. When a user does a backup of their iPhone to the Cloud, they can restore a completely different iPhone with the contents of their old phone.
3. A user's Apple ID is the account used to access Apple services like the App Store, Apple Music, iCloud, iMessage, FaceTime, and more. User's can sign into all Apple services with a single Apple ID and password and utilized the same Apple ID to log into multiple devices. As such, files such as photos taken on a user's iPhone will automatically sync across iCloud to an iPad or Mac computer that the user is also signed into.
4. FaceTime is Apple's video and audio calling service. Similar to iMessage, FaceTime calls also use the Apple Push Notification service to establish an initial connection to the user's registered devices. The audio/video contents of FaceTime calls are protected by end-to-end encryption, so no one but the sender and receiver can access them. Apple cannot decrypt the data.

{%p endif %}

{%p **if** GOOGLE %}

**BACKGROUND AND EXPLANATION OF GOOGLE INC.**

1. Google LLC is a globally recognized technology company that specializes in a broad range of internet-related services and products. Among the products and services Google offers are online advertising, cloud computing, hardware and software products, search engines, and productivity tools. Google’s core search engine is a widely popular product and offers users fast and accurate search results. Other work and productivity services offered by Google include Google Docs, Google Sheets, and Google Slides. The company also offers cloud storage, Google Drive, and an email service, Gmail.
2. Google offers multiple communication services such as video chat, instant messaging, and voice assistants, including Google Allo, Duo, Hangouts, and Google Assistant. The company also offers mapping and navigation services such as Google Maps, Google Earth, Waze, Street View, and language translation through Google Translate. Google has developed and leads the Android mobile operating system and the Google Chrome web browser. Additionally, the company offers Internet Service Provider and Mobile Telephony services such as Google Fiber, Google Fi, and Google Station.
3. Google collects user information in various ways, such as through user registration data and monitoring user activity. Registration information may include name, gender, birthdate, and phone number. Google tracks direct product usage, including recent Google searches, visited websites, and usage of smart home devices. It also records accurate location information, videos watched, voice interactions with Google Assistant, and voice recordings. Aggregated data is generated by combining search and viewing activity to determine user preferences and interests. This data is used to create a digital profile of users that Google primarily uses for targeted advertising and marketing data analytics.

{%p endif %}

**PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENT ACCESS**

1. As allowed per 18 U.S.C. § 2705(b), I request the service provider be ordered to NOT notify any other person of the existence of the warrant and subsequent records access by law enforcement for a period of at least 90 days.
2. This criminal investigation is ongoing, and it is likely that information and evidence obtained in the course of the service of this search warrant will result in further information concerning the identity and involvement of suspects in this case. As such, disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify co-conspirators, and flee from apprehension and prosecution.
3. Alerting the subscriber, customer or owner of the electronic communication information to which the materials relate, to the existence and service of this search warrant may have an adverse result, to include endangering the life or physical safety of an individual, flight from prosecution, destruction of, or tampering with, evidence, intimidation of potential witnesses, or otherwise seriously jeopardize the investigation or unduly delay a trial.
4. I have read this affidavit and the facts contained in here are the truth to the best of my knowledge.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Affiant)

{{ RANK|title }} {{ NAME|title }}

{{ AGENCY }}

DATE: {{ TODAY }}   
TIME:

I have reviewed this Affidavit and Application and hereby apply for a search warrant based upon this Affidavit and place my signature upon this Application.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Prosecuting Attorney)

DATE:

TIME:

Witness my hand and the seal of this Court on {{ TODAY }}.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   
(Signature of Judge)

DATE:

TIME:

|  |  |  |
| --- | --- | --- |
| IN THE CIRCUIT COURT OF {{COUNTY|upper }} COUNTY, MISSOURI | | |
|  | )  )  )  )  ) | Sikeston DPS: {{ CASE }} |
| STATE OF MISSOURI  COUNTY OF {{COUNTY|upper }} |
|  |  |  |
| **SEARCH WARRANT** | | |

**THE STATE OF MISSOURI TO ANY PEACE OFFICER IN THE STATE:**

**WHEREAS**, proof having been made before me by {{ RANK|title }} {{ NAME|title }}, the Judge of this Court has found probable cause to believe the allegations of the complaint to be true and that there is probable cause to believe that evidence pertaining to {{CRIME|title}}, a violation of RSMO § {{RSMO}} is presently located at the location(s) described herein.

**YOU ARE COMMANDED TO SEARCH THE FOLLOWING LOCATION(s):**

See Attachment "A"

**FOR THE FOLLOWING PROPERTY OR PERSON(s):**

See Attachment "B"

**NOW, THEREFORE**, you are directed to execute this search warrant, to seize, photograph, or copy the property, article, substance, or person found thereon or therein, and make return of this warrant to this court within ten (10) days after filing.

Witness my hand and the seal of this Court on {{ TODAY }} at \_\_\_\_\_\_\_\_\_ AM / PM.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Circuit / Associate Circuit Judge

TIME:

**ATTACHMENT "A"**

**TO MAKE A SEARCH OF:**

{%p **if** FACEBOOK %}

**Meta Platforms, Inc**1601 Willow Road,  
Menlo Park, Ca 94025

{%p endif %}

{%p **if** INSTA %}

**Meta Platforms, Inc**1601 Willow Road,  
Menlo Park, Ca 94025

{%p endif %}

{%p **if** SNAP %}

**THE ONLINE SERVICE PROVIDER known as Snap Inc.**Attn: Custodian of Records  
2772 Donald Douglas Loop   
North Santa Monica, CA 90405  
Service via upload to Snapchat Law Enforcement Service System: less.snapchat.com

{%p endif %}

{%p **if** APPLE %}

**THE BUSINESS known as: Apple Inc.**Attn: Corporate Legal Counsel  
1 Infinite Loop, M/S 36-SU  
Cupertino, CA 95014  
408-974-2095  
Service via email at lawenforcement@apple.com

{%p endif %}

{%p **if** GOOGLE %}

**THE INTERNET SERVICE PROVIDER known as: Google LLC**1600 Amphitheatre Parkway  
Mountain View, CA. 94043  
Attn: Custodian of Records  
Phone: (844) 383-8524  
Email: uslawenforcement@google.com  
Service via digital upload: Law Enforcement Request System (LERS)

{%p endif %}

**End of Attachment "A"**

**ATTACHMENT "B"**

FOR THE FOLLOWING RECORDS:   
Records from the above listed Service Provider for the Account: {{ ACCOUNT }}

Each of the types of records specified below shall be for the period of {{ STARTDATE }} to {{ ENDDATE }} for evidence related to the crime(s) of: {{ CRIME }}.

{Review the list below and remove things that aren’t needed in your case. If you add things, make sure you’re particular enough in describing them not to be seen as overbroad. REMOVE THIS PART BEFORE SUBMISSION}

{%p **if** FACEBOOK %}

**Meta Platforms Inc. (Facebook)**   
  
**Account Settings:** Account settings, including privacy settings for individual Facebook posts and activities, and records showing which Facebook users have been blocked by the Target Account.

**Account Usage:** Collected information about how the Target Account used Facebook Inc. products, such as the types of content viewed or engaged with; the features used; the actions taken; the people or accounts interacted with; and the time, frequency and duration of the Target Account activities.

**Cookies and Tracking information:** Information either directly collected or collected from service providers working on behalf of Facebook Inc. using various tracking technologies such as cookies and web beacons or "tracking pixels" or pixel tags, Local Shared Objects "LSO", and Google AdSense information to include the Target Account's associated Google Advertising ID.

**Device Information:** Records of the device(s) used by the Target Account to access Facebook Inc. services to include make and model, device IDs such as IMEI, GAID or IDFA, and other identifiers from games, apps or accounts, and Family Device IDs,

**Facebook Dating:** Records of the Target Account's Facebook Dating profile to include profile photos, location, gender, height, religion, job title, company, schools, other profile information; likes with attached messages and the associated liked accounts, photos and status updates; dating interests such as match preference with everyone, women, trans women, men and trans men; "secret crush" data and the associated profile indicator; and "Share Your Plans" events to include the profiles that plans were shared with.

**Facebook Marketplace:** Information about the Target Account access and use of Facebook Marketplace to include records of items purchased and transaction records.

**Facebook Messenger Records:** Records of Facebook Messenger communications and messages made or received by the user, including private messages, chat history, video calling history, and pending "Friend" requests to include stored content.

**Facebook Pay:** Records of the Target Accounts Facebook Pay information to include card or account information as well as records of purchases, sent or received money, or donations made by the Target Account.

**Facial Recognition Information:** Records of stored Facebook Inc. face recognition technology used to recognize the Target Account in photos, videos and camera experiences. Photos, videos and camera experience that the Target Account has been identified in shall also be provided to the Sikeston Department of Public Safety with an indicator to specify that the file was provided as a result of face recognition. These records shall include face-recognition records for associated Instagram profiles with their associated Instagram identifying information.

**Financial Information:** Records of purchases or other financial transactions including game purchases and donations as well as payment information that includes credit or debit card number and other card information; other account and authentication information; and billing, shipping and contact details.

**Friends Lists:** Past and present lists of friends created by or associated with the Target Account.

**Internet Protocol Logs:** Information related to the IP addresses used by the Target Account for account logins or access to include the associated dates, times, time zone and source port if available.

**Length of Service Records:** Records indicating the dates and time that the Target Account was created and should include the IP address and device identifier used to create the profile.

**Location Information:** Records of location-related information to include the Target Account's current or most recent location at the time the search warrant is served, records of where Facebook believes the Target Account lives, frequently visited places, and records of the businesses and people the Target Account is near that Facebook Inc. uses to provide personalized Facebook Products and ads. Location records shall include "precise device location", IP addresses, and information from the Target Account use of Facebook Products such as check-ins or attended events.

**Neoprint Information:** Neoprint of the Target Account to include records of profile contact information; News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the Target Account access and use of Facebook applications.

**Networks and Connections:** Records of collected information about the people, Pages, accounts, hashtags and groups the Target Account connected to and their interactions with them across Facebook Inc. products to include people the Target Accounts communicated with the most or associated groups.

**Partner Information:** Records of data provided to or received by Advertisers, app developers, and publishers through Facebook Business Tools including our social plug-ins such as the Like button, Facebook Login, Facebook Inc. APIs and SDKs, or the Facebook pixel.

**Passive Audio Recordings:** Stored audio recordings collected by Meta Platforms Inc. that are associated to the Target Account through passive listening from the installed Facebook app. Such recordings shall include the date and time of the recording and indicators of the device the recording was collected from.

**Photoprints:** Stored Photoprint images of the Target Account comprised of photos uploaded by the user that have not been deleted, along with photos that have the Target Account tagged in them.

**Search Records:** Records of searches performed by the Target Account on the Facebook Inc. service to include the content of the search, the results, and which results were selected by the Target Account.

**Stored Videos:** Stored videos, recorded Live videos, and 360 videos uploaded by Target Account to include the files associated original EXIF, metadata, and geo-location data as well as records indicating the original source of the upload such as direct upload for the user's computer or mobile phone, source URL, or associated service.

**Subscriber Information:** Subscriber information and contact information to include name, address, user identification number, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

**Support Records:** Records pertaining to communications between Facebook and the Target Account including contacts with support services and records of actions taken.

**Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal justification for the implementation of the following special procedures which shall be employed by the officers who execute this warrant:

**AUTHENTICITY OF RECORD ORDER**

IT IS HEREBY ORDERED that the Service Provider listed in the Attachment(s) shall provide a valid "Authenticity of Records" document consisting of an affidavit and that the document be returned to the Affiant along with a copy of the requested records.

**FIVE DAY RECORD PRODUCTION ORDER**

IT IS HEREBY ORDERED that the organizations described in this search warrant shall produce the requested records within five (5) days of receipt of this search warrant.

{%p endif %}

{%p **if** FBPING %}

**ONGOING LOCATION DATA ORDER**

IT IS HEREBY ORDERED that Meta Platforms Inc. (Facebook) shall query internal system that store geolocation data to determine the physical location of the Target Account's mobile device on the Meta Platforms Inc. (Facebook) network or with such other reference points as may be reasonable available.  The locations determined by Meta Platforms Inc. (Facebook) shall be provided in 15 minute intervals, or such intervals and times as directed by the law enforcement agent serving this order, for a period of (30) days from the execution of this warrant.

**PEN REGISTER AND TRAP TRACE ORDER**

IT IS HEREBY ORDERED that Meta Platforms Inc. (Facebook) shall install and monitor a pen register / trap and trace device to record, decode, and/or capture all non-content electronic transmission of data to and from the target Facebook Inc. account in an attempt to recover all data that constitutes contraband, fruits, evidence and / or instrumentalities of {{ CRIME }} and dominion and control of the target account for a period of 30 days from the date of this warrant.  The pen register / trap and trace is to be installed and used within the jurisdiction of this court and shall record:

1. Access logs - records of user activity for each connection made to or from the target account(s), including log files; the date, time, length, and method of connections; data transfer volume; and source and destination Internet Protocol (IP) addresses.
2. Information about each communication (not including content) sent or received by the target account(s), including message headers, the date and time of the communication, the method of communication, user names and account ID of participants, related IP addresses, and any the source and destination of the communications (such as source and destination Facebook Messenger messages, IP addresses, and associated telephone numbers), and user names and account ID of participants.
3. Ongoing GPS coordinates or other location information associated with the target account(s) and devices, such as location history and last location of device.

{%p endif %}

{%p **if** INSTA %}

**Meta Platforms Inc. (Instagram)**

**Archived Data:** Archived copies of the target Instagram pages/profiles or User Content to include photos, videos, chat communication, messages, friend lists, profile information, and files.

**Badge Records:** Records of Badges either purchased and used by the Target Account or, Badges purchased to support the Target Account while streaming live video. For Badge purchase records these records shall include dates and times of the purchases, amounts, and creator that the Badge(s) were purchased for. For Badges earned, these records shall include logs of Badges received, total amounts, and records of Badges being exchanged for currency.

**Communication Content:** Information including contents of communications, photo comments, or other data that would constitute other electronic communication information.

**Device Information:** Records to include Media Access Control (MAC) address, computer or device type, screen resolution, device manufacturer and model, language, Persistent Device Identifier or Ad ID, Internet browser type and version and the name and version of the Services the target is using; the operating system the target is using, the domain name of the Internet service provider and the "click path" through the Instagram site; browser or device information, app usage data, information through cookies, pixel tags and other technologies, and aggregated information.  
**Friends List:** Records of friends that the Target Account has added through the use of the Instagram "Find friends" feature either through their contacts list, third-party social media sites, or through a name search of Instagram usernames and data that indicates the method in which they were located if available.

**IP Address Logs:** All information related to IP addresses used for the creation of the account as well as IP address used by the Target Account to access Instagram services for the dates indicated.

**Linked Accounts:** Records of all linked external accounts (such as Twitter or Facebook) or associated email address, username, user ID numbers, or contact information.

**Location Information:** Information associated with files posted by the user that contains location data, including but not limited to, latitude & longitude data, GPS coordinates, or associated IP address.

**Log Information:** Records that Instagram servers automatically record in logs files to include web requests, browser type, referring / exit pages and URLs, number of clicks and how the Target Account interacted with links on the Service, domain names, landing pages, pages viewed, and other such information, and information collected from emails sent to the Target Account and data that indicates which emails were opened and which links were clicked.

**Metadata:** Records of technical data that is associated with the Target Account Content to include how, when and by whom a piece of User Content was collected and how that content is formatted, custom hashtag, geotag, comments or other data. If available, geotagged data shall include latitude and longitude.

**Stored Media:** All photographic/video/audio data and associated metadata, EXIF data, & geolocation data.

**Subscriber Information:** Subscriber information to include name, address, phone number, contact information, profile photo, and dates associated with account creation and/or suspension for the listed Target Account.

**Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal justification for the implementation of the following special procedures which shall be employed by the officers who execute this warrant.

**Authenticity of Record ORDER**

IT IS HEREBY ORDERED that the Service Provider listed in the Attachment(s) shall provide a valid "Authenticity of Records" document consisting of an affidavit and that the document be returned to the Affiant along with a copy of the requested records.

**Five Day Record Production ORDER**

IT IS HEREBY ORDERED that the organizations described in this search warrant shall produce the requested records within five (5) days of receipt of this search warrant.

{%p endif %}

{%p **if** INSTAPING %}

**Ongoing Location Data ORDER**

IT IS HEREBY ORDERED that Meta Platforms Inc. (Instagram) shall query internal system that store geolocation data to determine the physical location of the Target Account's mobile device on the Meta Platforms Inc. (Instagram) network or with such other reference points as may be reasonable available. The locations determined by Meta Platforms Inc. (Instagram) shall be provided in 15 minute intervals, or such intervals and times as directed by the law enforcement agent serving this order, for a period of (30) days from the execution of this warrant.

{%p endif %}

{%p **if** SNAP %}

**Snap Inc.**

**Bitmoji Records:** Records of the Target Account's Bitmoji to include current Bitmoji image and previously selected Bitmojis.

**Camera and Photos:** Records of Snap Inc. collected or user uploaded images and videos and other information from the Target Account device's camera and photos including associated exif or metadata.

**Communication Content:** Records of communication with other Snapchatters, including the complete message content, Snapchatter's names, the time and date of the communications, records of the Target Account's interactions with messages such as opening a message or capturing a screenshot, bitmoji reactions, and direct chat replies as well and records of communication with customer support. These records shall also include Audio or Video calls using the Snapchat App and their associated records such as dates and times of calls, call participants, duration of call, and stored call content if available.

**Content Information:** Records of content collected by Snap Inc. that the Target Account created, such as custom stickers, scans, and information about the content the Target Account create or provide, such as if the recipient has viewed the content and the metadata that is provided with the content.

**Cookies and Other Technologies:** Records of Snap Inc. cookies and other technologies, such as web beacons, web storage, and unique advertising identifiers, to collect information about the Target Account's activity, browser, and device. Additionally, it is requested that Snap Inc. provide whatever information is provided to Snap Inc. partners for advertising and commerce features.

**Device Information:** Records of information collected about the devices the Target Account used to access Snap Inc. services to include information about the hardware and software, operating system version, device memory, advertising identifiers, unique application identifiers, apps installed, unique device identifiers, browser type, language, battery level, and time zone, information from device sensors, such as accelerometers, gyroscopes, compasses, microphones, headphone connection status; and information about the Target Account's wireless and mobile network connections, such as mobile phone number, service provider, and signal strength.

**Device Phonebook:** Records of the Target Account's phonebook or contacts collected by Snap, or identifiers of other Snap user(s) that Target Account recently communicated with.

**Encrypted My Eyes Only Content:** The encrypted contents of the Target Account's "My Eyes Only" file. This file should also contain any relevant metadata such as when the My Eyes Only feature was first and used.

**Filter Information:** Records of filters the Target Account viewed or applied to Snaps, Stories the Target Account watched on Discover, the Target Account's use of Spectacles, and records of submitted search queries. These records shall also include community filter created by the Target Account and associated payment information to include full credit or debit card number and provided cardholder name.

**Location Information:** Records of precise location information associated with the Target Account including GPS, wireless networks, cell towers, Wi-Fi access points, and other sensors, such as gyroscopes, accelerometers, and compass data collected by Snap Inc.

**Log Information:** Log information regarding how the Target Account used Snap Inc. services such as Snaps, Stories, and Chats to include related metadata. Collected logs shall also include records of IP addresses used by the Target account for logins, logouts, and when snaps were sent/received by the Target Account.

**Subscriber Information:** Subscriber Information to include username, password, email address, phone number, date of birth, profile pictures, name, other useful identifying information, and commerce related information such as debit or credit card number and its associated account information.

**Third Parties Records:** Collected information that other users provide about the Target Account when using Snap Inc. services to include the identities of other Snap Inc. users where the Target Account is listed in their phonebook; records of data provided to affiliates and third parties including linked Bitmoji data, notification of installed applications from associated advertisers, and records of interactions with Snap Inc. advertisers.

**Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal justification for the implementation of the following special procedures which shall be employed by the officers who execute this warrant:

**Authenticity of Record ORDER**

IT IS HEREBY ORDERED that the Service Provider listed in the Attachment(s) shall provide a valid "Authenticity of Records" document consisting of an affidavit and that the document be returned to the Affiant along with a copy of the requested records.

**Five Day Record Production ORDER**

IT IS HEREBY ORDERED that the organizations described in this search warrant shall produce the requested records within five (5) days of receipt of this search warrant.

**Adverse Action ORDER**

IT IS ORDERED that Snap Inc. NOT take adverse action against the Target Account(s), such as disabling or terminating the accounts, as a result of the receipt of this warrant.

{%p endif %}

{%p **if** SNAPPRTT %}

**Pen Register and Trap Trace ORDER**

IT IS HEREBY ORDERED THAT Snapchat shall install and use a pen register or a trap and trace device to collect all information not revealing the content of message communication or public posts, but more generally provides information that the communication took place. This information shall be collected by any means available to Snap Inc. that will provide data regarding both sent and received Snaps or Chat messages to include their associated account identifiers, dates and times, associated IP addresses, originating device information, and accounts subscriber information. Furthermore, these records shall include all precise location data, such as GPS coordinates, related to snaps, stories, and interaction by the user with the Target Account. The installation and use of the pen register or a trap and trace device is authorized for a period not to exceed 30 days from the issuance of this warrant.

{%p endif %}

{%p **if** APPLE %}

**Apple Inc.**

**Apple Photos:** Record of the Target Accounts Apple Photos to include contents of the photo library, dates and times of files uploaded or downloaded, total Apple Photos library size, Memories, Photos categorizations, tagged faces within the People album, records of Photos shared with the Target Account with the account identifier of the person who shared the file, and indicators of files within the Hidden folder.

**Customer Information:** Basic registration or customer information to include name, address, phone number, contact information, additional accounts, and dates associated with account creation and/or suspension, iCloud feature connections, and connection logs with IP addresses for the above listed Target Account.

**Customer Service Records:** Information related to contacts with Apple customer service regarding a device or service to include records of support interactions regarding a particular Apple device or service, and information regarding the device, warranty, or repair.

**Digital Legacy Program:** Records of the Target Accounts participation in the Digital Legacy Program to include designated Legacy Contacts and attempts to utilize this service.

**Focus Records:** Records of the Target Accounts Focus settings including indications of scheduled Do Not Disturb sessions and indications of Focus settings being intentionally set of added through Apple contextual suggestions. These records shall also include names of Focus settings created by the Target Account, Driving auto-reply message text, and Target Accounts contacts identified for Urgent Messages.

**Health Records:** Records of data logged within the Target Accounts Health App and utilizing Apple's Health features to such as recorded logs of heart rate, sleep, steps, walking+running distance, step and speed, steadiness, Apple Fitness Ring history, and exercise minutes.

**Hide My Email Records:** A complete list of personal email addresses utilized by the Target Account to include each addresses associated App or service and the user's true email designated as the forwarding email.

**iCloud Content and Backups:** Stored content for the Target Account to include email, stored photos, documents, contacts, calendars, bookmarks, Safari browsing history and iOS device backups. iOS device backups may include photos and videos in the Camera Roll, device settings, app data, iMessage, SMS, and MMS messages and voicemail. Keys, passcodes, or software needed to access the files encrypted by Apple Inc.

**IP Address Logs:** IP address logs related to the Target Account for the specified period to include registration IP address and IP addresses used by the Target Account to access Apple Services. These logs shall also include automated Heartbeat IP addresses associated with the Target Account's registered devices.

**Live Text Visual Lookup:** Records of recognized text, objects and scenes identified by Apple's Live Text feature and indications of what the Target Account did with this information such as conducting a search for the identified item or sending a email to the identified address.

**My Apple ID and iForgot logs:** My Apple ID and iForgot logs to include information regarding password reset actions to include the associated IP addresses. and dates/times of access.

**Notifications:** Records of notifications delivered to the Target Account to include notifying App name and GUID, notification content, and notification delivery date and time.

**Online Purchase Records:** Apple Online Store purchase records to include name of the purchaser, shipping address, telephone number, email address, product(s) purchased, purchase amount, and IP address of the purchase. This purchase occurred using the Target Account.

**Reminder Records:** Reminders set by the Target Account to include Reminder content, date and time due, assigned tags and priority, reminder status as active or complete, and smart lists.

**Safari and Web Data:** Records of the Target Accounts internet activity as recorded by Safari or third party browsers, such as Google Chrome, if available. These records shall include histories of URLs and page titles visited, dates and times of activity, use of voice search features, Page Titles in Tabs at the time of search, utilized privacy protections and browser extensions, and the Target Accounts set start page URL.

**Sign in Logs:** Sign-on activity for the Target Account to Apple services such as iTunes, iCloud, My Apple ID, and Apple Discussions to include collected IP addresses and their associated date, time, and timezone.

**Siri Records:** Records of the Target Accounts use of Siri to include issued commands and stored voice recordings.

**Spotlight Activity:** Records of the Target Accounts Spotlight Activity to include search terms, results, and apps installed due to a Spotlight search.

**Facetime Records:** Records of Facetime calls placed and received to include the account identifier of the calling or recipient parties and data to determine the method of the call, either as audio or video as well as duration. These records shall also include indicators of the use of SharePlay features such as screen sharing and device identifiers of iOS devices used by the Target Account to participate in Facetime calls or SharePlay events.

**Mail Logs:** Apple Mail records to include the contents of incoming and outgoing communications and associated identifiers such as time, date, sender email addresses, and recipient email addresses. These records shall also include email header information and Apple Inc. stored electronic communications such as saved, deleted, sent, stored, & draft email.

**Game Center:** Information regarding Game Center connections including IP addresses, Game Center transactional records, records of the specific games accessed, and the account identifiers of the participants with whom the Target Account has played.

**iTunes Records:** Information regarding iTunes purchase/download transactions and connections, update/re-download connections, and iTunes Match connections. iTunes purchase/download transaction records and records of the specific content purchased or downloaded.

**Apple Card:** All Apple Card records associated with the Target Account to include issue date, detailed transaction history, billing statements, current balance, stored customer information such as signature cards, and records of devices associated with the use of the card.

**Apple Pay Records:** Records of the Target Accounts use of Apple Pay services to include transactions made with retailers and their associated merchant identifiers and receipts, money transfers both sent and received with indicators of the involved accounts, Target Account "Cash" balances, associated cards, and records of Apple Pay being shared with family members.

**Apple Wallet:** Records of stored items within the Target Account's Apple Wallet to include keys, cards, identification, passes and tickets to include images of stored items in an acceptable format such as PNG or JPEG.

**Gift Card Records:** Information related to Apple Store gift cards and iTunes Store gift cards include gift card purchaser information, associated purchase transactions, activation status, redemption status, redemption IP address, subscriber information for the related iTunes account, and items purchased. The requested information is related to the PIN codes listed as the Target Account.

**Retail Store Records:** Point of Sale transactions information to include the type of card associated with a particular purchase, name of the purchaser, email address, date and time of the transaction, and the amount of the transaction that occurred at an Apple Retail Store related to the Target Account. These records shall include duplicate copies of receipts and must include the retail transaction number associated with the purchase. These records shall also include and in-store surveillance video that may show the suspects and evidence of the transaction or attempted transaction.

**AirTag Records:** Records of AirTags associated to the Target Account to include device identifiers, date and time that the device was set-up or added to the account, records of the device being placed in lost mode and when the device was found, and all location data related to said devices for the specified time period.

These requested records shall also include the device identifiers and associated iCloud username of iOS device(s) that connected to or "located" the Target Accounts AirTag device while it was in a lost mode state.

**Apple Maps:** Records of the Target Accounts use of Apple Maps to include addresses of place/business names search for, directions to addresses that the Target Account search for, and dates and times of these searches. Direction records should include selected method of travel such as walking, public transit, or vehicle.

**Find My Records:** Records of the Target Accounts use of Find My the status of Find My being enabled or disabled and Find My transactional activity for requests to remotely lock, play a sound, erase a device and recorded separation alerts. Erasure records should include recorded GPS location information such as final location and other location within the requested search period.

**Location Information:** Records of all location related information to include the last known Target Account location, frequently visited places, and shall include "precise device location", approximated IP address locations, and information from the Target Account use of Apple Apps such as Maps. Location information shall also include the identifiers and specific location (including address or GPS coordinates and location name) of known Bluetooth beacons and Wi-Fi access points that the Target Account observed.

**Homekit Records:** Records of the Target Accounts use of Apple Homekit to include identified address where Homekit is installed, associated Homekit devices such as sensors, remotes, switches, and security systems, user specified room settings, user created scenes and home automations.

**Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal justification for the implementation of the following special procedures which shall be employed by the officers who execute this warrant:

**Authenticity of Record ORDER**

IT IS HEREBY ORDERED that the Service Provider listed in the Attachment(s) shall provide a valid "Authenticity of Records" document consisting of an affidavit and that the document be returned to the Affiant along with a copy of the requested records.

**Five Day Record Production ORDER**

IT IS HEREBY ORDERED that the organizations described in this search warrant shall produce the requested records within five (5) days of receipt of this search warrant.

{%p endif %}

{%p **if** GOOGLE %}

**Google LLC**

**Contacts:** Contacts stored by the Target Account including name, contact phone numbers, e-mails, social network links, and images.

**Device Information:** Records of the device(s) used by the Target Account to access Google LLC services. The records shall include Device attributes including but not limited to operating system information, hardware and software versions, battery level, signal strength, available storage space, browser type, app and file names and types, and plugins; Device operation information about operations and behaviors performed on the device such as whether a window is foregrounded or backgrounded, or mouse movements to help distinguish humans from bots; Unique identifiers, device IDs such as GAID or IDFA, and other identifiers from games, apps or accounts you use, and Family Device IDs, or other identifiers unique to Google Inc. products associated with the same device or account; Device signals including Bluetooth signals and MAC identifiers, and information about nearby Wi-Fi access points, beacons, and cell towers; Data from device settings such as access to GPS location, camera or photos; Network and connection information such as the name of the mobile operator or ISP, language, time zone, mobile phone number, IP address, connection speed and information about other devices that are nearby or on the Target Account network; and Cookie data stored on the Target Account device, including cookie IDs and settings.

**Google Files:** Records of the Target Accounts use of the Google Files app to include the names of files deleted using the Google Files app, if available, and information about files that were synced to Google drive or shared via the app.

**Google Keep:** All Google Keep records to include the content of Keep notes, embedded media, and stored files.

**IP Address Logs:** Information related to IP addresses used for the creation of the account whenever that may have occurred as well as any IP address assigned to the Target Account during the time period specified above.

**Linked Accounts:** Records of all linked external accounts or associated email address, username, or contact information connected to the Target Account including but not limited to recovery email addresses.

**Subscriber Information:** Basic registration or customer information to include name, address, phone number, contact information, additional accounts, and dates associated with account creation and/or suspension for the above listed Target Account.

**Gmail Records:** Google Gmail records related to the Target Account to include subscriber registration information; sign-in IP addresses and associated time stamps; email header information; and all Google LLC stored electronic communications including saved, deleted, sent, stored, & draft email; stored notes; stored chats and chat logs; account histories; attached files to include digital images, videos, documents, links, and any other files associated with the Target Account.

**Google Chat:** Records of the Target Accounts use of Google Chat to include stored copies of messages, threads, and thread participants. Such records shall also include records of collaborations with other users using Google Chat and connection to Google Workspace products.

**Google Messages:** Records of stored Google Messages both synced from Google devices used by the Target account or via Google Messaged for Web for the dates indicated. Such records shall include dates and times of messages, message sender and recipient identifiers, and message content with attachments.

**Google Find My Device:** Records of stored locations for the Target Account's device(s) as recorded by Google's Find My Device service to include the dates and times that the user accessed Find My Device and the location of the device at the time. Such records shall also include device identifiers such as user applied name and recorded device metrics such as "last seen" date, battery and signal level, or nearby devices.

**Google Maps:** Stored Google Map data of location searches conducted by the Target Account, stored maps, "my places" data, and stored markers or "pins".

**Location Information:** Records of location-related information to include the Target Account's location, frequently visited places, and the businesses and people the Target Account is near that Google LLC uses to provide Google Products and ads. Location records shall include "precise device location", IP addresses, and information from the Target Account use of Google Products such as check-ins. Location information shall also include the identifiers and specific location (including address or GPS coordinates and location name) of Bluetooth beacons and Wi-Fi access points that the Target Account's device observed.

**Authorization to implement special procedure(s):** The Affidavit filed herewith has demonstrated legal justification for the implementation of the following special procedures which shall be employed by the officers who execute this warrant:

**Authenticity of Record ORDER**

IT IS HEREBY ORDERED that the Service Provider listed in the Attachment(s) shall provide a valid "Authenticity of Records" document consisting of an affidavit and that the document be returned to the Affiant along with a copy of the requested records.

**Five Day Record Production ORDER**

IT IS HEREBY ORDERED that the organizations described in this search warrant shall produce the requested records within five (5) days of receipt of this search warrant.

{%p endif %}

**PRECLUSION OF NOTICE TO SUBJECT OF GOVERNMENT ACCESS**

IT IS FURTHER ORDERED, that the service provider, in accordance with 18 U.S.C. § 2705(b) “Delay of Notice” will NOT notify any other person of the existence of this warrant and any access of account records by law enforcement. This order is in effect for no less than 90 days from the date the warrant is issued.

**End Attachment “B”**