



WWW.GBGCONSULTING.ORG



SOCIAL MEDIA INVESTIGATIONS

COURSE MANUAL

VERSION 1.1 - UPDATED SEPTEMBER, 2025

LAW ENFORCEMENT SENSITIVE | FOR OFFICIAL USE ONLY (FOUO)



GBG Consulting, LLC. is proud to offer this social media investigations course handbook to law enforcement to support their cases involving social media platforms.

GBG Consulting, LLC. provides quality social media and technology-based investigation training to law enforcement investigators, analysts, and prosecutors. Below are some of the courses we offer:



PLUG
Investigations



SOCIAL MEDIA
INVESTIGATIONS



CHASING
DIGITAL MONEY



LOCATING FUGITIVES
UTILIZING SOCIAL MEDIA



SNAPCHAT
INVESTIGATIONS



CAL ECPA
1546 PC FOR INVESTIGATORS

VISIT OUR WEBSITE FOR INFORMATION ON HOSTING TRAINING!

GBGCONSULTING.ORG



TRADECRAFT TRAINING
FOR LAW ENFORCEMENT PROFESSIONALS

We proudly partner with **Tradecraft Training, LLC.** to provide **WEBINAR BASED** training on the classes above for students. Tradecraft Training also offers great classes by other industry experts and instructors on technology based topics. **Check out their website at www.tradecrafttraining.org to see upcoming classes, or register for a course!**

INTRODUCTION

Welcome to the *Social Media Investigations Student Handbook*, provided exclusively for law enforcement and working prosecutors by **GBG Consulting, LLC**.

This handbook is designed to accompany the various **Social Media Investigations Courses** instructed by GBG Consulting, LLC. The courses are delivered in multiple formats:

- In-person training hosted by law enforcement agencies, prosecutor offices, and at various law enforcement training events, summits and conferences.
- Webinar-based training delivered in partnership with **Tradecraft Training, LLC**, which offers several sessions each year to accommodate a broader audience.

This student manual *is intended to **supplement*** the training provided and particularly covers sample language for the legal process discussed during the course. The actual training courses cover best practices, strategies, and how to review the data productions from various social media platforms, report write it and present it for court.

Here's what to expect from this Student Handbook:

- Sample Affidavit Language Related to:
 - Social Media (Generally / Categorically)
 - Crime on Social Media of Various Types
- Sample "Items to be Seized" lists for Multiple Social Media Platforms
- Sample Affidavit Language Related to the above "Items to be Seized" Lists
- Court Order Language for:
 - Social Media Pen Registers
 - Peer-to-Peer Payment Application Seizures
 - Out of State Warrants to California Social Media Providers
 - Time of Compliance (5 Business Days)

This handbook is a "working document." As such, it is periodically updated by active practitioners, subject matter experts, and working law enforcement officers.

Those reviewing this manual are encouraged to check the **date** on the cover. If this manual appears outdated, former students should login to the Student Portal at www.gbgconsulting.org with their student credentials to download the most current version. Social media is a constantly evolving and ever changing landscape, and investigators are encouraged to seek the most up-to-date information.

DISCLAIMER

This handbook contains law enforcement sensitive information and is intended solely for the students of GBG Consulting, LLC and Tradecraft Training, LLC. The materials provided herein are for the exclusive use of law enforcement personnel who have attended this training. Unauthorized reproduction, distribution, or online posting of this material is strictly prohibited without the prior written consent of GBG Consulting, LLC or Tradecraft Training, LLC.

This handbook is intended for training and reference purposes only. It does not constitute legal advice. The investigative guidance, examples, and suggested legal process language contained herein are general in nature and may not address the specific legal standards, procedures, or requirements of every jurisdiction. Laws governing search warrants, subpoenas, and other forms of legal process may vary significantly between states, judicial districts, and individual courts.

Students and investigators using this handbook are strongly encouraged to consult with their agency's legal counsel, local prosecutors, or other legal advisors familiar with their applicable state and federal laws prior to drafting, submitting, or executing any legal process.

While this handbook offers examples of search warrant language and affidavit templates, these examples are intended to serve as a reference for crafting individualized legal documents based on the facts of each case. Investigators should not copy or submit any language from this handbook verbatim without proper legal review and agency approval.

GBG Consulting, LLC provides this handbook "as-is" with no warranties, guarantees, or representations as to its legal sufficiency or applicability. By participating in this training and utilizing the materials provided, students agree to hold harmless GBG Consulting, LLC,, their instructors, staff, and affiliates from any liability, claims, or consequences that may arise from the use or reliance upon this handbook or the information contained herein.

TABLE OF CONTENTS

EDUCATE YOURSELF ON THE PLATFORM(S) TARGETED.....	7
TECHNIQUES TO LEARN ABOUT A PLATFORM.....	8
THE EVOLVING DIGITAL LANDSCAPE OF SOCIAL MEDIA	9
STRUCTURE OF A SOCIAL MEDIA SEARCH WARRANT	10
AFFIDAVIT LANGUAGE: SOCIAL MEDIA DEFINITION	11
AFFIDAVIT LANGUAGE: SOCIAL MEDIA STATISTICS	14
AFFIDAVIT LANGUAGE: CRIME SPECIFIC	16
PLATFORM SPECIFICS: ITEMS TO BE SEIZED	24
FACEBOOK	26
INSTAGRAM.....	40
WHATSAPP.....	53
SNAPCHAT.....	60
TELEGRAM	71
SIGNAL	77
TIKTOK	78
X (FORMERLY TWITTER).....	88
REDDIT	96
KIK MESSENGER.....	105
DISCORD	111
YOUTUBE.....	120
TINDER	131
BUMBLE.....	138
HINGE	146
GRINDR	153
ONLYFANS	161
CASHAPP.....	169
VENMO	177

TEXT MESSAGING APPLICATIONS / VOIPS	184
OTHER SOCIAL MEDIA PLATFORMS: WHAT TO DO	191
COURT ORDERS: SOCIAL MEDIA PEN REGISTERS	194
COURT ORDERS: SEIZURES FROM P2P PAYMENT APPS	197
COURT ORDERS: OUT OF STATE WARRANTS TO CA	198
COURT ORDERS: CALIFORNIA TIME OF COMPLIANCE	199
TOOLS & RESOURCES	200
CONCLUSION	202

EDUCATE YOURSELF ON THE PLATFORM(S) TARGETED

When preparing legal process directed at social media providers, it is critical that investigators take the time to thoroughly research and understand the specific platform(s) they are targeting.

Each platform is different: What it enables users to do, how users communicate on it, what types of data it collects, what records are retained, how long data is preserved, and how legal process should be properly worded to obtain the information sought. A lack of familiarity with the social media platform(s) you're working with can pose challenges.

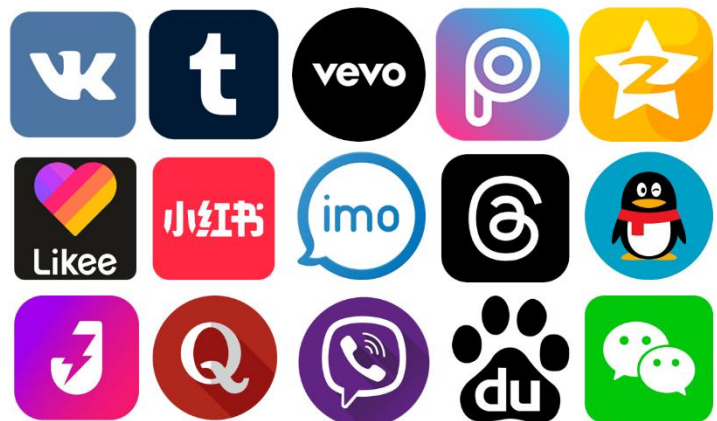
Judges, juries and even prosecutors are relying on you as the investigator to explain how the platform works. Many magistrates and jurors do not personally use platforms such as Snapchat, Instagram, or Telegram, and may have little understanding of how these services function in real-world criminal investigations.

It is easy to copy and paste language from this handbook, or to rely on templates and prior warrants to draft your legal process, submit it, receive the records, locate a highly incriminating video, and book that video into evidence. **But if you cannot explain to a jury how Instagram functions, what an “Instagram Story Archive video” is, how you located that video within the production, or why that specific content exists on the platform, the evidentiary value of your discovery is significantly diminished.** As investigators, our job is not only to locate digital evidence, but to be fully prepared to explain to prosecutors, judges, and juries what that evidence is, how it was obtained, and why it is reliable.

By demonstrating your knowledge of the platform's functionality, you strengthen your affidavit against potential defense challenges. Vague or generic language can invite motions to suppress if the court concludes that your request was speculative or lacked proper factual foundation. Taking the time to research the platform and accurately describe its features helps ensure your affidavit is thorough, persuasive, and legally sound.

Not to mention – social media is bigger than we know. Each icon to the right represents a social media platform, available for download in the US, with more than **100 million** daily users. Yet, we won't recognize most of them.

We may never know what social media platforms we may one day need to author legal process for related to an important case.



TECHNIQUES TO LEARN ABOUT A PLATFORM

Before we get started, we need to ask ourselves an important question:

Can I author legal process to this social media platform?

Of course, the answer is *technically* yes. We could write legal process to whatever we have probable cause for – but, before we do, we should consider if they even have data to produce (IE: Signal Messenger has **nothing** for us), if they are an overseas provider that will even respond to US legal process, and what data they retain.

To find out, consider the following resources:



Visit the platform's website

Check for a law enforcement page or guide that might help you understand what data is available and how they respond to legal process.



Check the application's page on NDCAC

An exclusive resource for law enforcement investigators, the NDCAC has extensive information on various platforms available to us.



Check the Search.org ISP List

Another great resource constantly updated by law enforcement investigators, Search.org's ISP list may have additional information.



Check Klovings's Law Enforcement Forum

Connect with other investigators and search for past posts, templates, or make a post asking about a specific platform that you're looking into.

Once you've determined what data is available with you and decide to move forward, now you need to learn more about the application. Consider:

1. Reviewing the platform's **privacy policy** to see what data they retain.
2. Speaking with the **victim** (if there is one) and having them walk you through the social media platform, how they used it and communicated with the suspect.
3. Conduct internet searches for guides or videos on how to use the platform.
4. **Download the platform yourself** and try it out with your partners at work to gain first-hand knowledge and experience with the social media platform.

THE EVOLVING DIGITAL LANDSCAPE OF SOCIAL MEDIA

As investigators, it's important to recognize that social media platforms are constantly evolving and sometimes disappearing altogether.

Take **Myspace** for example; one of the largest and most dominant social networking platforms in the early 2000s, Myspace rapidly declined as newer platforms like Facebook, Instagram, and Snapchat emerged. Today? Myspace is functionally obsolete.

Or perhaps circa 2015 you downloaded **Vine** for some entertainment on those long graveyard shifts. Vine was a short-form video platform that gained massive popularity for its six-second looping videos, but was discontinued *entirely* in 2017 after losing market share to competitors like Instagram and TikTok. Vine's servers were shut down, its data archived or deleted, and it no longer exists.

These examples highlight a critical point for investigators: **social media platforms come and go**. Sure, applications like Facebook, Instagram and Snapchat dominate the market today – but that **will change**. Companies merge or are sold, providers shut down services, and new platforms rise in popularity. Who had even heard of **Telegram** before 2023?

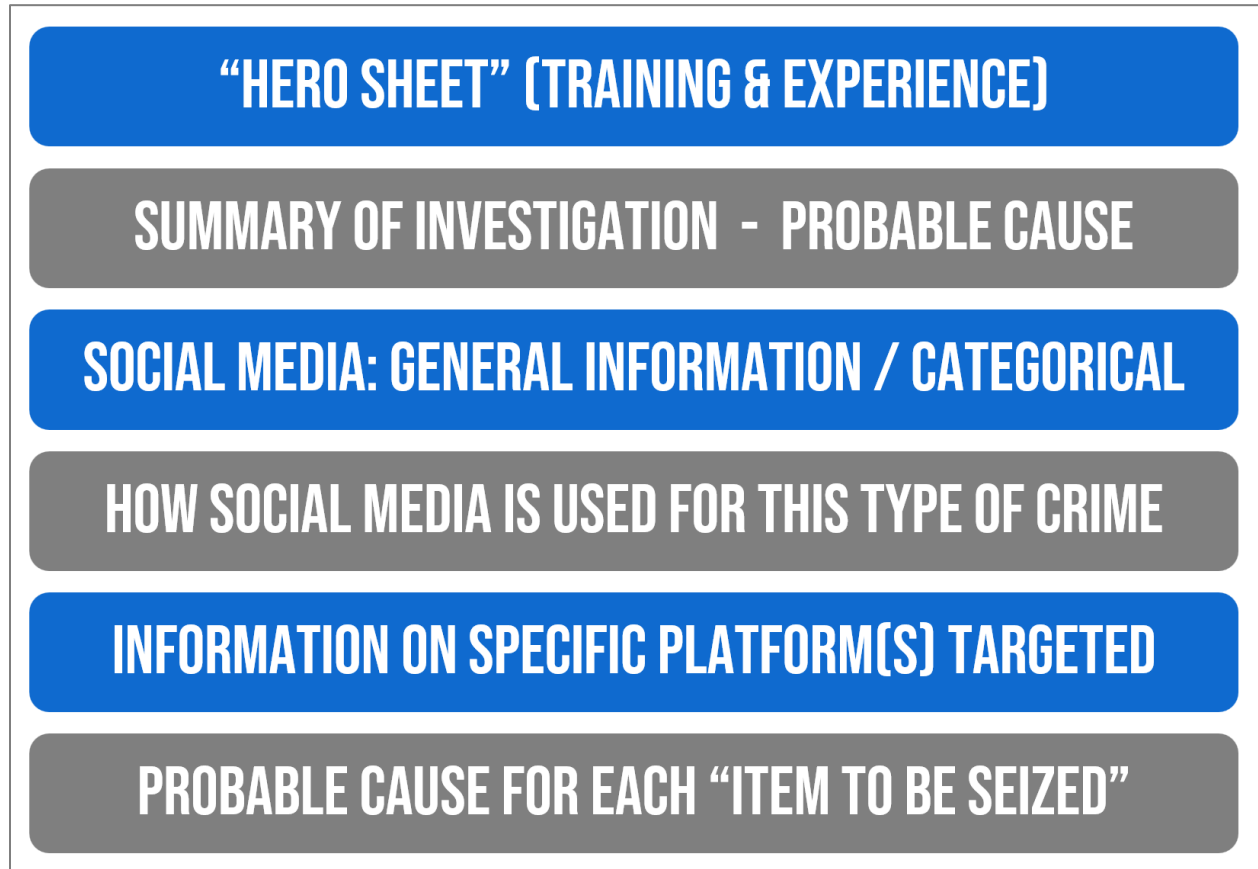
And even more important, to continue dominating the market, social media platforms are **frequently releasing new features** or changing. This is why simply recycling old affidavit language is risky, and a great way to miss valuable evidence. If the “go-by” template you are referencing was from 2015, I can almost guarantee that the platform has rolled out *numerous* new features and you are **not** asking for any of that valuable evidence.



(Once popular but now obsolete social media platforms.)

STRUCTURE OF A SOCIAL MEDIA SEARCH WARRANT

A typical affidavit for a social media provider can be structured as follows:



We can omit discussion of the first two standard sections commonly included in search warrants — the **Hero Sheet** and the **Summary of Investigation** — as these are widely recognized industry standards and are typical for most affidavits we author.

After establishing the affiant’s qualifications to offer expert opinions and draw investigative conclusions, and after outlining the probable cause, factual details of the offense under investigation, and the court’s jurisdiction to issue the requested warrant, we will turn our attention to the **social media-specific portion** of the search warrant. The following sections will break down how to effectively draft this portion of the affidavit.

Another consideration – many jurisdictions allow investigators to write to **multiple social media platforms** in the same warrant. I do this frequently – but just remember, you’ll need to describe *each* social media platform in your affidavit and these “combined” warrants can get wordy / lengthy.

AFFIDAVIT LANGUAGE: SOCIAL MEDIA DEFINITION

When drafting legal process directed to social media platforms, investigators should remain mindful that not all reviewing parties — including judges, magistrates, prosecutors, and defense counsel — are necessarily familiar with how social media operates, or may not personally utilize these platforms. For this reason, search warrants and affidavits should generally include foundational language that briefly explains what social media is, how users interact with it, and why records from these platforms are often relevant to criminal investigations.

One of the frequent challenges investigators encounter, however, is determining how to appropriately define “social media” within affidavits or while testifying within the courtroom.

The term “**social media**” itself is *broad* and encompasses a diverse and constantly evolving group of platforms, applications, and online services. Social media includes platforms that allow users to create profiles, share multimedia content, send private or group messages, engage in real-time communication, conduct financial transactions, and participate in online communities or interest groups. While the specific features and functions may vary from platform to platform, many share common elements that make them attractive tools for both lawful communication and criminal activity.

By incorporating a basic explanation of the general nature of social media, along with brief platform-specific descriptions, investigators strengthen the foundation of their legal process and assist judicial officers in understanding the significance of the requested records.

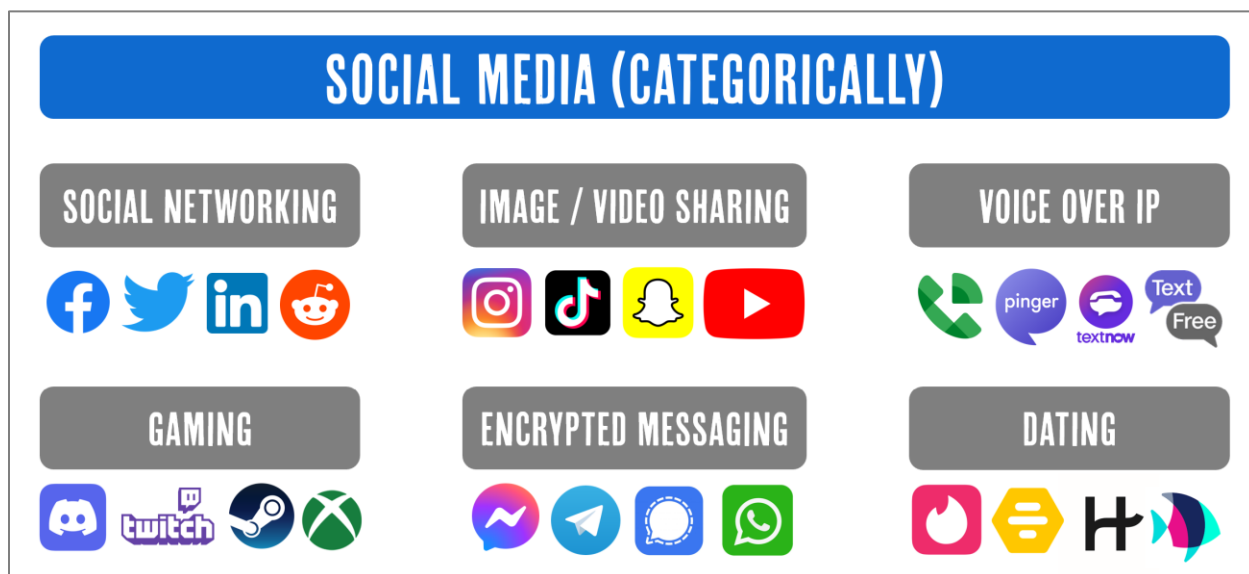
Example Affidavit Language Definition Social Media (Generally):

Based on my training and experience, I am aware that social media platforms are online services which allow users to create personal profiles or accounts, post and share content such as text, photographs, videos, and live streams, and communicate with other users through private messages, group chats, and public comment threads.

Such platforms include, but are not limited to, services such as Facebook, Instagram, Snapchat, TikTok, Telegram, WhatsApp, Discord, CashApp, and *many* others. While the specific features vary from platform to platform, many social media platforms allow users to message other users, conduct video or voice calls, participate in online communities, chats, or forums, and share multimedia. A majority of social media platforms are commonly accessible through mobile applications or internet-connected devices such as smartphones, tablets, and computers.

As emphasized throughout this course, investigators will find it significantly more effective to explain and testify about social media **categorically**, rather than relying on broad or overly generalized definitions.

As seen in the below example graphic, social media can easily be presented and explained when investigators consider various platforms “grouped” together based on similar functionality, features, and available evidence:



Imagine testifying in front of a jury about Instagram and Snapchat evidence you uncovered during a sex crimes investigation. Now, further imagine that more than *half* of the jury has never used Instagram, and *several* jurors have never used any form of social media. **This** is the realistic challenge we face. In this case, we would have no need to try and explain gaming or dating applications: We would simply describe social media in general (explaining it categorically) and then *focus* on image and video sharing applications, particularly Instagram and Snapchat.

Example Affidavit Language Definition (Categorically):

Based on my training and experience, I am aware that the term "social media" broadly encompasses a wide variety of online platforms and mobile applications, which can be categorized based on their primary functions and features.

Certain well-known platforms, such as Facebook, X (formerly Twitter), and Reddit, serve primarily as social networking and community discussion platforms, allowing users to share written posts, upload multimedia content, participate in shared-interest groups (such as Facebook Groups and Subreddits), and communicate directly with other users through private or group messaging features.

[Continued on Next Page]

Other social media platforms are primarily oriented toward multimedia sharing. Applications such as Instagram, TikTok, Snapchat, and YouTube focus on the creation and distribution of photographs and video content. Each platform offers distinct methods for users to create, upload, and share multimedia content with others, including features such as Instagram “Stories,” Snapchat “Snaps,” TikTok videos, YouTube “Shorts,” and live streaming capabilities.

In addition, some platforms are designed to connect users around specific subcommunities or interests. Online dating applications, such as Bumble and Tinder, allow users to create personal profiles for the purpose of seeking romantic relationships, while gaming platforms, including Discord, Xbox Live, and PlayStation Network, allow users to engage in voice, video, and text communication with others who share gaming-related interests.

Imagine testifying in front of a jury about Instagram and Snapchat evidence you uncovered during a sex crimes investigation. Now, further imagine that more than *half* of the jury has never used Instagram, and *several* jurors have never used any form of social media. **This** is the realistic challenge we face. In this case, we would have no need to try and explain gaming or dating applications: We would simply describe social media in general (explaining it categorically) and then *focus* on image and video sharing applications, particularly Instagram and Snapchat.

AFFIDAVIT LANGUAGE: SOCIAL MEDIA STATISTICS

Including this portion may **not** be necessary in cases where a direct and specific nexus already exists between criminal conduct and the targeted social media platform. *For example*, if a juvenile victim reports that an adult suspect engaged in exploitation specifically through Discord, the connection to that platform is clear and well-established.

However, it is not uncommon for investigators to seek search warrants directed to social media providers based on a reasonable belief that the suspect likely maintains one or more social media accounts, even when definitive evidence confirming the existence of those accounts is not yet available.

For instance, consider a scenario where a suspect is identified in connection with a burglary based on a cellular “area” dump, and the subscriber information indicates the phone is a prepaid device with no subscriber name attached. In such circumstances, investigators may submit that phone number to platforms such as Facebook, Instagram, or Snapchat in an effort to determine whether the suspect has registered social media accounts tied to that number, which could assist in positively identifying the suspect and corroborating their possession of the device.

In these situations, it is critical that the affidavit articulates why it is probable that the suspect maintains social media accounts on the platforms being targeted. This belief should be supported by facts, investigative experience, and, when appropriate, statistical data illustrating the prevalence of social media usage across the relevant demographic groups.

Example Affidavit Language for Social Media Statistics:

Based on my training and experience, I am aware that individuals who utilize mobile devices, such as smartphones, commonly maintain accounts with one or more social media platforms. Social media platforms frequently require or allow users to register accounts using personally identifiable information such as a phone number, email address, or device identifier. Even when a suspect’s identity is not fully confirmed, account registration data maintained by social media providers can assist law enforcement in identifying individuals associated with specific devices, phone numbers, or online activity.

Based on my training and experience, I believe it is highly probable that the suspect(s) in this case may have used the identified phone number to register accounts on one or more widely used social media platforms, including but not limited to Facebook, Instagram, Snapchat, and CashApp.

[Continued on Next Page]

Furthermore, based on national statistics and my training and experience, the overwhelming majority of individuals in the suspect's demographic group utilize social media. For example, recent studies by the Pew Research Center indicate that approximately 83% of adults in the United States use at least one social media platform, with usage rates approaching 99% for individuals between 18 and 29 years of age. These platforms frequently retain extensive subscriber information, including registration data, device connections, login history, IP addresses, and communication records, which may provide evidence relevant to the identity and activities of the suspect.

As demonstrated in the language above, probable cause has been established despite the absence of a direct link between the crime under investigation and the specific social media platform(s) targeted by the legal process.

The affidavit articulates a reasonable belief that records obtained from these platforms may contain evidence useful in identifying the suspect. Furthermore, based on the exceptionally high rates of social media usage reflected in national statistics, it is probable that the suspect maintains one or more accounts on the platforms identified. These usage rates far exceed the threshold of probability commonly associated with the legal standard for probable cause (51%).

AFFIDAVIT LANGUAGE: CRIME SPECIFIC

The next step is to establish a foundation explaining how offenders commonly utilize social media to facilitate the type of criminal activity under investigation. Given the wide variety of offenses that may involve social media in some capacity, it would be impractical to outline every possible scenario. Instead, the following examples are provided to serve as a starting point for crafting similar language tailored to the specific crime(s) you're investigating.

AUTOMOTIVE THEFT & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in auto theft frequently utilize social media platforms to facilitate various aspects of their criminal activity. Offenders may use platforms such as Facebook Marketplace, OfferUp, Instagram, Snapchat, and Telegram to advertise stolen vehicles or vehicle parts for sale, often attempting to quickly offload stolen property to unsuspecting buyers or co-conspirators.

I am further aware that social media also allows offenders to coordinate vehicle theft operations by communicating with associates regarding target vehicles, locations, and logistics in real time, often through private messaging features or encrypted messaging apps. In fact, I am aware that is relatively common for “scouts” to actively go search for high end vehicles parked in locations where they could easily be stolen (such as on the street, parking lots, etc.) and to sell these locations (commonly referred to as “Pin Drops”) to crews who actually perpetrate the auto thefts, oftentimes being paid digitally through social media platforms such as CashApp.

Additionally, based on my training and experience, I am aware that individuals involved in auto theft may post photos or videos of themselves with stolen vehicles, high-end cars, or vehicles obtained through fraudulent means, either for personal bragging rights or to promote their criminal enterprises. These postings often occur on platforms such as Instagram, Snapchat, and TikTok, where offenders can showcase vehicles or parts to wide audiences. Even when direct evidence of stolen vehicles is not posted publicly, they may be shared privately through private stories, direct messages, or discussed through private conversations.

ORGANIZED BURGLARY & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in organized burglary crews often utilize social media platforms to plan, coordinate, and communicate about their criminal activity. These crews frequently consist of multiple individuals with designated roles, such as lookouts, getaway drivers, and individuals tasked with entering and stealing property. Social media platforms — including group messaging features

[CONTINUED ON NEXT PAGE]

within Instagram, Snapchat, Telegram, and WhatsApp — are commonly used to facilitate real-time communication during the commission of these crimes, as well as to coordinate meeting locations, identify potential targets, or share information about surveillance or law enforcement presence in specific neighborhoods or retail areas.

In addition, based on my training and experience, I have observed that members of organized burglary crews may use social media to advertise or sell stolen property, particularly through online marketplaces such as Facebook Marketplace, OfferUp, or encrypted Telegram channels. It is also common for suspects to post photos or videos of high-value items, large amounts of cash, or luxury goods obtained through criminal activity, either to promote their status within the group or to attract buyers. These social media accounts, even when set to private or using fictitious usernames, often retain subscriber information, private messages, and media files that can provide valuable evidence linking individuals to the broader burglary crew, the stolen property, or the criminal conduct itself.

DRUG TRAFFICKING / SALES & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in drug trafficking frequently utilize social media platforms to advertise, arrange, and facilitate narcotics sales. Platforms such as Snapchat, Instagram, Facebook, and Telegram are commonly used to post photographs and videos of controlled substances, promote availability of drugs, advertise pricing, and communicate with buyers. These communications often occur through private messaging features, story posts, encrypted group chats, or disappearing message functions specifically designed to avoid detection by law enforcement.

In addition, based on my training and experience, I know that drug traffickers often use social media to expand their customer base, maintain contact with regular buyers, and coordinate delivery logistics. Many traffickers use emojis, coded language, slang terms, or hashtags to advertise the sale of narcotics in a manner intended to be recognizable to buyers while attempting to avoid scrutiny from law enforcement or platform moderators. Even when direct drug-related postings are not publicly viewable, social media accounts frequently contain subscriber information, communication records, media files, financial transaction discussions, and other metadata that can serve as valuable evidence in narcotics investigations.

Furthermore, I am aware that drug traffickers oftentimes accept payments for the sale of illicit controlled substances through peer-to-peer payment applications such as CashApp.

FIREARMS TRAFFICKING & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in firearms trafficking frequently utilize social media platforms to advertise, coordinate, and facilitate the illegal sale and distribution of firearms. Platforms such as Snapchat, Instagram, Facebook, Telegram, and various encrypted messaging applications are commonly used to post photographs or videos of firearms for sale, communicate with potential buyers, negotiate prices, and arrange meeting locations for unlawful transactions. Many of these communications occur through private direct messaging, encrypted group chats, disappearing message features, or closed online communities designed to limit law enforcement visibility.

Additionally, based on my training and experience, I know that firearms traffickers often exploit social media platforms to promote their inventory, establish reputations within criminal networks, and connect with a broad pool of potential customers, including prohibited possessors and individuals seeking firearms for criminal purposes. Offenders may display firearms, high-capacity magazines, or modifications (such as switches, extended magazines, or suppressors) in photos or videos posted online, sometimes alongside currency, narcotics, or other contraband. Even when explicit transaction details are not publicly visible, social media accounts often retain valuable evidence including subscriber data, private communications, photographs, IP addresses, device associations, and location metadata that can assist law enforcement in identifying individuals involved in the unlawful trafficking of firearms.

ROBBERIES & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in robbery schemes frequently utilize online marketplace platforms and social media applications to lure victims under the pretense of legitimate transactions. Offenders oftentimes post fraudulent advertisements for items such as vehicles, electronics, or high-value goods on platforms including Facebook Marketplace, OfferUp, Craigslist, and Instagram, as well as within private groups or chat applications such as Telegram and Snapchat. After contacting unsuspecting victims who respond to these ads, suspects arrange in-person meetings at predetermined locations where they commit armed robberies or thefts instead of completing the advertised sale, essentially “setting up” the victim to come to the pre-designated location with a large sum of cash.

I am further aware that individuals involved in these types of schemes commonly use social media to communicate with co-conspirators, coordinate the logistics of planned robberies, and discuss target selection or division of proceeds. Offenders may also use social media to publicly display large amounts of cash, expensive merchandise, or luxury items obtained through criminal activity in order to enhance their reputation, intimidate rivals, or promote themselves within criminal circles. These types of postings, along with subscriber data, private communications, account activity logs, and metadata maintained by social media providers, often contain valuable evidence that can link suspects to the planning and commission of these robbery schemes.

CHILD EXPLOITATION & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in the sexual exploitation of minors frequently utilize social media platforms, messaging applications, and gaming platforms to identify, groom, and exploit juvenile victims. Offenders often initiate contact with minors through platforms such as Snapchat, Instagram, TikTok, Discord, Kik, Telegram, and gaming-related chat features. These platforms provide offenders with access to large numbers of minors, many of whom maintain public profiles, share personal information, and may be susceptible to online grooming techniques.

I am further aware that offenders may use private messaging, disappearing content features, encrypted chat functions, and live video capabilities to engage in sexually explicit conversations, solicit sexually explicit images, and arrange in-person meetings for unlawful sexual contact. Offenders may also coerce, threaten, or blackmail victims into continued exploitation, often using prior communications or images as leverage.

I am further aware that individuals involved in these offenses may use multiple social media platforms simultaneously to exploit victims, communicate with co-conspirators involved in the production or distribution of child sexual abuse material, or to share or trade illegal content within closed online groups and encrypted channels. Offenders may also use social media to boast about their conduct to others within these illicit communities, seek validation, or recruit additional victims.

CHILD SEXUAL ABUSE MATERIAL & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in the possession, production, and distribution of child sexual abuse material (CSAM) frequently utilize social media platforms, encrypted messaging applications, and peer-to-peer networks to exchange illegal content and communicate with other offenders. Platforms such as Telegram, Kik, WhatsApp, Snapchat, Discord, and various darknet forums are commonly used to store, trade, and distribute CSAM due to features such as end-to-end encryption, disappearing messages, private groups, and anonymity.

I am further aware that offenders engaged in CSAM distribution often participate in online communities where they exchange illegal content, discuss methods to avoid law enforcement detection, share grooming techniques, and encourage one another's criminal behavior. Many offenders maintain extensive collections of illegal material on personal devices, cloud storage accounts, and social media messaging platforms. Even when content is deleted or concealed, account subscriber information, chat logs, group memberships, IP connection history, cloud backups, device identifiers, and associated metadata maintained by these platforms often contain critical evidence linking offenders to the possession, receipt, production, or distribution of CSAM. Additionally, social media records may identify co-conspirators, previously unknown victims, and devices used to create or traffic CSAM content.

FRAUD / IDENTITY THEFT & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in fraud and identity theft frequently utilize social media platforms, messaging applications, and online marketplaces to obtain, share, and exploit personally identifiable information (PII), as well as to advertise and facilitate fraudulent transactions. Offenders may use platforms such as Instagram, Snapchat, Facebook, Telegram, WhatsApp, and encrypted dark web forums to buy, sell, or trade stolen identities, compromised financial information, credit card data, account credentials, and counterfeit documents. Social media provides offenders with broad access to potential victims, co-conspirators, and customers for fraudulent goods or services.

I am further aware that suspects often use social media to communicate with co-conspirators regarding fraud schemes, advertise fraudulent services such as “credit repair,” “cash flipping,” or “bank drops,” and solicit individuals to participate in fraudulent activity, oftentimes under false pretenses. Offenders may also display large amounts of cash, high-end merchandise, or luxury items obtained through fraudulent means to promote their status and attract additional participants. Even when overtly fraudulent posts are not publicly viewable, social media platforms maintain subscriber data, private message histories, financial transaction discussions, IP logs, device associations, and other metadata that often contain valuable evidence directly linking suspects to identity theft, financial fraud, and related criminal conduct.

ORGANIZED RETAIL THEFT & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in organized retail theft (ORT) often utilize social media platforms to coordinate theft operations, recruit participants, and advertise stolen merchandise for resale. Offenders may use platforms such as Facebook Marketplace, Instagram, Snapchat, TikTok, Telegram, and encrypted messaging applications to communicate with co-conspirators regarding target locations, store layouts, security vulnerabilities, and escape routes. Group chats, private messages, and encrypted channels allow offenders to organize large-scale thefts involving multiple participants acting in concert, often across multiple jurisdictions.

I am further aware that suspects frequently use social media platforms such as Facebook Marketplace and OfferUp to advertise and resell stolen merchandise at discounted prices, often promoting high-end clothing, designer handbags, electronics, cosmetics, and household goods. Offenders may also post videos showcasing stolen property, large amounts of cash, or luxury items obtained through retail theft operations as a means of recruiting others, enhancing status, or concealing the true origin of the stolen goods under the guise of “small business” or “side hustle” operations. Even when public posts are deleted or accounts are set to private, subscriber data, private messages, transaction records, IP logs, device associations, and other metadata maintained by these platforms often contain critical evidence linking suspects to organized retail theft operations.

HUMAN TRAFFICKING & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in human trafficking and commercial sexual exploitation frequently utilize social media platforms and online applications to recruit, advertise, control, and exploit victims for financial gain. Offenders commonly use platforms such as Snapchat, Instagram, Facebook, TikTok, and encrypted messaging applications like Telegram, WhatsApp, and Signal to identify vulnerable individuals, initiate contact, and establish coercive relationships designed to manipulate victims into engaging in commercial sex acts.

I am further aware that traffickers often advertise victims for prostitution through online postings that include photographs, pricing, and contact information. These advertisements may be circulated via social media profiles, encrypted messaging groups, or third-party escort websites that are linked to social media accounts. Offenders frequently use social media to communicate with co-conspirators, coordinate meetings with buyers (also referred to as “johns”), arrange transportation, and collect payments. Traffickers may also utilize social media to intimidate, monitor, or threaten victims, as well as to display large amounts of cash or luxury goods obtained through trafficking operations as a means of recruiting additional victims or promoting their criminal enterprise.

SIDESHOWS & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in illegal sideshows and street takeover events frequently utilize social media platforms to promote, coordinate, and document these unlawful activities. Platforms such as Instagram, Snapchat, TikTok, Facebook, Telegram, and encrypted group messaging apps are commonly used to announce upcoming events, share locations, recruit participants, and broadcast live videos of ongoing sideshows. Organizers often post flyers or coded invitations online to quickly disseminate information to large groups, while avoiding detection by law enforcement.

I am further aware that participants and organizers frequently post photos and videos of themselves engaging in dangerous driving maneuvers, including “donuts,” high-speed racing, burnouts, and blocking public intersections. These postings are often used to promote status within the street racing community, attract larger crowds, and build online followings.

Even when public content is removed or restricted, social media platforms maintain subscriber records, private communications, metadata, device associations, and location data that can provide critical evidence identifying individuals involved in organizing, promoting, and participating in sideshow and street takeover activity.

GANG CRIME & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in gang-related criminal activity frequently utilize social media platforms to promote gang affiliation, recruit new members, coordinate criminal conduct, and intimidate rivals. Platforms such as Instagram, Snapchat, Facebook, TikTok, YouTube, Telegram, and encrypted messaging applications are often used to share photos and videos displaying gang signs, colors, firearms, narcotics, and large amounts of cash, often alongside music videos or posts designed to enhance reputation and status within the gang.

I am further aware that gangs frequently use social media to communicate with co-conspirators regarding planned acts of violence, retaliation against rival gangs, drug trafficking operations, and firearms trafficking. Offenders may post threats directed at rival gang members or challenge rival gang members through social media.

SCHOOL / ACTIVE SHOOTER THREATS & Social Media Example Language:

Based on my training and experience, I am aware that individuals who make violent threats, including threats of mass violence, school shootings, or other acts of targeted violence, often utilize social media platforms to post, share, or distribute these threats. Platforms such as Snapchat, Instagram, TikTok, Discord, YouTube, and various encrypted messaging applications are commonly used to publish written statements, videos, or images containing threats directed at schools, public events, specific individuals, or groups. These threats may be posted publicly, shared within private groups, or transmitted through direct messaging features.

I am further aware that suspects engaged in this type of behavior may use social media to seek attention, provoke fear, recruit others to join in planned acts of violence, or engage in ideologically motivated discussions that glorify past acts of mass violence. In some cases, offenders may live-stream threatening conduct, display firearms or tactical gear, or reference previous violent incidents as inspiration.

SEXTORTION & Social Media Example Language:

Based on my training and experience, I am aware that individuals engaged in extortion and sextortion schemes frequently utilize social media platforms to identify, contact, and exploit victims for financial gain. Offenders commonly initiate contact through platforms such as Instagram, Snapchat, Facebook, WhatsApp, TikTok, or encrypted messaging applications. Once communication is established, offenders often deceive victims into sharing compromising images, videos, or personal information, which is then used to threaten, blackmail, or coerce the victim into paying money. Offenders may threaten to publicly release the compromising material to the victim's family, friends, or employer unless demands are met. Social media platforms are central to the initiation, facilitation, and escalation of these extortion schemes.

HOMICIDE & Social Media Example Language:

Based on my training and experience, I am aware that individuals involved in homicides and related violent crimes frequently utilize social media platforms before, during, and after the commission of the offense.

Platforms such as Instagram, Snapchat, Facebook, and Telegram serve as communication tools that allow suspects to coordinate criminal activity, document violent acts, communicate with co-conspirators, and sometimes even boast about or reference their involvement in homicides. Social media plays a significant role in the activities of individuals involved in retaliatory violence, gang conflicts, targeted shootings, and interpersonal disputes that escalate to homicide.

I am further aware that suspects may use private or group messaging features to communicate plans to carry out acts of violence, share information regarding intended victims, arrange transportation or weapons acquisition, or coordinate with accomplices in the moments leading up to a homicide.

Following the commission of the crime, offenders may post or share content indirectly referencing the incident, including taunts directed at rival groups, coded messages, song lyrics, or cryptic references to recent violence. In some cases, suspects have posted photographs, videos, or status updates that celebrate, mock, or threaten others in the wake of a homicide, particularly when rival groups or gang affiliations are involved. In other cases, suspects have discussed homicides through private messages with friends or family members, or discussed specific acts after the homicide such as disposing of a murder weapon, concealing evidence, or eluding law enforcement.

Additionally, I am aware that associates or witnesses may also use social media to discuss details of homicides, share rumors or information not yet disclosed publicly, and disseminate recordings of related incidents. In modern investigations, social media platforms often serve as key sources for identifying relationships between suspects and victims, discovering motive, establishing premeditation, tracking retaliatory actions, and corroborating timelines of events surrounding the homicide.

As demonstrated in the preceding examples, the purpose at this stage of the search warrant affidavit is to establish a general foundation, based on the affiant's training and experience, explaining how individuals engaged in the particular criminal offense under investigation may utilize social media, and why evidence relevant to the offense is likely to be found on the identified platforms.

The examples provided are intentionally broad and intended to serve as reference points for investigators. They may be used as a starting point when drafting similar language tailored to the specific facts and circumstances of a particular investigation. However, best practice is to expand upon these examples by incorporating case-specific details, observations, and facts directly relevant to the investigation at hand, and to rely on the affiant's personal training, experience, and investigative knowledge rather than relying solely on these generalized summaries.

PLATFORM SPECIFICS: ITEMS TO BE SEIZED

The next large section of this handbook will include a breakdown of a number of social media platforms (Facebook, Instagram, WhatsApp, Snapchat, etc.) that investigators may need to author legal process to. Each application's pages will include information on:

- Basic information on the platform (for investigators who are unfamiliar);
- How to serve the platform with legal process;
- Where to address your legal process (IE: "Location to be Searched");
- An example "Items to be Seized" list;
- An example of effective affidavit language;
- Any additional information on that specific application that is useful for investigators to know when writing legal process;

I will regularly update this manual as new applications become prevalent, data retention policies change, and other new information becomes known.

It is not possible to cover every social media platform, so if you are trying to write for a platform that is not included within this handbook, refer to the section titled "**Other Social Media Platforms: What To Do**" for additional information.

Search Warrants to Social Media – Important Considerations

DON'T just Copy & Paste from Examples: This is a practice law enforcement should be getting away from as much as possible. We want our warrants to be current, up to date with platforms, based on our own expertise, and with a strong nexus to the specific facts of our investigation / case. The exemplars in this manual are *generic* on purpose: To give you an idea of how to write yours.

Be THOROUGH with your "Items to be Seized": Many social media providers (Meta, Snapchat, etc.) are **very** particular in reviewing our items to be seized list and deciding what information to give us. *Example: If you don't specifically ask for Instagram Archive Stories and just say "Stories," you likely won't get them.* With that in mind, our "Items to be Seized" lists should be lengthy and extremely thorough.

Avoid Outdated / Old Templates: Most of us probably have a "template" folder we got from a class we took in 2016, or that have been passed around amongst our local agencies for years. Take a hard look at those before you use them – social media is constantly changing, the platforms are rolling out *new features* that may contain *valuable evidence* every week. If we're using a warrant template from 2016, we're likely leaving behind *a lot* of information and data.

Avoid "Any and All" Language: If you write "any and all data, records, and content" in your list of Items to Seize, social media providers tend to consider this *overbroad* and

not *specific or narrowly tailored*. Break it down – describe the subscriber records you want with specificity: Usernames, full names, birthdates, email addresses, etc.

Don't be TOO Specific: Social media providers *won't* analyze your data for you. We see people write warrants that read “any messages between the Target Account and [Victim].” For most platforms – it's an all *or nothing* type of deal. Ask for **all messages** within a specified time frame, and go through them yourself. Who knows – you may find other victims or relevant evidence.

Do I Need That? This is a question we should be asking when crafting our Items to be Seized list. Sure, you can put “Religion” in a Facebook warrant and they will produce a record of what your suspect listed as their religion on Facebook. If this is a domestic terrorism case and you believe it may say something relevant, we'd probably ask for that. If this is a drug sales case – there's probably not a nexus. Always look at the Items to be Seized list and make sure you're not unintentionally crafting an overbroad warrant.

Support EVERYTHING you ask for in your Affidavit of Probable Cause: If your “Items to be Seized” list is 5 pages long – we need to justify PC for each item on the list. You can certainly group them together (IE: “Subscriber information such as names, date of births, emails, phone numbers...etc...will assist me in...”) but make sure you cover them. Think of it like a warrant for a house – we'd never write “I want to search the house and seize any contraband.” Within the Item's to be Seized list, we'd say we want to seize *narcotics* and in our PC Statement explain *why* we believe narcotics will be found. It's pertinent that we follow the same guidelines, even when dealing with digital evidence.

Write for YOUR AUDIENCE: Anticipate prosecutors and judges who know little to nothing about “that platform” to try and understand what you're saying. Avoid being overly technical, be thorough in your explanations, provide background information, and make sure that *anybody* reading your warrants can understand what you're after.

When in Doubt, Ask for Help: You can always reach out to your instructors, or other law enforcement investigators (local very tech savvy investigators, or even on websites like KLoveing and NDCAC) if you need help, support, or don't understand something. Also, **don't be afraid to ask the provider.** IE: *If you're looking at a suspect's account on a victim's phone but can't find a unique identifier to give the provider in your warrant – perhaps an email to their law enforcement team will get you on the right track. We get it – nobody likes to ask for help – but sometimes, there's somebody out there with far more training and experience who can guide you on the right path.*

With that, good luck! We hope that your social media legal process is *effective* and you find the evidence you need to *make your case(s)*.



Summary for Investigators:

Facebook is owned and operated by **Meta Platforms Inc.** Facebook is one of the largest and longest-running social media platforms, allowing users to create personal profiles, share written posts, photos, and videos, connect with friends or followers, and interact through private messaging (via Messenger).

Facebook offers a wide range of features including public posts, private groups, event creation, live streaming, marketplace listings, location tagging, and story sharing. Users can communicate one-on-one or within group chats, join interest-based communities, and share media content that may remain permanently posted or be set to expire after a period of time (via Stories).

How to Serve with Legal Process:

Meta accepts legal process electronically through their law enforcement portal:

<https://www.facebook.com/records>

Meta also accepts preservation requests and emergency disclosure requests through the above listed portal. It's also worth noting that this is where you log in to download your warrant productions once Meta notifies you they are available.

Location to be Searched:

META PLATFORMS, INC.
1 Meta Way
Menlo Park, CA 94025

Identify Accounts By:

Per Facebook's Law Enforcement Guidelines webpage (<https://about.meta.com/actions/safety/audiences/law/guidelines>), they require that we provide one of the following account identifiers:

- User ID Number (<http://www.facebook.com/profile.php?id=1000000XXXXXXX>)
- Username (<http://www.facebook.com/username>)
- Target Email Address(es)
- Target Phone Number(s)

Items to be Seized:

FACEBOOK DATA:

To the extent that the information described is within the possession, custody, or control of Meta Platforms, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Meta Platforms, Inc., or have been preserved pursuant to a request, Meta Platforms Inc. is required to disclose the following information for the *Target Account(s)*. **All of the following records, ranging from the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. **Account Username(s)** and history of any and all account username changes.
 - b. **Vanity Name(s)** and history of changes made to the user's vanity name(s).
 - c. **Birthdate(s)** provided to Facebook for the history of the account.
 - d. **Mobile Phone Number(s)** and history of changes made to phone numbers on the account.
 - e. **Email Address(es)** and history of changes made to the account email address.
 - f. **Profile Photographs** of the target account(s).
 - g. **Self-Reported Profile Information**, including but not limited to:
 - i. Profile biography text, "About Me" sections, introductions, or other self-reported summary fields;
 - ii. Education history including schools attended, degrees, fields of study, and years;
 - iii. Employment history including employers, job titles, dates of employment, locations, and descriptions;
 - iv. Hometown, current city, prior locations, or residences disclosed on profile or timeline;
 - v. Relationship status, spouse or partner links, family members, or familial relationships linked to other Meta accounts;
 - vi. Life events including weddings, moves, births, anniversaries, employment milestones, or other major events disclosed on timeline or profile;
 - vii. Religious views, political views, gender identity, sexual orientation, languages spoken, and other self-reported demographic information;

- viii. Interests, hobbies, favorite activities, and entertainment preferences reported or inferred by Facebook;
 - ix. Personal websites, linked social media accounts, or external links provided in profile;
 - x. Any aliases, alternate names, nicknames, or alternate spellings submitted by the user;
 - xi. Any privacy settings, visibility settings, audience selections, or historical changes made to any of the above profile data.
 - xii. Profile avatars, Bitmojis, or digital likenesses generated by the Target Account(s).
 - h. **Account Creation Date / Time** and IP address information captured at the time of the accounts' creation.
 - i. **Account Deletion Date / Time** if applicable, with associated IP address information captured at the time the account was deleted.
 - j. **Logs** of any instances of account deactivations / reactivations.
 - k. **Logs** of any and all changes made to the account, including password changes, name changes, email or phone number updates, changes to profile information, or other changes made to the target account(s).
 - l. **Two-Factor Authentication information** including all registered devices or phone numbers, recovery codes, and security keys used for account access.
 - m. **Linked financial accounts**, payment methods, or billing addresses provided for Facebook Pay or advertising services.
 - n. **Any consents, acknowledgments, or acceptance logs** related to Facebook's privacy policy, terms of service, or updated agreements.
2. **Device Information** related to the Target Account(s), including:
- a. **Device Identification Numbers** such as IMEI numbers, IMSI numbers, MAC address numbers, or any unique device identification numbers possessed by Meta Platforms, Inc.
 - b. **Logs** of any and all devices connected to the account and connection logs and device history.
 - c. This shall include **all device information** related to logins on the web version of Facebook by the target account(s), as well as **all** other websites maintained by Meta Platforms, Inc.
 - d. Browser user-agent strings, operating system versioning, and application version numbers associated with device logins, sessions, or connections to Meta Platforms, Inc. services.

3. **IP Address Information** for the Target Account(s), to include **logs of ALL IP addresses** used to access the account, log in to the account, log out of the account, or utilize the account in any way, including passive collection logs, system-generated logs, or automatically collected telemetry data, whether generated through app use, background activity, third-party app connections, or Meta-owned auxiliary services. Such IP addresses should be provided in IPv4 and IPv6 format, if available to Meta Platforms, Inc., and shall include **PORT INFORMATION** if available.
4. **Linked Accounts** to the Target Account(s), to include records of any and all linked accounts associated to the Target Account(s) through **cookies, user settings, or Meta Platforms Account Control Center**, including by way of example (but not limited to) linked Facebook and/or Instagram accounts, or linked accounts with any other service provider, such as Google.
5. **Logs** of Target Account(s) usage and activity, including the following logs:
 - a. **IP Addresses** used to access or utilize the target account(s).
 - b. **Direct Messages** (including but not limited to: the sender, recipient, date, and time, **media files sent and received via chat with identification numbers**, and the text of any conversations in possession of Meta Platforms, Inc. which were **sent** or **received** by the Target Account(s)).
 - c. **Group Messages** in which the Target Account(s) have sent, received, shared, or otherwise participated in, including **all chats**, logs of media (with identification numbers, dates, timestamps, and the text of any group chats or conversations saved by Meta Platforms).
 - d. **Account Access**, to include logins, logouts, and other connections.
 - e. **Account Activity**, as further described below:
 - i. **Likes** made by the Target Account(s) on any Facebook posts, multimedia, stories, or other users' multimedia, with information or copies of the multimedia liked, along with any associated metadata, timestamps, and copies or identifiers of the underlying media involved.
 - ii. **Shares** made by the Target Account(s) on any Facebook posts, reels, stories, or other users' multimedia, with information or copies of the multimedia liked, along with any associated metadata, timestamps, and copies or identifiers of the underlying media involved.
 - iii. **Comments** made by the Target Account(s) on any Facebook posts, reels, stories, or other users' multimedia, with information

or copies of the multimedia liked, along with any associated metadata, timestamps, and copies or identifiers of the underlying media involved.

- iv. **Tags** made by the Target Account(s) on any Facebook posts, reels, stories, or other users' multimedia with information or copies of the multimedia in which the target account is tagged.
- v. **Deletion Logs** of any content shared with the account, to include the dates / times the content was deleted.
- vi. **Deletion Logs** of any conversations or direct messages, to include the dates / times the messages were deleted.
- vii. **Password Changes** made by the account holder, with the dates and times.
- viii. **Deletions** of the account, or attempted deletions of the account, with the dates and times of the deletions.
- ix. **Search History** of searches made by the Target Account(s) within the Facebook application, or profiles browsed / viewed by the Target Account(s).
- f. **Contacts** obtained from the target account's mobile device shared with the Facebook application.
- g. **Logs or records of "Friends,"** including of all usernames **who are "friends"** with the Target Account(s), and all usernames who the Target Account(s) **follow**, commonly referred to as Followers and Following, including the date and times that they followed one another, if available.
- h. **Friends Activity** including all details of account(s) which the Target Account(s) have blocked, unfollowed, deleted, follow requested, or accounts which have been follow requested by the Target Account(s), and ignored accounts;
- i. **Additional Account Features and Platform Usage Data**, further described as any and all records related to usage of Facebook features, tools, and platform services by the Target Account(s), including but not limited to:
 - i. **Check-ins or location-based postings** submitted by the Target Account(s), including venue, location metadata, date, time, captions, media attachments, or tagged individuals;
 - ii. **Saved content and Collections**, including any saved posts, photos, videos, links, events, groups, or multimedia items;
 - iii. **Video Watch history** and Facebook Watch viewing logs;
 - iv. **Pokes**, nudges, or other social gestures initiated or received;

- v. **Pages created, owned, administered, or managed** by the Target Account(s), including business pages, fan pages, organizations, or associated accounts;
 - vi. **Commerce Manager, Business Suite, Ads Manager, or Shops data**, including product listings, inventory, financial transactions, sales, order history, product details, and advertisements created or managed by the Target Account(s);
 - vii. **Algorithmic social graph data**, including Facebook-inferred social connections, frequent interaction partners, recommended friends, friends-of-friends mapping, and other associative relationship models generated by Meta Platforms, Inc.
6. **ALL Content**, including photographs, videos, audio files, text, encrypted or partially encrypted content (including any end-to-end encrypted conversations or media where keys remain available to Meta Platforms, Inc.), maintained by Meta Platforms, Inc., related to the Target Account(s), including:
- a. **Posts**, to include photographs, videos, graphics, text-based posts, or other multimedia shared or posted to the account, publicly or privately.
 - b. **Tags**, specifically any and all items of multimedia or posts in which the Target Account(s) are tagged in.
 - c. **Story Content**, to include any saved or preserved story posts containing multimedia or other content in possession of Meta Platforms, Inc.
 - d. **Message Content**, specifically any photographic, video or voice multimedia attached to direct messages.
 - e. **Archived or recovered content** including content previously deleted but available to Meta through retention policies, account recovery logs, or backups.

This request includes any content previously deleted by the account holder but still recoverable by Meta Platforms, Inc., whether fully or partially, through retention policies, preservation requests, account recovery logs, disaster recovery systems, backups, caching, or system-generated storage.

NOTE: Such content, as described above in A-F within subsection 6, **shall include** all associated metadata, including timestamps, timestamps, location data, device information, and any other such data available to Meta Platforms, Inc., whether stored in associated metadata fields, logs, database entries, media titles, embedded EXIF data, or system-level properties maintained by Meta Platforms, Inc.

7. **Location Data** collected, retained or possessed by Meta Platforms, Inc. for the Target Account(s) **or any linked accounts**, to include, but not limited to, GPS coordinates, cellular location data commonly referred to as CSLI, or other specialized location data. This shall further include location history logs derived from GPS, IP addresses, device signals, Wi-Fi, Bluetooth beacons, or other location-based services Meta collects across its apps and services. This includes “location history” and “last known location” records.
8. **Marketplace and Commerce Activity**, further described as all information related to any activity conducted by the Target Account(s) on Facebook Marketplace, including but not limited to:
 - a. Listings created, updated, edited, or deleted by the Target Account(s);
 - b. Purchase and sale history, including transaction details, item descriptions, prices, payment methods, buyer/seller information, and delivery/shipping information;
 - c. Communications related to Marketplace activity (such as inquiries, messages, or negotiations conducted via Marketplace or Messenger related to Marketplace listings);
 - d. Reviews or ratings left or received by the Target Account(s) related to Marketplace activity;
 - e. Financial and payment processing information associated with Marketplace transactions, to include Facebook Pay (if applicable).
9. **Facebook Pay or Any Financial Records / Information**, further described as all financial and payment information retained or possessed by Meta Platforms, Inc. related to Facebook Pay or other financial transactions conducted by the Target Account(s), to include:
 - a. Payment methods, linked financial accounts, and credit card information;
 - b. Transaction history, purchase dates, amounts, recipients, and associated communications;
 - c. Billing addresses and payment-related IP logs;
 - d. Refund requests, disputes, or chargeback information.
10. **Group Activity**, further described as all information related to participation by the Target Account(s) in Facebook Groups, including but not limited to:
 - a. Group memberships (current and historical);
 - b. Content posted by the Target Account(s) to any group (including text, images, video, audio, files, or other media);

- c. Comments, likes, shares, or other interactions within groups;
- d. Group admin or moderator status;
- e. Group invitations sent or received by the Target Account(s).

11. **Facebook Events**, further described as all information related to Facebook Events involving the Target Account(s), including:

- a. Events created, joined, declined, marked as “interested” or “going”;
- b. Invitations sent or received;
- c. Event details, locations, times, descriptions, attendees lists, and associated content (photos, videos, chats, or posts);
- d. Private event communications related to events.

12. **Facebook Dating Activity**: All records of the Target Account’s use of Facebook Dating, including dating profiles, preferences, matches, likes/dislikes, messages exchanged, blocked users, and interaction logs related to Dating features.

13. **Third Party App Integrations and Authorized Apps**, further described as all records of any third-party applications, websites, or services connected to or authorized through the Target Account(s), including:

- a. List of third-party apps connected to the account;
- b. Dates and times of authorizations or revocations;
- c. Permissions granted to third-party apps (including data sharing levels);
- d. Any data shared with or obtained from third-party applications.

14. **Advertising and Behavioral Data**, further described as all records of advertising-related data collected or retained by Meta Platforms, Inc., related to the Target Account(s), including but not limited to:

- a. Advertisements viewed, clicked, or interacted with by the Target Account(s);
- b. Advertising profiles, including demographic profiles, interests, or inferred data used for ad targeting;
- c. Audience network participation;
- d. Advertisements created by the Target Account(s), including payment and billing information for ads.

15. **Security-Related Data**, further described as all security logs and account protection data, including:

- a. Two-factor authentication records, devices registered for multi-factor authentication;

- b. Recovery email addresses, phone numbers, or contacts used for account recovery;
- c. Suspicious login notifications, security alerts, or compromised account flags;
- d. Password reset requests, recovery codes issued, and security settings history.

16. Biometric Information (if available): If Meta retains biometric data related to the Target Account(s), such as facial recognition data derived from uploaded photographs or videos, provide:

- a. Templates or data points derived from biometric analysis;
- b. Dates of enrollment or deactivation of facial recognition services.

17. Data Subject Activity & Consent History, further described as all consents, user agreements, privacy policy acceptances, terms of service acceptances, and opt-in/opt-out logs associated with the Target Account(s), including timestamps.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Facebook is a widely used global social media platform owned by Meta Platforms, Inc. Meta also owns Instagram, Messenger, WhatsApp, and other related services. Facebook offers a wide variety of features allowing its users to communicate, share content, organize groups, conduct financial transactions, and store extensive personal information. The data maintained by Facebook is hosted on servers owned and controlled by Meta Platforms, Inc., independent of the user's physical device, and is accessible by Meta through lawful process such as court orders and search warrants.

Facebook allows users to create personal profiles which may include their legal names or pseudonyms, profile photographs, and extensive self-reported information such as biographical summaries, employment history, educational background, places lived, relationship status, family members, religious and political views, languages spoken, sexual orientation, and personal interests. This information can assist law enforcement in identifying and confirming the individual(s) who control a given Facebook account and may establish links to known suspects, co-conspirators, criminal organizations, or victims.

Facebook users can share posts containing text, photographs, videos, hyperlinks, and multimedia content to their timelines. These posts may be public, limited to friends, restricted to private groups, or accessible only to specific individuals, depending on

user-controlled privacy settings. The posts may include geotagged location data, timestamps, captions, and tagged individuals, which can directly evidence criminal activity, establish timelines, corroborate events under investigation, or identify additional individuals involved.

In addition to posting public content, Facebook offers a robust private messaging system known as Messenger, allowing users to engage in one-on-one or group chats. Messenger allows for the transmission of text messages, photographs, videos, voice recordings, file attachments, and video calls. Through my training and experience, I know that Messenger is frequently used by individuals engaged in criminal activity to plan, coordinate, or discuss illegal conduct with co-conspirators, customers, or victims. The private nature of these communications often gives suspects a false sense of security, believing the content is inaccessible to law enforcement. However, Facebook retains extensive records of these communications, including metadata such as sender, recipient, timestamps, message content, attached media, and deletion logs.

Beyond direct communication, Facebook provides many interactive features that create digital footprints relevant to criminal investigations, including:

- Likes, comments, shares, and tags, which demonstrate engagement with specific content or individuals, reveal networks of association, and may reflect interests or participation in criminal activity.
- Groups and Events, which allow users to organize private communities, coordinate meetings, promote illegal enterprises, or recruit individuals into criminal organizations.
- Saved Content and Collections, which may include bookmarks of incriminating content, contacts, or evidence of interest in criminal activity.
- Check-ins and location-based posts, which may place individuals at or near locations relevant to an investigation at critical times.

Facebook also offers an integrated Marketplace platform where users can buy and sell goods, including contraband or stolen property. Criminal actors may utilize Facebook Marketplace to facilitate illegal commerce, trafficking, or financial fraud. Records of listings, sales, transaction details, payment methods, communication logs, and shipping records may reveal unlawful activity.

Furthermore, Facebook maintains financial transaction records through Facebook Pay and integrated advertising services. Payment information, linked financial accounts, credit cards, billing addresses, purchases, refunds, and chargeback disputes may reflect financial motives, proceeds of crime, or fraudulent transactions related to criminal enterprise.

Through my training and experience, I know that criminal subjects often operate multiple Facebook and Instagram accounts simultaneously, sometimes under alternate names, nicknames, or pseudonyms to compartmentalize their criminal activity.

Facebook maintains records of linked accounts, third-party applications authorized by the user, and shared device identifiers, which may expose otherwise unknown accounts used by the subject or co-conspirators.

In addition to content and communications, Facebook collects extensive device and location data associated with user activity, including:

- IP address logs reflecting where and when accounts are accessed.
- Device identifiers (IMEI, IMSI, MAC address, browser user-agent strings) which may link specific devices to the account.
- GPS coordinates, Wi-Fi location data, Bluetooth beacon proximity data, and cell tower-based location data, which may place suspects at relevant locations during key periods of criminal activity.

Even if suspects attempt to delete content, I know that Facebook retains archived, deleted, or system-cached records for extended periods under their internal retention policies, which may remain accessible upon service of a lawful warrant. Deletion logs may also evidence consciousness of guilt, attempts to obstruct investigation, or recent efforts to conceal criminal activity.

Finally, Facebook maintains records of security activity including password resets, suspicious login alerts, recovery contacts, two-factor authentication devices, and system-generated activity flags, which may provide additional evidence regarding account control, unauthorized access, or attempted account compromises relevant to the investigation.

In my training, experience, and consultation with other investigators, I am aware that individuals engaged in criminal conduct regularly use Facebook for purposes directly related to their criminal activity. Criminal actors utilize Facebook's broad features in diverse ways to facilitate and conceal criminal conduct. These activities include, but are not limited to:

- **Communication and Coordination:** Criminal actors use Facebook Messenger and group chats to privately exchange messages, photographs, videos, documents, and voice recordings related to criminal planning, illegal transactions, recruitment, or coordination with co-conspirators. These communications often occur in private groups, encrypted chats, or through the use of multiple linked accounts.
- **Promotion and Advertisement of Criminal Conduct:** Individuals involved in narcotics trafficking, illegal firearm sales, stolen property distribution, fraud schemes, and human trafficking frequently advertise illegal goods or services through public posts, Facebook Marketplace, private groups, or covertly coded messages in posts and stories.

- **Recruitment and Exploitation:** Offenders engaged in gang activity, violent organizations, sex trafficking, and online exploitation often recruit vulnerable individuals through Facebook connections, direct messages, targeted friend requests, or introductions through mutual friends. Facebook's suggested friend algorithms and group recommendations may facilitate rapid network expansion for these criminal enterprises.
- **Financial Transactions and Monetization:** Criminal actors utilize Facebook Pay, Marketplace payment tools, advertising services, and off-platform financial integrations to monetize illegal activity, launder proceeds, or conceal the source of funds. Payment histories, refunds, chargebacks, linked bank accounts, and billing information may directly evidence financial motives and profit derived from criminal acts.
- **Post-Offense Discussions and Boasting:** Based on my training and experience, offenders frequently utilize social media platforms like Facebook to discuss, reference, or boast about their involvement in criminal activity after the offense has occurred. Suspects may post coded messages, photographs, celebratory posts, or indirect references to acts of violence, financial gain, successful crimes, or challenges to rival individuals or groups. Such post-offense discussions may provide critical admissions, identify previously unknown associates, document possession of contraband, or reveal ongoing criminal activity not yet detected by law enforcement.
- **Concealment and Evasion:** Facebook allows for the rapid deletion of posts, messages, or entire accounts, offering offenders the ability to attempt to obscure evidence. However, Meta Platforms retains logs of deletion activity, timestamps of removed content, and archives of previously deleted material under their retention policies. Criminal actors may operate multiple accounts under different names, pseudonyms, or fake identities, often maintaining separate accounts for public versus private criminal activity. They may also employ VPNs, anonymizing tools, or third-party integrations to attempt to obfuscate their true identity and location while using the platform.
- **Location-Based Offending and Surveillance:** Through check-ins, geotagged posts, location history, and device telemetry data, Facebook may capture extensive records of where a suspect was located at specific times. Such records may place a subject at or near the scene of a crime, establish alibis, or contradict false statements during an investigation.
- **Association Mapping:** Criminal networks frequently use Facebook's friend lists, groups, event participation, tagged photos, and comment threads to build and maintain extensive social networks. These associations may reveal otherwise unknown co-conspirators, victims, criminal enterprises, or organizational hierarchies critical to understanding broader conspiracies or ongoing criminal organizations.

In my experience, Facebook's vast data holdings serve as a comprehensive repository of a suspect's communications, online activities, associations, movements, and financial transactions. Because Facebook stores this data on its own centralized servers (rather than solely on the suspect's physical devices), valuable evidence remains preserved even if a suspect's phone, computer, or tablet is seized, destroyed, factory-reset, or placed into airplane mode at the time of law enforcement contact. In many instances, obtaining these records directly from Meta Platforms, Inc., through lawful process, is the only method available to recover complete, accurate, and historical evidence of a suspect's criminal conduct, contacts, and coordination with others.

For all of the above reasons, I believe that the requested records maintained by Meta Platforms, Inc. concerning the identified Facebook account(s) will contain evidence, fruits, and instrumentalities of violations under investigation.

Additional Considerations for Facebook:

When crafting our “Items to be Seized” list, we should be **very specific** about what we want when dealing with Meta Platforms, as Meta will not produce records specifically mentioned in this list:

- Avoid “any and all records, data” type general requests, as they will not produce *a lot* of valuable content.
- The above example is “all encompassing” and includes almost every Facebook feature we could find. *It is highly unlikely* that you will need all of these – so be sure to “narrowly tailor” your warrant appropriately and remove items on that list if you can’t establish the relevance (or potential relevance) to your case.

As of 2025, *most* Facebook messenger content is *encrypted* and cannot be produced in response to search warrants. We will need the suspect's phone to obtain these.

As of 2025, Facebook is **only producing warrant returns as HTML files** and is no longer producing PDF versions. This is useful because they are easier to review and we can watch videos and listen to audio files that we previously couldn't with PDFs.

Many investigators (myself included) have experienced challenges in opening these HTML files, particularly for large time periods or active accounts, as the large file sizes can crash our internet browsers and computers. **My Suggestions:** Turn off Javascript on your web browser (work with your agency's IT for help if needed), use Mozilla Firefox to open them (as it handles the large “webpages” better than Chrome or Edge), using a computer with excellent specs (high RAM, etc.) can help and finally if you access to tools that parse these returns such as Magnet Axion or Nighthawk, these can resolve that issue for investigators.

Even better? Use NDCAC's FREE tool for law enforcement called .Social. It's linked within the student portal or accessible by visiting the NDCAC law enforcement portal (you will have to register an account). My personal opinion is that it is probably one of the best available tools right now for us to parse and review Meta accounts. (If you've used it in the past – they rolled out a brand new version of it in 2025 that was rebuilt from the “ground up” and is a significant improvement on the former .Social).

When accounts are **deleted** by users (in their entirety, not just specific things on the account deleted), Facebook will place them in a state called “deactivated” for 30 days, giving users time to consider if they *really want to* delete their account. As such, if a suspect deletes their account, we *may* have up to 30 days to get a preservation letter into Meta Platforms and still obtain the data. Act quickly!

INSTAGRAM



Summary for Investigators:

Instagram is also owned and operated by **Meta Platforms Inc.** Instagram is a social media platform primarily focused on sharing photos, videos, and short-form content. Users create personal or business profiles where they can post images, videos, and captions to their "Feed," which is visible to their followers. The platform also offers "Stories," temporary posts that disappear after 24 hours. Instagram supports both private and public accounts, giving users control over who can view their content.

In addition to posting content, Instagram offers features like direct messaging (DMs) for private conversations, live video streaming, and "Reels," which are short, often music-backed video clips designed for entertainment and discovery. Users can engage with each other's content by liking, commenting, sharing, or saving posts. Instagram also includes a search and discovery function, where users can explore trending content, hashtags, and suggested profiles based on their interests.

How to Serve with Legal Process:

Meta accepts legal process electronically through their law enforcement portal:
<https://www.facebook.com/records>

Meta also accepts preservation requests and emergency disclosure requests through the above listed portal. It's also worth noting that this is where you log in to download your warrant productions once Meta notifies you they are available.

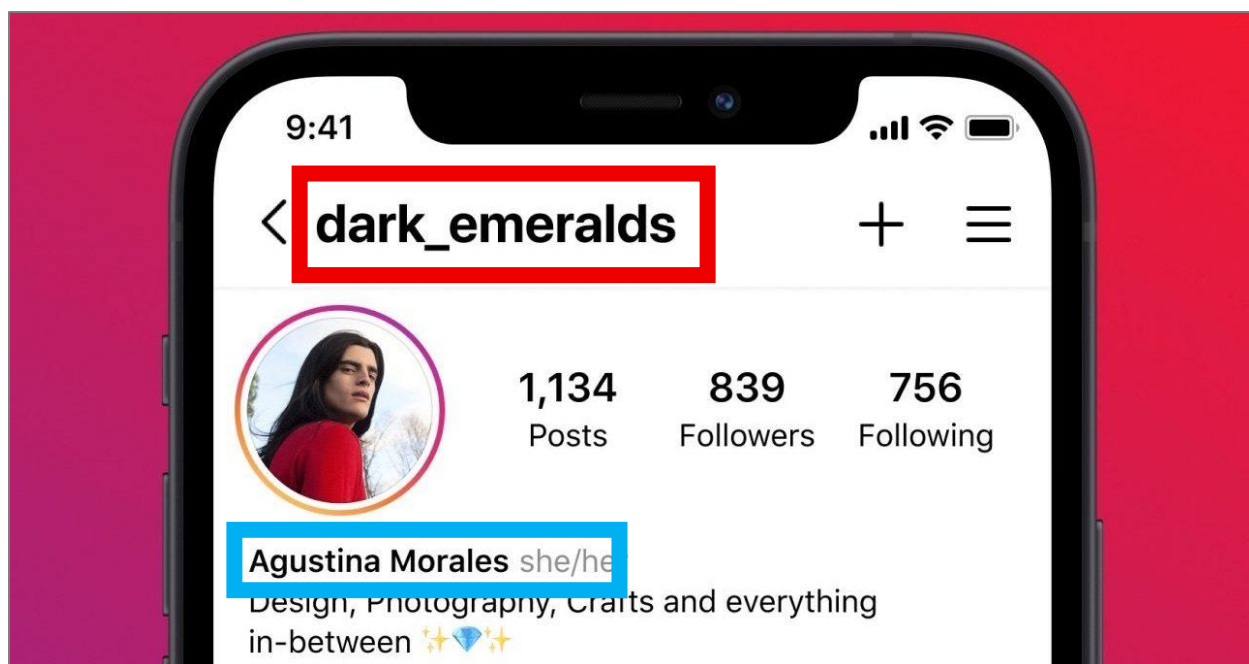
Location to be Searched:

META PLATFORMS, INC.
1 Meta Way
Menlo Park, CA 94025

Identify Accounts By:

Per Facebook's Law Enforcement Guidelines webpage (<https://about.meta.com/actions/safety/audiences/law/guidelines>), they require that we provide one of the following account identifiers:

- User ID Number (*You'll only have this if you use a tool or have a warrant return*)
- Username (**See below. DO NOT accidentally use their vanity name!**)
- Target Email Address(es)
- Target Phone Number(s)



*Very Important: In the above image, the **username** (which we need for legal process) is highlighted with a **RED BOX**. The blue box below it is a **vanity name**. If you provide Instagram with a vanity name by mistake, they **will NOT** produce records. **Careful!***

Items to be Seized:

INSTAGRAM DATA:

To the extent that the information described is within the possession, custody, or control of Meta Platforms, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Meta Platforms, Inc., or have been preserved pursuant to a request, Meta Platforms Inc. is required to disclose the following information for the Target Account(s). **All of the following records, ranging from the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Account Username(s), all username change history, and any previously used or retired usernames, aliases, alternate spellings, nicknames, or vanity handles associated with this account or linked Meta Accounts, even if no longer actively displayed;
 - b. Vanity name(s), account display names, and associated change history;
 - c. Birthdate(s) and any age information provided or updated;

- d. Mobile phone number(s) associated with the account, including all changes over time;
- e. Email address(es) associated with the account, including all changes over time;
- f. Profile photographs, avatars, and any digital likenesses or Bitmojis generated by the user;
- g. Self-reported profile information, including:
 - i. Profile biography ("About Me") text;
 - ii. Personal websites, linked social media, or external links;
 - iii. Pronouns, Gender, sexual orientation, political views, religious views, and language preferences (if provided);
 - iv. Locations listed (hometown, current city, prior residences);
 - v. Relationship status, linked family members or tagged partners;
- h. Account creation date/time with IP address captured at account registration;
- i. Account deletion date/time (if applicable), with IP addresses recorded at deletion;
- j. Deactivation/reactivation history;
- k. All changes made to account security settings (password changes, two-factor authentication enrollment, recovery codes, security keys, recovery contacts, privacy setting adjustments);
- l. Linked financial accounts, payment methods, or billing addresses associated with advertising, subscriptions, or commerce features;
- m. Any consent acknowledgments related to Meta's Terms of Service, Privacy Policy, or other user agreements.

2. **Device Information** related to the Target Account(s), including:

- a. Device identification numbers (IMEI, IMSI, MAC address, device IDs);
- b. Logs of all devices connected to the account, including device connection history;
- c. Device and app session information related to logins across web, mobile app, and third-party integrations;
- d. Browser user-agent strings, operating system versions, and app version numbers associated with device access.

3. **IP Address Information** for the Target Account(s), to include but not limited to:

- a. Logs of all IP addresses used to access, log into, log out of, or utilize the Target Account(s), including passive collection logs, background session telemetry, or system-generated logs from third-party integrations;

- b. IP addresses provided in both IPv4 and IPv6 format, including **port information**, if available to Meta Platforms, Inc.

4. **Linked Accounts** to the Target Account(s), to include:

- a. Facebook accounts via Meta Account Center;
- b. Additional Instagram accounts (managed or alternate accounts);
- c. Accounts linked via cookies, device fingerprints, app authorizations, or Meta-integrated identity management services (Google, Apple, etc.).

5. **Usage Logs and Account Activity** of Target Account(s), including the following:

- a. IP addresses used for account access or activity;
- b. Direct Message records (sender, recipient, date/time, message content, attached media, identification numbers, and media files), including any profile contact cards, phone numbers, usernames, links to third-party platforms, or external contact information shared via Direct Messages or group chats, whether as text or embedded contact attachments;
- c. Group Message records (group participants, content, timestamps, media files, and group chat histories);
- d. Close Friends lists and group membership logs, including membership changes over time;
- e. Account access logs (login, logout, device connection timestamps);
- f. Complete account activity logs, including:
 - i. Likes, shares, and comments on posts, stories, reels, and other media, with copies of liked or commented media, timestamps, and metadata;
 - ii. Tags applied by or involving the Target Account(s);
 - iii. Story viewer logs showing which users viewed the Target Account's stories, including timestamps of viewing activity;
 - iv. Deletion logs for content and messages, including timestamps of deletion;
 - v. Password changes, account recovery attempts, or security events;
 - vi. Search history and profile browsing history;
 - vii. Saved content (collections, bookmarks, or saved reels/posts);
 - viii. Broadcast Channel participation, creation, or messaging content;
 - ix. Story viewer logs showing who viewed posted Stories, including dates/times;
 - x. Emoji reactions or other story reaction features submitted or received;
 - xi. Polls, quizzes, questions stickers submitted or answered;

- xii. Pinned content;
 - xiii. Saved drafts (draft posts, drafts of reels or stories not yet posted);
 - xiv. Deleted or abandoned drafts that were saved as drafts but deleted prior to posting, including the media content, captions, tags, location data, and timestamps associated with each discarded draft;
 - g. Interaction metrics related to posts, stories, reels, and videos, including view counts, impressions, reach, audience retention, average watch time, forward/backward skips, shares, saves, replies, and engagement ratios;
 - h. Administrative logs related to pending account deletions, deactivations, username changes, appeals, moderation strikes, or enforcement actions pending Meta internal review;
 - i. Internal machine learning content classification tags applied to account content by Meta Platforms, Inc., including automated flags for violence, illegal goods sales, child endangerment, nudity, sexual exploitation, hate speech, or other platform violations;
 - j. Contact lists uploaded or synced from the user's mobile device;
 - k. In-app purchases, subscription history, account balances, credits, and financial transactions conducted via Instagram platform;
 - l. Full records of Friends, Followers, Following lists, requests, blocked accounts, muted accounts, unfollowed accounts, and pending requests with associated dates/times.
6. **ALL Content**, including photographs, videos, audio files, text, and encrypted files, maintained by Meta Platforms, Inc., related to the Target Account(s), including:
- a. **Posts** (public and private), including text captions, hashtags, photographs, videos, graphics, and audio content. This shall include collaborative posts, shared ownership posts, or co-authored reels, with full participant lists, timestamps, and revision history;
 - b. **Reels** content (public, private, and drafts);
 - c. **Story** content:
 - i. Active Stories;
 - ii. Story Archive (all preserved Stories even if no longer public);
 - iii. Story Highlights (collections curated by user), including historical versions or modifications of Highlight collections over time, even if source Stories were later deleted, altered, or expired, including timestamps of creation, edits, renames, additions, removals, and reordering of Story Highlights;

- iv. Close Friends stories;
- d. **Live Video** content:
 - i. Live video sessions;
 - ii. Archived Live Videos;
 - iii. Deleted Live sessions preserved under Meta retention policies;
 - iv. Audio Room sessions (if applicable), including participants, session metadata, recordings, timestamps, and message/chat content generated during live audio discussions.
- e. **Direct Messaging Content**, including text, emojis, icons, GIFs, links, location pins, or attachments in the form of multimedia (photographs, videos, or audio recordings);
- f. **Audio recordings, voice notes, and voice message attachments** sent or received in Direct Messages or group chats, including all associated metadata;
- g. **Recently Deleted content** (within Meta's "Recently Deleted" recovery feature);
- h. **Tags** applied to or by the Target Account(s);
- i. **Overlays** to any multimedia described above, including drawings, designs, emojis, text, images gifs, or other alterations made by the target account(s) to multimedia;
- j. **Notes** (short status updates posted by the Target Account(s)), including text, timestamps, emoji, and associated metadata;
- k. **Broadcast Channels** created, followed, subscribed to, or administered by the Target Account(s), including message content, media attachments, timestamps, participants, interaction metrics, and associated metadata;
- l. Moderation and filtering settings applied to comments, messages, or followers, including hidden words, blocked phrases, muted words, filtered content, and ignored interactions;
- m. Linked external services, applications, or platforms disclosed in profile bios, stories, captions, or via app integration (e.g., Snapchat usernames, Telegram channels, encrypted chat links, other social media cross-promotion);
- n. **Media Metadata** for all content described above, including:
 - i. EXIF data (if retained);
 - ii. Upload timestamps;
 - iii. Device identifiers linked to upload;
 - iv. Geolocation data embedded in uploaded media.

7. **Location Data** collected, retained or possessed by Meta Platforms, Inc. for the Target Account(s):
 - a. GPS coordinates, device-based location logs, cellular location (CSLI), Wi-Fi signals, Bluetooth beacons, IP-based geolocation, or any other location data collected or retained by Meta Platforms, Inc.;
 - b. Location history logs generated by Instagram usage or Meta cross-platform services;
 - c. Check-ins or tagged locations attached to posts, stories, or reels.
8. **Instagram Shopping and Commerce Activity**, including:
 - a. Product listings, shops managed, commerce transactions, order history, delivery information, linked financial accounts, or payment data associated with purchases or sales conducted by the Target Account(s).
9. **Instagram Subscriptions, Monetization, Creator Payments, and Revenue Data**, including:
 - a. Subscription feature usage, including subscriber lists, subscriber-only content (posts, reels, stories), pricing tiers, subscriber engagement logs, and subscription payment history;
 - b. Creator monetization tools, including revenue earned from badges, virtual gifts, affiliate marketing commissions, sponsorships, branded content partnerships, and promotional collaborations;
 - c. Records of brand partnership disclosures, brand tagging history, and enforcement of Instagram's branded content guidelines;
 - d. Payout logs, payment account linkage, transaction history, disbursement amounts, linked banking or financial institutions associated with payouts, and any suspended or frozen earnings;
 - e. Historical earnings summaries, monetization eligibility audits, and participation in Meta's Creator Marketplace or other pilot monetization programs.
10. **Advertising and Behavioral Data**, including:
 - a. Advertisements viewed, clicked, engaged with, or dismissed by the Target Account(s);
 - b. Advertising profiles maintained by Meta, including:
 - i. Inferred interests, behaviors, demographics, location targeting;
 - ii. Audience targeting segments the user is assigned to;
 - iii. Ad engagement history;
 - c. Sponsored posts interacted with;

- d. Advertisements created, managed, or paid for by the Target Account(s);
- e. API interaction logs reflecting use of third-party automation tools, scheduling services, follower-boosting bots, engagement services, or other external tools interacting with Instagram via automated means, whether authorized via OAuth or detected through API monitoring, including app names, vendor identifiers, device/browser signatures, and timestamps of API requests.

11. **Behavioral Personalization Data** related to Explore page curation, Reels recommendations, Suggested Users, content categories, hashtags, themes, topics, or interest groupings assigned to the Target Account(s), including algorithmically-inferred interests, associations, and trending interaction profiles.

12. **Third Party Application Integrations**, including:

- a. List of third-party apps authorized through Instagram OAuth;
- b. Authorization timestamps and revocation history;
- c. Permissions granted to authorized apps;
- d. Data shared between Instagram and authorized third parties.

13. **Security and Account Protection Data**, including:

- a. Two-factor authentication enrollment, recovery codes, security keys;
- b. Account recovery emails, phone numbers, or contacts;
- c. Suspicious login notifications, location mismatch warnings, or account compromise alerts;
- d. Password reset history, including recovery attempts.

14. **Biometric Information** (if available), further described as facial recognition data, facial mapping templates, or machine-learning derived biometric data generated through the user's uploaded photographs or videos.

15. **Consent and Legal Agreement History**, further described as all consents, user agreements, privacy policy acceptances, terms of service agreements, opt-in/opt-out logs, and related timestamped records.

NOTE: This request includes any content, communications, or data that may have been deleted, archived, or modified by the user but remains accessible to Meta Platforms, Inc. through internal data retention systems, preservation holds, recovery policies, server-side backups, disaster recovery snapshots, or cached storage, whether as full content, partial logs, metadata, or system-maintained records.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Instagram is a widely used global social media platform owned by Meta Platforms, Inc. Meta also owns Facebook, Messenger, WhatsApp, and other related services. Instagram offers a wide variety of features allowing its users to share multimedia content, communicate privately, organize groups, conduct financial transactions, and maintain extensive personal and behavioral data profiles. The data maintained by Instagram is hosted on servers owned and controlled by Meta Platforms, Inc., independent of the user's physical device, and is accessible by Meta through lawful process such as court orders and search warrants.

Instagram allows users to create personal profiles which may include their legal names or pseudonyms, profile photographs, biography text, and extensive self-reported profile information such as pronouns, relationship status, locations, interests, external websites, and social media cross-links. This profile information may assist law enforcement in identifying and confirming the individual(s) who control a given Instagram account and may establish connections to suspects, co-conspirators, criminal enterprises, or victims.

Instagram users may post a variety of multimedia content, including photographs, videos, short-form videos known as "Reels," Stories (which expire after 24 hours unless archived), and live video broadcasts. These posts may include geotagged location data, timestamps, hashtags, tagged individuals, captions, and interaction data such as likes, comments, and shares. Posts may be public, restricted to approved followers, or viewable only to "Close Friends" depending on privacy settings. This content may provide direct evidence of criminal conduct, establish timelines, corroborate events, or identify involved individuals.

In addition to public posting, Instagram offers private communication features, including Direct Messaging (DMs), group chats, and private story groups. Through my training and experience, I know that Direct Messaging is frequently used by individuals engaged in criminal activity to conduct conversations related to illegal transactions, planning, coordination with co-conspirators, recruitment, or post-offense boasting. These communications may include text, photographs, videos, emojis, voice recordings, contact cards, and external links. Instagram retains extensive records of these communications, including sender, recipient, message content, timestamps, attached media, deletion logs, and metadata.

Beyond messaging, Instagram provides numerous interactive features that generate extensive digital records relevant to criminal investigations, including:

- Likes, shares, comments, reactions, polls, questions, quizzes, and stickers, which may reflect user interests, intent, associations, or participation in criminal activity.
- Tagging of other users, locations, or media that can demonstrate relationships and place individuals at relevant locations or times.
- Saved Content and Collections, which may include bookmarks of incriminating material, communication threads, or evidence of involvement in criminal conduct.
- Story Viewer Logs, which reveal who has viewed posted Stories, including timestamps of viewing activity, even for content that may have since expired.

Instagram also includes features that enable financial activity. Instagram Shopping allows users to promote and sell goods, while subscription and monetization features permit creators to earn revenue from exclusive content, affiliate programs, sponsorships, and direct payments from followers. Criminal actors may utilize these commerce features to facilitate financial fraud, laundering of proceeds, trafficking, or monetizing illegal enterprises. Instagram maintains records of purchases, sales, payouts, payment accounts, subscriber lists, linked financial institutions, and transaction histories.

Through my training and experience, I know that criminal subjects often operate multiple Instagram and Facebook accounts simultaneously, sometimes under different names or aliases, to compartmentalize their activity. Meta Platforms retains detailed information regarding linked accounts, shared devices, third-party app authorizations, OAuth integrations, API interactions, and shared device fingerprints that may expose otherwise undisclosed accounts connected to the subject.

In addition to content and communications, Instagram collects extensive device, network, and location data associated with user activity, including:

- IP address logs showing where and when accounts are accessed;
- Device identifiers (IMEI, IMSI, MAC address, user-agent strings, device IDs) which may directly link physical devices to accounts;
- GPS coordinates, Wi-Fi-based location, Bluetooth beacon proximity, cellular tower location (CSLI), and other telemetry signals, which may place a suspect at specific locations or times critical to the investigation.

Even if suspects attempt to delete content, Instagram maintains archived, deleted, or system-cached records for extended periods pursuant to internal retention policies and preservation capabilities. Deletion logs may also reflect efforts to obstruct justice, conceal criminal activity, or demonstrate consciousness of guilt.

Instagram maintains robust security, account protection, and enforcement data, including:

- Password reset history, recovery attempts, and changes to authentication credentials;
- Two-factor authentication enrollment, security key registrations, and device authentication logs;
- Suspicious login notifications, geographic login mismatches, flagged activity, or compromised account warnings;
- Content moderation actions, enforcement flags for policy violations (including content flagged for illegal activity such as child exploitation, firearm trafficking, narcotics sales, human trafficking, or violence).

In my training, experience, and consultation with other investigators, I am aware that individuals engaged in criminal conduct regularly utilize Instagram for purposes directly tied to their criminal activity. These activities include, but are not limited to:

- **Communication and Coordination:** Criminal actors use Instagram Direct Messaging, group chats, and story replies to privately exchange messages, videos, photographs, contacts, and location pins related to criminal planning, sales transactions, recruitment, or post-offense coordination with co-conspirators and victims.
- **Promotion and Advertisement of Criminal Conduct:** Narcotics traffickers, firearms dealers, organized theft rings, and fraud networks regularly advertise contraband, stolen property, illegal services, or financial scams via public posts, stories, reels, and private groups, often utilizing coded language, emojis, hashtags, or visual imagery designed to evade detection.
- **Recruitment and Exploitation:** Offenders involved in gang activity, violent organizations, sexual exploitation, or human trafficking often recruit vulnerable individuals through Instagram's network features, private messaging, story interactions, and follower suggestions generated by Meta's algorithms.
- **Financial Transactions and Monetization:** Criminal actors use Instagram's Shopping, Subscriptions, Commerce Manager, and monetization tools to receive payments, launder illicit proceeds, or conceal financial transactions associated with unlawful activity. Financial logs, transaction histories, payout accounts, refunds, and payment records may reflect direct financial gain from criminal conduct.
- **Post-Offense Boasting and Admissions:** Based on my training and experience, offenders often utilize Instagram to reference, brag about, or indirectly discuss crimes after they occur. These may include photographs with weapons, currency, stolen goods, coded captions referencing violent acts or criminal affiliations, or celebratory posts following criminal activity.
- **Concealment and Obfuscation:** Instagram allows users to rapidly delete posts, stories, messages, or even entire accounts. Suspects may use multiple burner accounts, VPNs, anonymization services, or external encrypted messaging platforms cross-linked via Instagram to obscure their identity or conceal illicit communications. However, Meta Platforms retains deletion logs, audit trails, and

archived versions of deleted or modified content that may still be recovered via lawful process.

- **Location-Based Surveillance:** Through location-tagged posts, geotagged media, story check-ins, and passive device telemetry, Instagram may record precise historical location data placing suspects at specific geographic coordinates relevant to the crime under investigation.
- **Network and Association Mapping:** Instagram’s follower lists, friend requests, tagged posts, shared stories, broadcast channels, group chats, and comment threads often reveal the subject’s criminal network, co-conspirators, and organizational hierarchy, which may otherwise remain hidden without these records.

In my experience, Instagram’s extensive data retention serves as a detailed historical record of a suspect’s communications, associations, financial activity, movements, and criminal enterprise. Because this data is stored directly by Meta Platforms, Inc. on company-controlled servers, it remains accessible even if a suspect’s phone or computer is seized, reset, wiped, or placed into airplane mode at the time of law enforcement contact. In many cases, obtaining these records directly from Meta Platforms, Inc., via lawful search warrant, is the only method available to fully reconstruct historical criminal activity and recover evidence essential to this investigation.

For all the reasons set forth above, I believe the requested records maintained by Meta Platforms, Inc. related to the identified Instagram account(s) will contain evidence, fruits, and instrumentalities of violations under investigation.

Additional Considerations for Instagram:

When crafting our “Items to be Seized” list, we should be **very specific** about what we want when dealing with Meta Platforms, as Meta will not produce records specifically mentioned in this list:

- Avoid “any and all records, data” type general requests, as they will not produce *a lot* of valuable content.
- The above example is “all encompassing” and includes almost every Instagram feature we could find. *It is highly unlikely* that you will need all of these – so be sure to “narrowly tailor” your warrant appropriately and remove items on that list if you can’t establish the relevance (or potential relevance) to your case.
- **Note how we specifically use Instagram’s “names” for things like Reels, Story Archives, and Story Highlights?** It’ll ensure you don’t miss evidence.

As of 2025, *end to end encryption* is *allegedly* “rolling out” to Instagram direct messages. At some point in the future, if not already, it likely will not be able to be produced in response to search warrants and we’ll need the suspect’s phone.

As of 2025, Instagram is **only producing warrant returns as HTML files** and is no longer producing PDF versions. This is useful because they are easier to review and we can watch videos and listen to audio files that we previously couldn't with PDFs.

Many investigators (myself included) have experienced challenges in opening these HTML files, particularly for large time periods or active accounts, as the large file sizes can crash our internet browsers and computers. **My Suggestions:** Turn off Javascript on your web browser (work with your agency's IT for help if needed), use Mozilla Firefox to open them (as it handles the large "webpages" better than Chrome or Edge), using a computer with excellent specs (high RAM, etc.) can help and finally if you access to tools that parse these returns such as Magnet Axiom or Nighthawk, these can resolve that issue for investigators.

Even better? Use NDCAC's FREE tool for law enforcement called .Social. It's linked within the student portal or accessible by visiting the NDCAC law enforcement portal (you will have to register an account). My personal opinion is that it is probably one of the best available tools right now for us to parse and review Meta accounts. (If you've used it in the past – they rolled out a brand new version of it in 2025 that was rebuilt from the "ground up" and is a significant improvement on the former .Social).

When accounts are **deleted** by users (in their entirety, not just specific things on the account deleted), Instagram will place them in a state called "deactivated" for 30 days, giving users time to consider if they *really want to* delete their account. As such, if a suspect deletes their account, we *may* have up to 30 days to get a preservation letter into Meta Platforms and still obtain the data. Act quickly!

August 2025 Update: Instagram is now capturing and retaining significantly more geolocation data for the purpose of their "Story Map" and other relevant features. We have started to see much more geolocation data being produced in response to Instagram warrants (this is still dependent on user's settings). Be sure to include language in your warrants seeking geolocation data!

WHATSAPP



Summary for Investigators:

WhatsApp is a globally popular messaging application owned by Meta Platforms, Inc. It allows users to send encrypted messages, voice recordings, photos, videos, documents, contact cards, and location information to individuals or groups. WhatsApp operates primarily through mobile phone numbers — each account is tied to a phone number at registration, though users can change phone numbers or devices after initial setup. One of WhatsApp's most notable features is its end-to-end encryption, which means message content is not visible to Meta or third parties while in transit; however, WhatsApp still maintains metadata records, including contact lists, account registration information, IP address logs, timestamps, and device identifiers. Group chats allow multiple users to communicate simultaneously, and participants may be added, removed, or leave at any time. WhatsApp also supports voice and video calling, file sharing, and location sharing features.

For law enforcement, WhatsApp is frequently encountered in a wide variety of criminal investigations, particularly involving drug trafficking, organized crime, fraud, child exploitation, and violence. Offenders often believe that WhatsApp's encryption makes their activities undetectable, but important investigative leads can still be developed through subpoenas and search warrants. Subscriber data, group memberships, connection logs, phone numbers, associated devices, IP addresses, and uploaded contact lists can help identify suspects, link co-conspirators, corroborate timelines, and build communication networks. Even when suspects delete content from their own devices, WhatsApp retains some server-side data that may still be accessible to law enforcement under legal process.

How to Serve with Legal Process:

VERY IMPORTANT / COMMON MISTAKE: Although WhatsApp is owned by Meta Platforms (like Facebook and Instagram), it operates as it's own LLC entity (WhatsApp, LLC.) and legal process **must be addressed differently (see below) and submitted differently** than we would for Facebook or Instagram records. *Or they will NOT comply!*

WhatsApp, LLC. accepts legal process electronically through their law enforcement portal: <https://www.whatsapp.com/records/login/>

WhatsApp also accepts preservation requests and emergency disclosure requests through the above listed portal.

Location to be Searched:

WHATSAPP, LLC.
1 Meta Way
Menlo Park, CA 94025

Identify Accounts By:

- Target Phone Number(s)
- Username (*Newer feature – not all users may create a username*)
- Target Email Address(es)

Items to be Seized:

WHATSAPP DATA:

To the extent that the information described is within the possession, custody, or control of WhatsApp, LLC (a subsidiary of Meta Platforms, Inc.), including any records, messages, content, logs, files, metadata, or deleted materials still accessible to WhatsApp, LLC or preserved pursuant to legal process or internal retention, **WhatsApp, LLC is required to disclose the following information for the Target Account(s) for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account phone number(s) registered to the WhatsApp account;
 - b. All prior phone numbers linked to the account (historical changes and verification attempts);
 - c. Account display names, profile photographs, “About” status messages, emoji statuses, and linked external websites;
 - d. Self-reported profile information including name, nickname, business name, short bio text, or tagline;
 - e. Account creation date and time, including registration IP address and device data;
 - f. Account deletion date and time, if applicable;
 - g. Timestamps of consent to WhatsApp Terms of Service, Privacy Policy, End-to-End Encryption notices, and other consent logs;
 - h. Push tokens associated with devices receiving push notifications for the Target Account(s).
2. **Device Information** related to the Target Account(s), including:

- a. Device identification information, including device make, model, IMEI, IMSI, MAC address, device tokens, and hardware identifiers used during registration or access;
 - b. Logs of all devices used to access the account and associated connection history;
 - c. Operating system versions, app version history, mobile carrier information, device language settings, and mobile network country codes.
 - d. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
- 3. **IP Address Information** for the Target Account(s), to include but not limited to:
 - a. Complete logs of IP addresses used to register, access, or transmit data through WhatsApp services;
 - b. IP addresses in both IPv4 and IPv6 format, with corresponding timestamps and port information if available.
- 4. **Linked Accounts & Meta Account Associations** to the Target Account(s), to include:
 - a. Facebook accounts linked via Meta infrastructure (if applicable);
 - b. Instagram or other Meta-owned platforms linked to the Target Account(s);
 - c. Device-based associations to Meta Platforms (cross-platform usage linkage via Meta's internal data).
- 5. **Usage Logs, Account Activity, and Metadata** for the Target Account(s), including the following:
 - a. Contact lists uploaded or synced by the Target Account(s), including phone numbers, names, and sync timestamps;
 - b. Group participation data, including:
 - i. Group chat names;
 - ii. Group participant rosters (current and historical members);
 - iii. Group creation dates, admins, owners, invitations sent/received, and join/leave events;
 - iv. Group metadata including group descriptions, photos, and identifiers;
 - c. Message metadata for all messages sent and received, including:
 - i. Message IDs;
 - ii. Sender and recipient(s);
 - iii. Timestamps of message transmission;

- iv. Message type (text, media, file, call, sticker, emoji, etc.);
 - v. Status indicators (delivered, read receipts, deleted messages, revoked messages);
 - d. Call logs, including voice and video call records, participants, start/end times, call durations, and metadata;
 - e. Status (Stories) usage including posted status updates, timestamps, viewers, and content types.
- 6. **Content (if available)**, including:
 - a. Any unencrypted message content recoverable by WhatsApp pursuant to preservation requests, or system failures resulting in server-side retention;
 - b. Media files uploaded but not yet delivered to recipients, temporarily cached on WhatsApp servers (including photographs, videos, voice recordings, or attachments);
 - c. Content associated with backups (to iCloud or Google Drive) if in possession of Meta Platforms, Inc., pursuant to lawful process (noting that backups may be separately subpoenaed from Apple/Google).
- 7. **Security and Account Protection Data**, including:
 - a. Two-factor verification settings, including PIN codes, security email addresses (if provided), and recovery credentials;
 - b. Device registration logs, encryption key rotation logs, and multi-device support logs;
 - c. Account compromise alerts, suspicious activity notifications, or unusual login events.
- 8. **Financial Transactions (if applicable)**, including WhatsApp Pay transaction records (where available), including payment method, sender/recipient, timestamps, transaction amounts, payment processor details, and financial account linkage.
- 9. **Consent, Legal Agreements, and Policy Acknowledgments**, including records of terms of service agreements, privacy policy acceptances, end-to-end encryption notifications, and timestamped records of user consents.
- 10. **Consent and Legal Agreement History**, further described as all consents, user agreements, privacy policy acceptances, terms of service agreements, opt-in/opt-out logs, and related timestamped records.

NOTE: This request specifically includes any content, metadata, and communications that may have been deleted, archived, modified, or hidden but remains accessible through WhatsApp's internal storage, caching, disaster recovery, or backup systems.

Affidavit Language:

Based upon my training, experience, consultation with other investigators, and information obtained during this investigation, I believe the following to be true:

WhatsApp is a globally popular encrypted communication platform owned by Meta Platforms, Inc., which also owns Facebook, Instagram, and other related services. WhatsApp offers users secure messaging, voice and video calling, file sharing, and multimedia communication features. Unlike many social media platforms, WhatsApp accounts are directly tied to a verified mobile phone number and utilize end-to-end encryption by default for most communications. The data maintained by WhatsApp is hosted on servers owned and controlled by Meta Platforms, Inc., independent of the user's physical device, and is accessible to law enforcement through lawful process such as search warrants or court orders, subject to certain limitations based on encryption and data retention.

WhatsApp users register with an active mobile phone number, which functions as the primary account identifier. In addition, users may set optional profile names (display names), profile photographs, and short status messages ("About" fields), which can assist law enforcement in identifying or corroborating account ownership. Device synchronization allows WhatsApp users to access their accounts across multiple devices, including mobile phones, tablets, desktop applications, and web browsers. WhatsApp maintains logs of device activity, including device identifiers, browser information, session timestamps, and related metadata, which can link a user to specific devices or access locations.

WhatsApp provides both one-on-one messaging and group chats. Users can exchange text messages, voice notes, images, videos, documents, contact cards, GPS location pins, and external links through these private encrypted conversations. While message content is typically encrypted end-to-end and not accessible to WhatsApp itself after delivery, WhatsApp does retain important metadata that is accessible to law enforcement through legal process. This metadata includes:

- Subscriber information such as the phone number associated with the account, registration timestamps, linked device identifiers, and limited account profile data;
- Contact lists synchronized from the user's device, including other WhatsApp accounts with which the user has communicated;
- Group membership records including group identifiers, creation timestamps, invited participants, and group subject names;
- Messaging metadata including sender and recipient phone numbers, message

- timestamps, media types exchanged, and message routing records;
- Connection logs showing IP addresses used to register, log in, and access WhatsApp services;
- Device metadata including platform versions, application versions, hardware identifiers, and multi-device synchronization records.

WhatsApp also collects financial information related to its WhatsApp Pay system (in regions where it is active), including payment account linkage, transaction records, recipient identifiers, and payment metadata. Although financial features are not currently widely deployed in the United States, they are increasingly present in international markets.

Based upon my training and experience, I am aware that criminal actors utilize WhatsApp for a wide variety of criminal activity because of its strong encryption, global reach, and widespread adoption. Offenders frequently exploit WhatsApp for:

- Narcotics trafficking coordination and negotiations via private messages and group chats;
- Child exploitation offenses involving grooming, illicit file exchanges, and coordination of illegal activity;
- Firearms trafficking, including exchange of contraband images, prices, and delivery arrangements;
- Human trafficking, organized theft rings, financial fraud schemes, and money laundering activity;
- Cross-border conspiracies involving foreign nationals using internationally registered phone numbers.

Because WhatsApp requires only a phone number for registration and allows users to create multiple pseudonymous accounts, suspects may use burner phones, anonymized SIM cards, or foreign phone numbers to conceal their identity. Additionally, the use of VPNs, anonymization tools, and multi-device syncing across multiple geographic regions can complicate identification efforts. However, WhatsApp's centralized servers maintain critical metadata records, subscriber information, connection logs, device information, and group membership records that may directly identify the user, their associates, devices used, and the scope of criminal activity.

Even if content is deleted by the user or devices are seized in airplane mode or wiped, much of the metadata and account information described above remains accessible via legal process directly to Meta Platforms, Inc. Through my experience, records maintained by WhatsApp are frequently the only means available to establish communication patterns, identify co-conspirators, corroborate victim disclosures, attribute devices to accounts, and reconstruct criminal activity that would otherwise remain hidden from law enforcement.

For these reasons, I believe that the requested records maintained by WhatsApp and Meta

Platforms, Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for WhatsApp:

WhatsApp is pretty heavily favored right now for the exchange of CSAM and is heavily used by drug trafficking organizations (DTOs) to communicate between the organizations and low level traffickers or “runners” moving contraband across borders or domestically. As such, it’s an application we’re likely to come across.

When crafting our “Items to be Seized” list, we should be **very specific** about what we want when dealing with Meta Platforms, as Meta will not produce records specifically mentioned in this list:

- Avoid “any and all records, data” type general requests, as they will not produce *a lot* of valuable content.
- The above example is “all encompassing” and includes almost every WhatsApp feature we could find. *It is highly unlikely* that you will need all of these – so be sure to “narrowly tailor” your warrant appropriately and remove items on that list if you can’t establish the relevance (or potential relevance) to your case.

End to End Encryption: WhatsApp is end to end encrypted communication, a feature which is *always* turned on for users’ accounts. As such, we will get *very limited* content from WhatsApp. This doesn’t mean that the content we do get won’t be useful, and we can definitely use the subscriber information and IP address information to tie suspect(s) to crimes perpetrated through WhatsApp.



Summary for Investigators:

Snapchat is a widely used social media and messaging application that allows users to send photos, videos, and text messages that are designed to disappear after being viewed. Originally popularized for its disappearing Snaps, Snapchat has since evolved into a robust multimedia platform featuring Stories, Group Chats, video calls, subscription channels, Spotlight videos, and Snap Map location sharing. Users create personal profiles using pseudonyms, Bitmoji avatars, or display names, often not tied to their legal identities, and communicate primarily through short-lived photo and video messages. The app is extremely popular among teenagers and young adults, making it a frequent platform of interest for law enforcement investigations involving juveniles, narcotics trafficking, exploitation, firearms trafficking, or fraud.

Despite its reputation for ephemeral content, Snapchat retains extensive metadata and account records on its servers that may be accessible through lawful legal process. These records can include subscriber registration data, device identifiers, phone numbers, IP address logs, Friends Lists, direct messages (to the extent saved by users), Memories, Private Stories, Group Chats, Snap Map location history, and My Eyes Only encrypted content. Snapchat's disappearing message design often gives offenders a false sense of security; however, the company's internal retention of metadata, device data, location information, and deleted content logs often provide critical digital evidence even if content is no longer visible on a suspect's device.

How to Serve with Legal Process:

Snap, Inc. accepts legal process electronically through their law enforcement portal: <https://less.snapchat.com>

Snapchat also accepts preservation requests and emergency disclosure requests through the above listed portal.

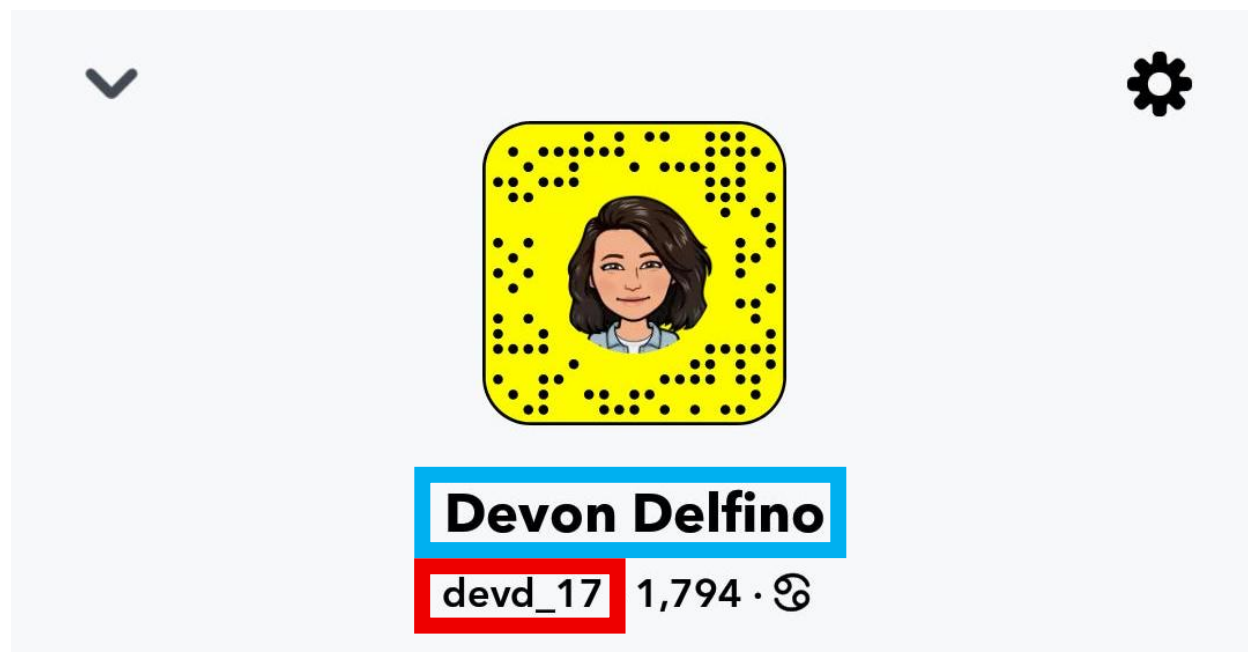
Location to be Searched:

SNAP, INC.
2772 Donald Douglas Loop,
Santa Monica, CA 90405

Identify Accounts By:

Snapchat accounts can be identified in legal process by:

- User ID Number *(You'll only have this if you have a warrant return)*
- Username **(See below. DO NOT accidentally use their vanity name!)**
- Target Email Address(es)
- Target Phone Number(s)



*Very Important: In the above image, the **username** (which we need for legal process) is highlighted with a **RED BOX**. The blue box below it is a **display name**. If you provide Snapchat with a display name by mistake, they **will NOT** produce records. **Careful!***

Items to be Seized:

SNAPCHAT DATA:

To the extent that the information described is within the possession, custody, or control of Snap Inc., including any records, content, files, messages, logs, metadata, behavioral profiles, deleted materials still available to Snap Inc., or preserved pursuant to lawful legal process, Snap Inc. is required to disclose **the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account Username(s), historical usernames, display names, vanity names, alternate handles, aliases, retired usernames, and pseudonyms ever associated with the account;
 - b. Account creation date, timestamp, originating IP address, device identifiers at creation;
 - c. Account deletion date, deactivation/reactivation timestamps, and IP/device information associated with deletion or recovery;
 - d. Legal name (if provided), profile name, pronouns, birthdate, self-reported demographic information, gender identity, and language preferences;
 - e. Email addresses (current and historical, verified or unverified), mobile phone numbers (current and historical, verified or unverified), and timestamps of additions, verifications, or removals;
 - f. Bitmoji data linked to the account, including custom Bitmoji avatars, outfits, 3D Bitmojis, "Friendmoji" data, Bitmoji Stories participation;
 - g. Public Profile information, including Public Story status, subscriber counts, Spotlight eligibility, public bio, external website links, and visibility settings;
 - h. Snapchat+ Subscription status, tier level, subscription start/end dates, perks or experimental features enabled;
 - i. Payment and billing profile details including full billing names, addresses, credit/debit card numbers (obfuscated or tokenized as retained), linked payment processors, and purchase histories (Snapchat+, Boosting, Spotlight promotions, Lens Store purchases, Snap Token balances, in-app purchases);
 - j. Privacy Settings to include whether stories and snaps are shared with friends or public.
2. **Device Information** related to the Target Account(s), including:
 - a. Device identification data (IMEI, IMSI, MAC address, Device Fingerprint ID, Android ID, UDID, Advertising ID, Apple Identifier for Advertisers);
 - b. User-agent strings, device models, hardware platform versions, operating system versions, app versions, timezone settings, and regional configurations;
 - c. Complete device history reflecting all devices accessing the account, connection timestamps, login methods (biometric unlock, FaceID, etc), biometric enrollment tokens (if applicable);

- d. Web-based logins at accounts.snapchat.com or Snap Web versions, including browser identifiers, cookies, and session metadata.
 - e. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
3. **IP Address Information** for the Target Account(s), to include but not limited to:
- a. Complete IP logs for all account sessions, logins, logouts, Snap Map check-ins, Spotlight uploads, chat sessions, audio/video call sessions, subscription management, purchases, advertising interactions, third-party logins;
 - b. IPv4, IPv6 addresses, port numbers (if available), session start/end times, passive telemetry (background refreshes, app updates, push notification polling).
4. **Financial, Billing, and Monetization Records** for the Target Account(s), to include:
- a. Complete transaction histories related to Snapchat+, in-app purchases, Boosts, Spotlight payments, Snap Tokens, premium Lenses, Snap Map ads, AR Lens campaigns, business advertisements, or creator monetization payouts;
 - b. Linked payment instruments, tokenized card details, refund histories, payout account information for creators (bank account details for Spotlight earnings), and suspended or frozen balances due to violations.
5. **Usage Logs and Account Activity** of Target Account(s), including the following:
- a. Conversations (1:1 or Group Chats), including sender/recipient information, message content, timestamps, read receipts, message deletion logs, unsend attempts, message edit history (if applicable), records of screenshots / screen recordings / saves, emojis, stickers, Bitmoji reactions, contact cards, shared profiles, external links;
 - b. Chat Media content, either sent or received by the Target Account(s), including any photographs, videos, audio files, captions, filters, overlays, drawing annotations,;
 - c. Snap Media (sent and received): photo, video, AR Lenses used, captions, filters, overlays, drawing annotations, augmented reality (AR) content created or used;

- d. Stories (Public Stories, Private Stories, Shared Stories, Group Stories), including posting times, audience lists, Snap IDs, GPS tags, media overlays, and subscriber viewing logs;
- e. Memories: All saved Snaps, Stories, Chat attachments, including metadata, creation timestamps, location data, source, upload device, EXIF data, edits, replays, and shares;
- f. My Eyes Only: All secured, PIN-locked content with timestamps, storage identifiers, and associated encrypted data (whether or not recoverable to Snap Inc.);
- g. Spotlight: Full submission history including videos submitted for Spotlight, monetization eligibility status, reward payouts, performance analytics, engagement metrics, and takedown logs;
- h. Subscriptions (Public Post subscriptions, channel follows), including subscription join dates, notification settings, follow/unfollow logs, channel interaction histories;
- i. Call Logs for voice and video calls, including participant lists, call durations, timestamps, connection quality metrics, and participant device metadata;
- j. Friends Lists & Friends Logs (current and historical), including date friendships were established, friend removals, blocks, unfriends, friend requests sent/received, ignored requests, and information on who requested / added / blocked / deleted who;
- k. Contacts uploaded or synced from device address books;
- l. Search Histories (usernames searched, Snap Map searches, Spotlight searches, Lens searches, hashtag searches);
- m. Snap Map usage logs, including location-based search queries, Place tagging, and Discover content viewed.

6. Deleted Content and Deletion Logs, including:

- a. Deletion logs for all Snaps, Chats, Memories, Stories, or Spotlight posts deleted by user, including deletion timestamps;
- b. Content flagged by Snap Inc. for potential Terms of Service violations, suspected prohibited content, or enforcement flags.

7. Location Data collected, retained or possessed by Snap Inc. for the Target Account(s):

- a. GPS coordinates, Wi-Fi proximity, Bluetooth beacons, IP-based geolocation, device-based location logs, cell site location information (CSLI), or any other geospatial data collected or retained by Snap Inc.;

- b. Complete Snap Map data, including live locations, Ghost Mode toggling history, Bitmoji location updates, location sharing settings, passive background telemetry, check-in history, Places visited, home/work location inference models;
 - c. Geolocation metadata embedded in Snaps, Stories, Memories, and Spotlight submissions.
- 8. **Advertising, Behavioral Targeting, & Algorithmic Personalization Data**, including:
 - a. Interest profiles derived by Snap Inc. based on user behavior including content preferences, subscription interests, Snap Map exploration, Spotlight trends, engagement with AR lenses, Snap Kit connected apps, demographic models, and affinity clusters;
 - b. Ad targeting records including ad impressions, clickthrough histories, ad engagement logs, purchase behaviors, device targeting parameters, ad preferences and suppression lists;
 - c. Advertiser profile segments assigned to the Target Account(s), including inferred demographics, psychographic segments, AR shopping behavior, virtual try-on activity, and purchase intent data.
- 9. **Third Party Integrations & Authorized Applications**, including:
 - a. OAuth authorized apps via Snap Kit platform, including Bitmoji third-party integrations, Gaming SDK authorizations, and external platform logins;
 - b. Connection timestamps, scopes of permissions granted, revocations, external account identifiers, and data exchanged between Snapchat and authorized third-party applications.
- 10. **Security and Account Protection Data**, including:
 - a. Password changes, reset history, recovery attempts, phone/email recovery credential usage;
 - b. Two-factor authentication (TFA) enrollment, trusted device registrations, biometric unlock enrollments, and security event logs;
 - c. Suspicious login flags, anomalous geolocation access attempts, VPN or proxy detection flags, and login anomaly alerts;
 - d. Session hijacking flags, bot detection events, and account compromise records.
- 11. **Biometric, AI, and Moderation Data**, further described as:

- a. Content flagged through Snap’s Trust & Safety AI scanning systems, including automated CSAM detection, extremist content flags, prohibited goods sales detection (firearms, drugs, etc.), sextortion markers, nudity detection, or grooming behavior models;
- b. AI-based image, text, and video scanning summaries used for compliance and moderation.

12. Consent and Legal Agreement History, further described as all consents, user agreements, privacy policy acceptances, terms of service agreements, opt-in/opt-out logs, and related timestamped records.

NOTE: This request encompasses any data that may have been deleted, modified, archived, or hidden but remains accessible to Snap Inc. via internal data retention systems, backups, preservation holds, disaster recovery processes, cached storage, encrypted archives, or system-maintained metadata repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Snapchat is a widely used mobile-based social media and messaging platform owned and operated by Snap Inc., headquartered in Santa Monica, California. Snapchat offers users a variety of communication features including multimedia messaging, temporary content sharing, persistent saved content, voice and video calling, public content publishing, and a location-based social discovery system. Snapchat operates through centralized servers controlled by Snap Inc., and data stored on the platform remains accessible to Snap Inc. through lawful legal process such as search warrants, subpoenas, and preservation requests, even if users attempt to delete content or reset devices.

Snapchat users create accounts using email addresses and mobile phone numbers, and accounts are operated under self-selected usernames and public display names. Snapchat allows users to customize profiles with Bitmojis (personalized cartoon avatars), profile photos, bios, and public display information. Many users employ pseudonyms or screen names instead of legal names. Despite this, subscriber registration records, verified contact information, device metadata, and IP address logs retained by Snap Inc. can assist law enforcement in identifying account holders and linking devices to accounts.

Snapchat’s primary form of communication is its multimedia messaging system known as “Snaps” — temporary photos, videos, and messages that are designed to disappear after viewing but may be preserved under certain conditions. Users may also engage in traditional text-based “Chats” which can include text, emojis, stickers, Bitmojis, voice

notes, video attachments, and external media links. Snapchat allows individual private messaging as well as group chats, many of which support multimedia file sharing, file attachments, and real-time voice and video communication. Based on my training and experience, these private messaging features are frequently exploited by criminal actors to coordinate illegal activities.

Snapchat includes numerous additional features generating digital evidence relevant to criminal investigations, including:

- Stories: Temporary posts (photos, videos, or text) viewable by all friends, select friends (“Private Stories”), or public followers, often containing metadata such as timestamps, geotags, device identifiers, and lists of viewers;
- Spotlight: A public-facing content-sharing feature for viral short videos, including likes, comments, shares, and engagement metrics;
- Public Profiles and Subscriptions: Allowing users to publicly publish content, gain followers, monetize their content, and create branded or influencer-based accounts;
- Memories: A persistent cloud-based storage system where users save Snaps, Stories, and other content indefinitely, including separate encrypted storage called “My Eyes Only” which may contain sensitive or illicit materials;
- Location Features (Snap Map): A geolocation tool which displays a user’s current or historical location data, including real-time movements, passive background location collection, and location-based tagging attached to Snaps and Stories;
- Group Stories and Shared Group Environments: Enabling collaborative posting and media sharing across multiple users;
- Friends Lists and Friends Activity Logs: Showing friendships, friend requests, blocking, muting, and account interaction history over time;
- Voice and Video Call Logs: Capturing metadata on real-time audio and video calls conducted via Snapchat.

Snapchat maintains extensive server-side metadata related to content deletion, edits, password resets, security events, and account recovery attempts. Even when users attempt to delete messages, memories, stories, or entire accounts, deletion logs often remain available to Snap Inc. that can demonstrate when and how content was modified or removed.

In addition to content and communications, Snapchat collects extensive device, technical, network, and location data associated with user activity, including:

- IP Address Logs (both IPv4 and IPv6), with session timestamps, connection durations, and associated port data;
- Device Identifiers including IMEI, IMSI, MAC addresses, device fingerprints, browser versions, app versions, operating system data, and hardware specifications;
- OAuth-linked third-party applications or integrations connecting Snapchat

- accounts to other platforms;
- Geolocation data including real-time GPS, Wi-Fi signals, cellular tower triangulation (CSLI), Bluetooth proximity signals, inferred “Home” and “Work” locations derived through Snap’s machine learning analysis.

Snapchat also maintains financial and transactional records for in-app purchases, Snapchat+ subscriptions, Spotlight monetization payouts, creator monetization programs, and payments associated with premium features or advertising activity. These financial records can provide additional identifying information including linked credit cards, billing addresses, financial account numbers, and transaction histories.

In my training and experience, individuals involved in criminal activity often use Snapchat to engage in a variety of unlawful conduct, including but not limited to:

- Narcotics trafficking where offenders advertise controlled substances through Stories, Private Stories, Spotlight videos, and “emoji-coded” Snaps, then negotiate transactions privately via chat or calls;
- Weapons trafficking where individuals exchange photos or videos of firearms, post firearms-for-sale content in Private Stories, or coordinate illegal firearms transactions via private group chats;
- Sexual exploitation or human trafficking where offenders locate, recruit, exploit, or groom vulnerable victims through private chats, location-based discovery features, and encrypted “My Eyes Only” storage;
- Fraud, identity theft, and financial scams where criminal actors share stolen personal identifying information, financial credentials, or conduct financial fraud through peer-to-peer contact facilitated by Snapchat’s social discovery tools.

Criminal suspects frequently attempt to conceal their identity on Snapchat through the use of burner phones, pseudonymous usernames, temporary emails, VPNs, proxies, and privacy settings designed to limit public visibility. However, Snap Inc. retains extensive internal records — including subscriber registration logs, IP address histories, device metadata, contact sync uploads, friend activity logs, location data, deleted content logs, and financial transaction records — which are essential to identifying suspects, corroborating victim disclosures, and documenting criminal networks.

Even when content has been deleted, Snap Inc.’s servers may preserve records through backup retention, system logs, caching, disaster recovery, preservation requests, and server-side metadata which remains accessible through lawful legal process.

In my experience, data maintained by Snap Inc. serves as a critical resource for reconstructing historical communications, identifying co-conspirators, recovering deleted evidence, documenting criminal intent, and establishing the full scope of criminal activity associated with Snapchat accounts. Because Snapchat data is hosted entirely on Snap Inc.’s servers, search warrants issued directly to Snap Inc. often represent the only method available to law enforcement to fully recover evidence relevant to the investigation.

For these reasons, I believe that the records maintained by Snap Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for Snapchat:

When crafting our “Items to be Seized” list, we should be **very specific** about what we want when dealing with Snapchat, as Snap Inc. will not produce records specifically mentioned in this list:

- We routinely see Snapchat data productions that are missing things like birthdates, privacy settings, memories logs, etc. because they weren’t specifically requested. We aren’t kidding – they’re *that* specific.
- Avoid “any and all records, data” type general requests, as they will not produce *a lot* of valuable content.
- The above example is “all encompassing” and includes almost every Snapchat feature we could find. *It is highly unlikely* that you will need all of these – so be sure to “narrowly tailor” your warrant appropriately and remove items on that list if you can’t establish the relevance (or potential relevance) to your case.
- **Note how we specifically use Snapchat’s “names” for things like Snaps, Memories and Chat Media?** It’ll ensure you don’t miss evidence.

In 2020, Snapchat’s response to warrants could take 2-3 months. This is no longer the case! In most instances, data is produced within **a few days**.

Snapchat produces **all records** as multimedia files or spreadsheets, making going through the production data easy with some basic Microsoft Excel knowledge.

Prior to 2025, if Snapchat did not have anything, they didn’t produce a log. We were left to wonder if they *really* didn’t have anything, or if they checked and confirmed this. That was recently changed – and now we will receive logs that say “No responsive data found.” This should minimize instances where we *wonder* if they *really checked*.

Snapchat maintains extensive IP addresses – although they didn’t always. Historically it was *just* logins and logouts, but today we see most activity on Snapchat resulting in IP addresses being captured. Expect *thousands* of IP address records.

*Note: Within the IP address logs, we’ll see login / logout history. Most Snapchat users will **not** regularly login and logout. If you are seeing **tons** of logins and logouts – it’s indicative that your suspect likely has more than one Snapchat account and is jumping back and forth (because Snapchat only allows you to be logged in to one account at a time).*

Snapchat may possess location data in two locations: a spreadsheet titled “Geolocations” and a spreadsheet titled “Memories.” Ask for both and check both!

If you ask for a “friends **list**” in your warrant you will get *just that* – literally a list of somebody’s friends. We should be asking for the “friends **log**” which will contain far more data and information for us such as who added who, timestamps, and activity (blocks, deletions, requests, etc.).

All multimedia files contain corresponding logs (IE: Memories files are detailed with associated metadata and information in the “Memories Log.”) Ask for these!

My Eyes Only files come through as encrypted files that are essentially useless and cannot be decrypted by us or Snap, *but* they will indicate to us that a user takes advantage of that “hidden” multimedia vault and we may prioritize getting a passcode to access it from a user’s phone when they are arrested.

Conversations can be *hit or miss*. We may get *a ton*, and we may get very little. It’s dependent on a number of factors such as the user’s settings, how they interact with Snapchat (if they “save” chats regularly), and how often they use Snapchat.

Memories remains the **#1 location** where we tend to find a majority of our incriminating content evidence. Memories are kept *indefinitely* until a user deletes their account (see below) or are individually deleted by users.

When accounts are **deleted** by users (in their entirety, not just specific things on the account deleted), Snapchat will place them in a state called “deactivated” for 30 days, giving users time to consider if they *really want to* delete their account. As such, if a suspect deletes their account, we *may* have up to 30 days to get a preservation letter into Snapchat and still obtain the data. Act quickly!

Final note – A *LOT* of data on Snapchat is **very perishable** including conversations (chats), story posts, snaps, etc. I cannot emphasize this enough: Submit a preservation letter as soon as you can. Take for example story posts – they remain up and available for 24 hours. If somebody posted a video of a murder on their story, you have 24 hours to preserve that or it may be gone (assuming they didn’t save it to their memories). Authoring a quick search warrant (IE: “I’ll just knock out a warrant real quick”) is not a substitute for a preservation request – it may take Snap, Inc. 3-5 days to process your warrant (well outside the 24 hours we have to capture a story). Preservation requests are processed *much quicker* and increase our likelihood of capturing vital evidence.

TELEGRAM



Summary for Investigators:

Telegram is a cloud-based messaging platform that has become one of the most widely used applications by criminal actors as of 2025. While originally marketed as a secure alternative to mainstream messaging apps, Telegram offers a combination of features highly attractive to offenders — including the ability to create accounts with minimal identity verification, support for large group chats (channels), encrypted messaging, self-destructing messages, file sharing, and a strong culture of privacy and minimal moderation. Telegram allows users to join massive public and private groups related to any topic, including drug sales, fraud, firearms, cryptocurrency scams, child exploitation, and other criminal enterprises. The platform's ease of use, global reach, and weak enforcement of content violations make it one of the most prolific modern platforms for organized criminal activity.

Unlike some other social media platforms, Telegram provides extremely limited data in response to legal requests. Telegram may only provide basic subscriber records such as the registered phone number, username, account ID, recent IP addresses, and last login time. Telegram typically does not provide message content, chat logs, or media files, even when served with lawful process, making proactive investigative techniques, undercover operations, open-source monitoring, and device-based extractions critical when investigating Telegram-based criminal activity. As of 2025, Telegram remains one of the highest-priority platforms for law enforcement due to its widespread adoption by criminals across nearly every investigative discipline.

How to Serve with Legal Process:

Telegram **did not** comply with legal process prior to 2024. Since then, they have produced *extremely limited data* to US law enforcement responsive to legal process.

Telegram accepts legal process via email at content-referral-u1@telegram.org.

As of the time of this writing, it is believed Telegram **will not** cooperate with preservation requests or emergency disclosure requests.

Location to be Searched:

TELEGRAM

Law Enforcement Response Team

**Telegram does not provide a service address.*

Accepts legal process online via email at: content-referral-u1@telegram.org

Identify Accounts By:

- Username
- Target Phone Number(s)

Items to be Seized:

TELEGRAM DATA:

To the extent that the information described is within the possession, custody, or control of Telegram Messenger LLP, including any account registration information, technical logs, records, metadata, or historical access information that remains available to Telegram Messenger LLP, or has been preserved pursuant to legal process or internal retention, Telegram Messenger LLP is required to disclose the following records for the Target Account(s), for the time period of **January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Telegram account User ID number(s);
 - b. Telegram username(s), including current and historical usernames, display names, handles, vanity names, or pseudonyms associated with the account;
 - c. Mobile phone number(s) linked to the account, including current and historical phone numbers used for registration, reactivation, or account recovery;
 - d. Account creation date and time, including IP address and device metadata (if retained) at the time of account registration;
 - e. Account deletion date and time (if applicable), with any associated IP addresses or device identifiers;
 - f. Consent, user agreements, or legal acknowledgments maintained by Telegram associated with the Target Account(s).
2. **Device Information** related to the Target Account(s), including:
 - a. Full historical IP address connection logs reflecting logins, logouts, active sessions, device connections, or authentication attempts, including timestamps, IPv4 and IPv6 addresses, and port information (if available);
 - b. Device identifiers, device models, operating systems, user-agent strings, and platform versions associated with account logins or active sessions (if retained);
 - c. Geolocation metadata (if retained) related to any IP address, device session, or logins for the Target Account(s);

- d. Last known login date/time and IP address for the Target Account(s), including active or most recent session information available to Telegram.

3. Cross-Account Associations and Linked Accounts, including:

- a. Any alternate Telegram accounts linked via the same mobile phone number, device identifier, or cross-registration data (if available);
- b. Known device-based associations between the Target Account(s) and any additional Telegram user accounts accessed from the same hardware or IP addresses.

4. Payment and Financial Account Information (if available):

- a. Any payment methods, financial instruments, or billing addresses provided to Telegram Messenger LLP related to premium subscriptions, Telegram Premium, Telegram Ads, or other monetization features connected to the Target Account(s);
- b. Transaction history, payment dates, subscription enrollment dates, payment processors used, and linked financial institutions (if retained).

5. Account Enforcement, Warnings, and Sanctions, including:

- a. Any internal flags, policy violations, content moderation reports, or administrative sanctions issued against the Target Account(s);
- b. Suspension history, warning notifications, or moderation actions undertaken by Telegram Messenger LLP against the Target Account(s).

NOTE: This request includes any subscriber or technical account data, logs, records, or metadata, even if content of messages or chats is not accessible to Telegram Messenger LLP due to their encryption model, but remains otherwise available through internal record-keeping, preservation requests, backup systems, disaster recovery servers, or cached administrative logs.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Telegram is a global encrypted messaging and social media platform operated by Telegram Messenger Inc., which maintains infrastructure outside the United States and operates in multiple jurisdictions. Telegram allows its users to communicate via private messaging, group chats, public channels, and file-sharing services. Telegram is widely

used for both legitimate communications and for criminal activity due to its strong privacy features, minimal moderation policies, end-to-end encryption options, and decentralized global presence. Information retained by Telegram remains accessible to law enforcement through lawful legal process, though Telegram's publicly stated cooperation with law enforcement is limited and typically confined to production of limited subscriber records when compelled by valid court orders.

Telegram allows users to create accounts using only a mobile phone number, without requiring a real name or verifiable identity. Users may operate under pseudonyms, screen names, vanity usernames, or aliases, and may utilize profile photos, avatars, biography text, and external links to further obscure their identity. Telegram permits the operation of multiple accounts, and user accounts may be linked to multiple devices simultaneously. Telegram's username-based system allows users to communicate without sharing their actual phone numbers, complicating efforts to directly associate a Telegram account to a real-world individual absent subpoenaed records.

Telegram offers a variety of communication features commonly exploited by individuals engaged in criminal conduct, including:

- One-on-one encrypted chats (Secret Chats), which utilize end-to-end encryption and leave no server-side record on Telegram's infrastructure;
- Standard cloud-based chats (non-encrypted server-side storage), which are accessible across devices and are retained by Telegram;
- Group chats, which allow up to thousands of users to communicate, including organized criminal groups using large private communities;
- Public and private "Channels," which operate like broadcast feeds where one or more administrators distribute messages, videos, images, files, or hyperlinks to mass audiences;
- File-sharing functionality allowing users to distribute large multimedia files (including video, audio, documents, compressed archives, or application packages).

Based on my training and experience, Telegram's privacy features are regularly exploited by individuals involved in criminal activity, including child sexual exploitation, narcotics trafficking, firearms trafficking, money laundering, fraud, identity theft, organized criminal enterprises, terrorism, and the sale of illicit digital content. Offenders often utilize Telegram to coordinate criminal activity with large distributed groups of co-conspirators while avoiding conventional law enforcement detection. Telegram's allowance for large file transfers, minimal content moderation, and the ease of operating anonymously or pseudonymously make it particularly attractive to offenders seeking to distribute illegal content or plan criminal operations.

In my training and experience, Telegram retains limited account data accessible to law enforcement under valid legal process, which may include:

- The registered mobile phone number used to create or verify the account;
- The user's Telegram username, including current and prior usernames;
- An internal Telegram account ID number unique to each account;
- The most recent IP address used to log into the account;
- The last login date and time associated with the account;
- Device metadata, such as authorized session devices, connected clients, operating system versions, application version numbers, and limited device identifiers.

While Telegram does not typically retain message content for end-to-end encrypted Secret Chats, standard cloud chats, public channels, and large group chats may leave server-side records accessible internally to Telegram for operational purposes, though production of such content to law enforcement has been limited historically. Telegram's published law enforcement policy indicates that full message content disclosure occurs only in limited circumstances involving terrorism-related offenses pursuant to applicable laws in the jurisdictions where Telegram operates.

Even where Telegram accounts are deleted or reset, Telegram may retain certain internal identifiers, registration records, and limited login metadata that may allow law enforcement to identify account holders, confirm device usage patterns, trace IP addresses to locations or service providers, and associate otherwise anonymous Telegram activity to known suspects when correlated with other evidence.

In my experience, the subscriber information, IP address logs, phone number records, username history, device sessions, and account creation metadata maintained by Telegram may provide critical leads to positively identify suspects, corroborate victim or co-conspirator statements, and reconstruct communications central to ongoing criminal investigations. Due to the nature of Telegram's infrastructure, this server-side data is often the only method available to law enforcement to associate Telegram activity with real-world identities when physical devices or account credentials are unavailable.

For these reasons, I believe that the requested records maintained by Telegram Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for Telegram:

When it comes to “the application” for criminal activity on social media right now, Telegram is the one. Prior to 2024, they did *not* comply with any US legal process. That changed (and I won’t get into *why*), but now they produce *very limited information*. However, they do comply with US legal process (including state level warrants).

As you’ll see, they don’t provide an “address of service” but rather an email address only. This is in line with their practices of confidentiality and anonymity. This can be off-putting to some issuing magistrates reviewing warrants and court orders.

The “Items to be Seized” list encompasses a lot of things that *we believe* based on a review of their privacy policy that Telegram likely possesses, but don’t expect all of that in your legal process productions. What we’ve seen is an email response that typically includes:

- Telegram username (which you probably already have)
- Telegram account number (which doesn’t really mean anything to us)
- Phone number
- IP address
- The last time the account was logged in to.

And that’s it. *But – with that being said*, if we’re working a Telegram account selling CSAM material, drugs, firearms, fraud, identity theft, etc., that can be *more than useful* to help us identify the account holder or tie evidence we’ve obtained in other ways to them – so don’t underestimate the value of a Telegram search warrant, despite how limited the response may be.

IMPORTANT NOTE: We recently have heard reports that Telegram will *refuse to honor legal process* if the “Nature of the Investigation” and the “Nexus to Telegram” are not **clearly** outlined within the legal process, or at least the portion of the legal process we send Telegram. Despite the fact that Telegram *probably can’t require that* and furthermore *it’s likely within our Affidavit of Probable Cause* which we won’t typically send to Telegram – it’s likely worth including *just to avoid the headache*.

It’s worth noting *we have absolutely no idea* if Telegram actually complies with non-disclosure orders or extensions to them, so consider that when serving legal process.

It’s also worth noting that the **most effective way** of working Telegram cases still remains undercover accounts and trying to work off the platform. If we can convince a suspect to give up his/her CashApp account (to accept payment for contraband) or meet us to sell us drugs, that remains the best strategy to working these cases.

Summary for Investigators:

Signal is a secure messaging application heavily favored by individuals engaged in criminal activity due to its strong encryption, privacy features, and minimal data retention policies. All messages, calls, voice notes, attachments, and group chats on Signal are end-to-end encrypted by default, meaning Signal itself cannot access or decrypt message content, call logs, or media files. Even metadata such as who is messaging whom is limited or deliberately obfuscated. Signal does not store contacts, message history, IP address logs, or traditional subscriber information on its servers. The app is linked only to a phone number for account creation and does not require usernames or email addresses, further enhancing anonymity.

Because of these security features, Signal is often used by criminal actors for activities including drug trafficking, firearms transactions, money laundering, fraud, exploitation, and criminal conspiracy communications.

Information on Legal Process to Signal

Signal *can* be served with a search warrant if you provide them an account phone number. They will produce the following:

- Date / Time Account was Created
- Date / Time Account was Last Logged Into

Yep – that’s it. Pretty useless for most investigations. And FYI – they will post a redacted copy of your warrant on their website to bolster their reputation as being exceptionally private and unable to provide data to law enforcement. If they aren’t authorized to, they will go to court and fight to unseal records so they can post it.

See their “Government Requests” webpage: <https://signal.org/bigbrother/>

As such, I’m not including any affidavit language or warrant language for Signal at this time. If the situation with Signal changes, I will update this guide.



Summary for Investigators:

TikTok is a short-form video sharing platform that allows users to create and share videos up to several minutes in length, often featuring music, filters, text overlays, and special effects. The app's core feature is the "For You" page — a highly personalized feed where TikTok's algorithm recommends content based on a user's prior activity, interests, and interactions. Users can follow accounts, like videos, leave comments, share content, and participate in viral trends using popular sounds, hashtags, and challenges. Features like "Duets" and "Stitches" allow users to remix or respond to other users' videos, fostering interaction and content chaining.

While TikTok can be used purely for entertainment, it also functions as a robust social media platform with direct messaging, livestreaming, and even e-commerce capabilities. Many users share personal information through their profile bios, tagged locations, or live video interactions. Because TikTok's algorithm often exposes content to large audiences far beyond a user's existing followers, strangers can easily discover, follow, and interact with minors or vulnerable users — making it increasingly relevant in criminal investigations involving child exploitation, drug sales, threats, or recruitment into illicit activity.

How to Serve with Legal Process:

TikTok accepts legal process electronically through their law enforcement form:
www.tiktok.com/legal/report/lawenforcementrequest

Meta also accepts preservation requests and emergency disclosure requests through the above listed form, and emergency disclosure requests here:
<https://www.tiktok.com/legal/report/EDR>.

Location to be Searched:

TIKTOK, INC.
5800 Bristol Parkway Suite 100
Culver City, CA 90230

Identify Accounts By:

Per Facebook's Law Enforcement Guidelines webpage (<https://about.meta.com/actions/safety/audiences/law/guidelines>), they require that we provide one of the following account identifiers:

- User ID Number *(You'll only have this if you use a tool or have a warrant return)*

- Username (**See below. DO NOT accidentally use their vanity name!**)
- Target Email Address(es)
- Target Phone Number(s)

Items to be Seized:

TIKTOK DATA:

To the extent that the information described is within the possession, custody, or control of TikTok Inc., including any messages, records, files, logs, or information that have been deleted but are still available to TikTok Inc., or have been preserved pursuant to a request, TikTok Inc. is required to disclose the following information for the Target Account(s).

All of the following records, ranging from the time period of January 1, 2025 to the date this search warrant is signed:

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Account usernames, all historical username changes, previously used handles, vanity names, retired aliases, alternate spellings, and nicknames associated with this account or any linked accounts;
 - b. Display names, account presentation names, and associated change logs;
 - c. Birthdate, stated age, and any age verification or adjustments applied to the account;
 - d. Mobile phone numbers associated with the account, including all historical changes or deletions;
 - e. Email addresses associated with the account, including historical changes, deletions, or updates;
 - f. Profile photographs, avatars, Bitmojis, or digital likenesses uploaded or generated for the account profile;
 - g. Self-reported profile information, including biography text, personal website links, external social media handles, pronouns, gender identity, sexual orientation, political views, religious affiliations, language preferences, location information (hometown, residence history), and relationship status including linked friends, family members, or tagged partners;
 - h. Account creation date and time, including IP address captured during initial registration;
 - i. Account deletion date and time (if applicable), including any associated IP address data;
 - j. Records of account deactivation, reactivation, or reinstatement history;

- k. Historical security and privacy setting changes, including password modifications, enrollment in two-factor authentication, generation of recovery codes, use of security keys, privacy setting adjustments, and account recovery contact information;
 - l. Linked financial accounts, billing addresses, payment methods, and any financial information provided for in-app purchases, TikTok Coins, subscriptions, Creator Fund, advertising services, or e-commerce tools;
 - m. Records of user consents, terms of service acceptances, privacy policy acknowledgments, community guidelines acceptances, and any other consent logs associated with the Target Account(s).
2. **Device Information** related to the Target Account(s), including:
- a. Unique device identifiers including IMEI, IMSI, MAC addresses, hardware IDs, and device fingerprints;
 - b. Logs of all devices accessing the Target Account(s), including device type, device model, manufacturer, and device connection histories;
 - c. Complete device session logs reflecting logins via mobile apps, web browsers, third-party integrations, or authorized connected devices;
 - d. Browser user-agent strings, operating system versions, app version numbers, and platform identifiers captured during device access sessions.
3. **IP Address Information** for the Target Account(s), to include but not limited to:
- a. Complete logs of all IPv4 and IPv6 addresses utilized to access, log into, log out of, stream from, or otherwise interact with the account, including passive telemetry, background activity, app updates, content uploads, streaming sessions, API activity, and any other device-initiated or system-initiated sessions;
 - b. Port information associated with all IP address logs, if available.
4. **Linked Accounts** to the Target Account(s), to include:
- a. Facebook, Instagram, Google, Apple, or other third-party accounts linked to the Target Account(s) via cookies, device sharing, OAuth integrations, or cross-platform login services;
 - b. Alternate TikTok accounts managed or accessed by the same user or device fingerprint, including pseudonymous or business accounts;
 - c. Device-based linkage of accounts via hardware signatures or app session metadata.
5. **Usage Logs and Account Activity** of Target Account(s), including the following:

- a. Full Direct Message and Group Message records including sender, recipient(s), date, time, message content, attached media files (photos, videos, audio), embedded links, contact cards, or profile sharing elements transmitted through messaging services;
 - b. All content interactions on videos, including likes, comments, shares, reposts, saves, reposted content metadata, and any user-generated engagement;
 - c. Detailed logs of Duet and Stitch activities including participant identifiers, timestamps, media content attached, and engagement metrics;
 - d. Story usage data, including Story creation, Story viewer lists, Story engagement logs, reactions, comments, audience selection (e.g., Close Friends or private Stories), and story expiration or deletion timestamps;
 - e. LIVE stream session logs, including participant lists, moderators, gift transactions, chat interactions, viewer counts, session durations, recording metadata, archived or deleted LIVE content, and monetization details associated with live broadcasting sessions;
 - f. Audio Room sessions or multi-hosted live sessions, including participant rosters, chat logs, timestamps, and associated metadata;
 - g. Saved content and personal media collections, including bookmarked posts, favorited videos, archived stories, or stored drafts;
 - h. Comprehensive search and browse history across the application, including search queries, profile views, hashtag searches, trending content interaction, and viewed creator profiles;
 - i. Administrative enforcement logs reflecting moderation actions, content takedowns, community guideline strikes, appeal outcomes, or account restriction history;
 - j. Internal content classification tags generated by TikTok's automated moderation systems including, but not limited to, flags for illegal drug sales, weapons, violence, sexual exploitation, CSAM, or extremist content detection;
 - k. API activity logs related to any automated third-party tools, scheduling bots, automation services, engagement amplification services, or externally operated tools interacting with the Target Account(s) whether authorized via OAuth or detected through backend analysis.
6. **ALL Content**, including photographs, videos, audio files, text, and encrypted files, maintained by TikTok Inc., related to the Target Account(s), including:
- a. All video posts uploaded or shared to TikTok, whether public, private, draft, or deleted;

- b. Duet, Stitch, Reply Videos, or collaborative posts with other users;
 - c. LIVE video sessions and archived live recordings, including sessions previously deleted or archived via TikTok's retention policies;
 - d. Story content including active Stories, archived Stories, expired Stories, and curated Story Highlights;
 - e. Audio recordings, voice notes, voice effects, and sound overlays generated or uploaded by the Target Account(s);
 - f. Overlays, stickers, text annotations, drawings, effects, face filters, GIFs, or other modifications applied to any uploaded media;
 - g. Metadata associated with all media including upload timestamps, EXIF data, device information, geolocation data, embedded file metadata, and title or caption information applied at upload.
7. **Location Data** collected, retained or possessed by TikTok Inc. for the Target Account(s):
- a. GPS coordinates, Wi-Fi proximity, Bluetooth beacons, IP-based geolocation, device-based location logs, cell site location information (CSLI), or any other geospatial data collected or retained by TikTok Inc.;
 - b. Check-ins, tagged locations, and location references embedded in media posts, captions, or live broadcasts;
 - c. Location history logs compiled via app usage or cross-platform integrations.
8. **Commercial, Financial, Shopping and Creator Monetization Activity**, including:
- a. Product listings, TikTok Shop commerce transactions, sales history, order processing, delivery/shipping data, and financial accounts linked to commerce activity;
 - b. Creator monetization and influencer partnership data, including participation in TikTok Creator Fund, LIVE gifting, virtual coins, tipping, badges, affiliate marketing, brand sponsorships, revenue earned from live stream monetization tools, brand partnerships, or promotional collaborations;
 - c. Payout logs, payment account linkage, payout methods, disbursement history, held funds, frozen balances, and monetization eligibility status.
9. **Advertising, Targeting, and Behavioral Profiling Data**, including:
- a. Advertisements displayed, clicked, engaged with, or dismissed by the Target Account(s);

- b. Behavioral interest profiles maintained by TikTok's recommendation and ad systems, including inferred interests, targeted demographics, behavioral patterns, viewing habits, ideological preferences, or flagged content tendencies;
- c. Audience segmentation assignments applied to the Target Account(s) for advertisement delivery;
- d. Sponsored content engagements and advertisements created, managed, or paid for by the Target Account(s).

10. Algorithmic Recommendation & Personalization Data, including:

- a. Algorithmic personalization signals including Explore/For You page assignments, recommended creators, content affinity scores, interaction profiles, trending interests, hashtag groupings, topics of interest, ideologically aligned content clusters, and video consumption pattern logs used to generate the individualized feed delivered to the Target Account(s).

11. Third Party Integrations & Authorized Applications, including:

- a. Complete list of third-party applications connected to the Target Account(s) via OAuth authorization;
- b. Historical records of permission grants, revocations, and access levels granted to third-party integrations;
- c. Shared data exchanged between TikTok Inc. and third-party service providers authorized by the account holder.

12. Security and Account Protection Data, including:

- a. Two-factor authentication enrollment records, recovery code generation, registered security keys, or biometric authentication tokens;
- b. Account recovery information including alternate email addresses, phone numbers, backup contacts, or trusted devices;
- c. Suspicious login alerts, location mismatch notifications, account compromise warnings, or anomalous activity flags;
- d. Password reset history, recovery attempts, and related security events.

13. Biometric Information (if available), further described as facial recognition data, facial mapping templates, or machine-learning derived biometric data generated through the user's uploaded photographs or videos.

14. Consent and Legal Agreement History, further described as all consents, user agreements, privacy policy acceptances, terms of service agreements, opt-in/opt-out logs, and related timestamped records.

NOTE: This request encompasses any content or data previously deleted, archived, modified, or otherwise concealed by the user, but still recoverable through TikTok Inc.'s internal data retention policies, backup systems, disaster recovery processes, caching servers, preservation holds, or system-generated metadata repositories.

Affidavit Language:

Based upon my training, experience, consultation with other investigators, and information obtained during this investigation, I believe the following to be true:

TikTok is a widely used global social media platform operated by TikTok Inc., which allows users to create, share, and interact with short-form video content, livestream broadcasts, private messaging, and numerous interactive features. TikTok users can maintain extensive personal profiles, communicate privately or publicly, monetize their accounts, and engage in both personal and commercial activity. The data maintained by TikTok is hosted on company-controlled servers independent of the user's physical device and remains accessible through lawful legal process, including search warrants.

TikTok accounts contain identifying subscriber information, including usernames, vanity names, profile photographs, biography text, self-reported location data, pronouns, relationship status, external website links, and cross-linked social media accounts. This profile data can assist law enforcement in confirming the identity of the person controlling the account, establishing connections to co-conspirators, victims, criminal enterprises, and financial activities.

TikTok's primary functionality centers on short-form video posting. Users upload videos ranging from a few seconds to several minutes, often enhanced with text overlays, stickers, captions, filters, effects, soundtracks, and hashtags. Users may interact with others through collaborative features such as "Duet" and "Stitch," which combine or reference multiple users' content. TikTok also provides livestream broadcasting ("LIVE") where users interact in real time with viewers, receive virtual gifts, conduct financial transactions, and earn monetization revenue. These posted videos, livestreams, and collaborative features may contain direct evidence of criminal conduct, including recorded crimes, recruitment efforts, financial transactions, contraband promotion, or post-offense boasting. TikTok maintains detailed records of this content, including deleted, archived, or modified media, drafts, and system-retained versions.

In addition to public posting, TikTok includes private communication features such as Direct Messaging and group chats. Based on my training and experience, individuals engaged in criminal conduct often utilize these private messaging services to coordinate illegal activity, discuss transactions, plan offenses, recruit associates, and conceal criminal conduct. These communications may include text messages, voice recordings, photographs, videos, embedded links, contact cards, and external chat handles. TikTok retains extensive messaging records including message content, participants, timestamps, attached media, deletion logs, and system metadata.

TikTok collects extensive behavioral and interactive data related to user activity, including:

- Likes, comments, reposts, shares, favorites, saves, and reactions to videos and livestreams;
- Duet, Stitch, and Reply Video interactions linking multiple users and collaborative activity;
- Story creation and viewer logs reflecting who viewed and engaged with temporary story posts;
- Watch time analytics, swipe behavior, replay counts, audience retention, and interaction metrics;
- Saved drafts, archived stories, deleted posts, and bookmarked or favorited content.

TikTok also includes financial tools that allow users to engage in commerce, receive payments, and monetize their content. These include TikTok Shop, Creator Fund payments, LIVE gifting, virtual coins, tipping, affiliate marketing, brand sponsorships, and promotional collaborations. Based on my training and experience, individuals involved in financial fraud, narcotics sales, money laundering, organized theft, human trafficking, or fraud schemes may leverage these tools to advertise illegal services, transfer funds, or launder proceeds. TikTok maintains extensive records related to monetization and commerce, including purchase history, payouts, linked financial accounts, disbursement logs, monetization eligibility reviews, and suspended or frozen account balances.

Criminal suspects often attempt to conceal their identity on TikTok through pseudonymous usernames, fake email addresses, burner phones, anonymized phone numbers, and the use of VPNs or anonymization services to hide their true IP address and location. TikTok retains comprehensive access logs that include IP addresses, device identifiers (IMEI, IMSI, MAC address, device IDs), browser user-agent strings, OAuth authorizations, and device fingerprints, which may link otherwise unknown accounts or devices to the same suspect.

TikTok further collects extensive location data related to user activity, including:

- Precise GPS coordinates, Wi-Fi and Bluetooth proximity, cellular location

- (CSLI), IP-based geolocation, and device telemetry;
- Location tags embedded within video captions, live broadcasts, or profile settings;
- Historical location logs compiled through app usage and device interactions.

Even if suspects attempt to delete posts, stories, livestreams, messages, or entire accounts, TikTok maintains archived versions, preservation holds, backup copies, and deletion logs, which may preserve critical evidence. Deletion logs may also indicate attempts to conceal criminal activity or obstruct law enforcement investigations.

TikTok also maintains extensive security, account protection, and enforcement data, including:

- Password reset history, recovery attempts, and account authentication logs;
- Two-factor authentication enrollment, recovery codes, registered security keys, and device authentication records;
- Suspicious login activity, geographic login mismatches, compromise flags, or anomalous behavior alerts;
- Content moderation enforcement flags for violations related to narcotics trafficking, firearms sales, sexual exploitation, child exploitation (CSAM), money laundering, and organized criminal conduct.

Based on my training and experience, individuals engaged in criminal conduct may utilize TikTok for purposes directly tied to their unlawful activity. These include:

- Promotion, advertisement, and solicitation of illegal goods or services through public video posts, hashtags, Duet/Stitch collaborations, and coded video captions;
- Recruitment of co-conspirators, victims, or vulnerable individuals through TikTok's content algorithms, suggested follower lists, interactive comments, and private messaging;
- Private coordination of criminal transactions using Direct Messages, embedded contacts, or profile-linked external messaging platforms;
- Monetization and laundering of proceeds through TikTok's financial features, creator payments, e-commerce tools, and sponsorship revenues;
- Post-offense boasting, indirect admissions, celebratory content, and visual displays of contraband, firearms, large sums of cash, or references to prior criminal activity;
- Concealment through burner accounts, pseudonyms, rapid deletions, VPNs, anonymized registrations, and cross-platform coordination with encrypted apps promoted through TikTok profiles or DMs;
- Location placement and geographic corroboration via geotagged video uploads, livestream metadata, or device telemetry.

In my training, experience, and consultation with other investigators, I know that TikTok's extensive data retention policies provide a uniquely detailed historical record of a suspect's communications, associations, activity, financial transactions, and geographic movement. Because this data is hosted directly by TikTok Inc., it remains accessible even if a suspect's physical device has been seized, wiped, reset, or placed into airplane mode. In many cases, obtaining TikTok records directly from the provider via lawful search warrant is the only method available to fully reconstruct a suspect's historical conduct and preserve critical evidence.

For all of the reasons stated above, I believe that the records maintained by TikTok Inc. related to the identified Target Account(s) will contain evidence, fruits, and instrumentalities of violations under investigation.

Additional Considerations for TikTok:

There is a common misconception that we cannot serve TikTok with US legal process because they are "in China." This is not the case: There are four "headquarters" (per se) for TikTok: One in the US (California specifically), one in London, one in Ireland, and one in Singapore. We can absolutely serve legal process to TikTok based on their United States business presence.

TikTok is **extremely** slow at data productions. As of 2024, some agencies reported waiting *up to 6 months* to receive a production and when following up with TikTok's law enforcement team, did not receive a response.

X (FORMERLY TWITTER)



Summary for Investigators:

X (formerly known as Twitter) is a large global social media platform where users post short written messages known as "posts" (formerly "tweets"), along with photos, videos, links, livestreams, and polls. Users can interact publicly by replying, reposting, quoting, liking, or following one another. Many accounts are operated under pseudonyms or handles, allowing users to conceal their true identities. The platform also features private Direct Messaging (DM) capabilities, community-based chat groups, and subscription options. In recent years, X has expanded features such as "Spaces" (live audio discussions), Communities (group forums), and "Premium" subscription content where users can monetize their content or gain additional platform privileges.

While X is used for legitimate public discourse, breaking news, political debate, and entertainment, it has increasingly been exploited for criminal activity. Offenders may use X to recruit followers, coordinate illegal activity, promote extremist ideology, advertise illegal goods or services, or stalk and harass victims. X offers limited user verification, making it easy for offenders to operate anonymously or with multiple burner accounts. However, X retains detailed user records, including IP address logs, device metadata, push tokens, linked accounts, deleted post records, and backend metadata that can assist law enforcement in identifying suspects, reconstructing communications, and establishing evidence of criminal conduct.

How to Serve with Legal Process:

X accepts legal process via their law enforcement portal, located at <https://t.co/lr> or <https://legalrequests.twitter.com>. X accepts emergency disclosure requests and preservation requests through the same law enforcement portal.

Location to be Searched:

X CORP.
Attention: Safety / Legal Process
865 FM 1209 Building 2
Bastrop, Texas 78602

Identify Accounts By:

- Username (@username)
- Profile URLs
- Target Phone Number(s)
- Target Email Addresses

Items to be Seized:

X (FORMERLY TWITTER) DATA:

To the extent that the information described is within the possession, custody, or control of X Corp., including any records, messages, posts, metadata, communications, or deleted materials still available to X Corp. or preserved pursuant to lawful process or internal retention policies, X Corp. is required to disclose the following information for the Target Account(s), for the time period of **January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), including:
 - a. Account usernames, handles (“@” names), historical username changes, display names, vanity names, retired aliases, and pseudonyms associated with the account;
 - b. Account creation date and time, including the IP address and device identifiers used at registration;
 - c. Account deletion date and time, if applicable, with associated IP and device identifiers;
 - d. Legal name (if provided), bio description text, profile fields, pronouns, location fields, website links, birthdate, and self-reported demographic information;
 - e. Email addresses associated with the account, including prior addresses, historical changes, and verification status;
 - f. Mobile phone numbers linked to the account, including addition/removal history and verification status;
 - g. Profile photographs, header images, avatars, profile videos, banners, or other media uploaded as part of profile content;
 - h. Consent logs, terms of service acceptances, privacy policy acknowledgments, and timestamped legal agreements.
2. **Device Information** related to the Target Account(s), including:
 - a. Device identification data including device IDs, IMEI, IMSI, MAC addresses, hardware fingerprints, user-agent strings, browser types, operating system versions, and app versions;
 - b. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
 - c. Logs of devices used to access the account, including session dates, times, durations, and associated device metadata;

- d. Device pairing data with other X-owned services, including mobile app integrations, Twitter Blue sessions, and hardware device registrations.
3. **IP Address Information** for the Target Account(s), to include but not limited to:
- a. Full logs of all IP addresses used to access, post, message, browse, or interact with the account;
 - b. IPv4 and IPv6 addresses with associated timestamps, session start/end times, passive telemetry, app updates, background activity, port information, and geolocation data where available.
4. **Linked Accounts and Cross-Platform Associations** to the Target Account(s), to include:
- a. Alternate X accounts registered or accessed using common email addresses, phone numbers, cookies, browser fingerprints, or device identifiers;
 - b. OAuth and third-party linked accounts (Google, Apple, Meta, or others);
 - c. Cross-platform integrations with other Musk-owned services (e.g., X Payments, Tesla services, Neuralink trials, etc., if applicable).
5. **Usage Logs, Content, and Account Activity**, including:
- a. Complete post history, including tweets, retweets, replies, reposts, quote tweets, drafts, scheduled posts, deleted tweets, and edited tweets with all associated metadata (timestamps, geotags, device IDs);
 - b. Media content uploaded, including images, videos, GIFs, voice notes, and Spaces recordings;
 - c. Direct Messages (DMs), including 1:1 messages, group chats, encrypted DMs (if applicable), attachments, links, voice messages, GIFs, contact cards, reactions, deletion history, edit history, and timestamps;
 - d. Bookmarks, saved posts, liked tweets, favorited media, pinned tweets, and saved thread history;
 - e. Search history, hashtag searches, trending topic interactions, explore feed curation, and recommendation algorithm inputs;
 - f. Spaces participation and hosting data, including audio recordings, chat logs, invitees, participants, speakers, moderators, and timestamps of participation or listening;
 - g. Circle usage history (private audience tweets), including membership lists, audience lists, recipients, and sharing parameters;
 - h. List creation, following, list membership changes, and list content;
 - i. Follower/following data, pending requests, blocked accounts, muted accounts, shadowbans, suspensions, bans, and appeals.
6. **Location Data** collected, retained or possessed by X for the Target Account(s):

- a. GPS coordinates, Wi-Fi proximity, Bluetooth beacons, IP-based geolocation, device-based location logs, cell site location information (CSLI), or any other geospatial data collected or retained by X Corp.;
- b. Check-ins, tagged locations, and location references embedded in media posts, captions, or live broadcasts;
- c. Location history logs compiled via app usage or cross-platform integrations.

7. Behavioral, Algorithmic, and Personalization Data, including:

- a. Algorithmic content affinity profiles, trending interaction logs, content suggestion clusters, interest modeling, influencer networks, and behaviorally inferred demographic targeting;
- b. Audience modeling signals used for ad targeting, feed customization, and content ranking algorithms.

8. Financial and Monetization Records, including:

- a. X Blue subscription data, including payment history, financial accounts linked, billing addresses, payment processors, refunds, credits, chargebacks, and revenue earned through monetization features;
- b. Creator monetization activity including Super Follows, Tips, Subscriptions, Sponsored Content, Ad Revenue Sharing, Payout History, Linked Financial Institutions, and Creator Payment Accounts;
- c. Financial logs associated with crypto wallets (if applicable) or integrations with X Payments features.

9. Advertising, Marketing, and Sponsored Activity, including:

- a. Advertising accounts managed by or linked to the Target Account(s), including promoted tweets, campaign history, budgets, audience segments, ad engagement metrics, payments, and financial transactions;
- b. Sponsored content interactions, clickthroughs, video ad views, impressions, conversions, and ad account management logs.

10. Security, Enforcement and Account Protection Data, including:

- a. Two-factor authentication records, trusted devices, recovery keys, device pairing, biometrics (if applicable), and security credential changes;
- b. Password reset history, recovery email/phone history, compromise reports, suspicious activity alerts, location mismatches, high-risk login flags, and fraud detection logs;
- c. Internal enforcement flags, moderation strikes, content takedown logs, legal takedown notices, terms of service violations, appeals, and administrative reviews.

11. **Biometric and Automated Moderation Data**, further described as any facial recognition, image hashing, CSAM detection hashes, violence, terrorist content detection, or machine-learning generated moderation flags maintained on submitted content.
12. **Third-Party Application Integrations**, including:
 - a. Third-party app authorizations granted via X OAuth, including scopes, permissions granted, revocation history, app IDs, API tokens, external data sharing transactions, and automated service activity;
 - b. Bot accounts operated, scheduled posting clients, scraping tools, API usage history, automation services, mass engagement bots, or amplification tools interacting with the Target Account(s).
13. **Consent and Legal Agreement History**, further described as all records of terms of service acceptance, privacy policy agreements, consent history, opt-in/opt-out records for data sharing, advertising personalization, content visibility settings, and timestamped legal acknowledgments.

NOTE: This request includes any and all information, content, metadata, system logs, and communications that may have been deleted, hidden, archived, modified, or subject to retention holds, but which remain recoverable through internal X Corp. data retention systems, disaster recovery processes, backup storage, preservation holds, caching servers, or internal data integrity systems.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

X (formerly Twitter) is a widely used global social media and microblogging platform operated by X Corp.. X allows users to publicly share short text-based messages known as “posts” (formerly called “tweets”), as well as photographs, videos, polls, live broadcasts, and external links. In addition to public posting, X provides numerous private communication, financial, and content monetization features. The data maintained by X is hosted on servers owned and controlled by X Corp., independent of any user’s personal device. Information retained by X remains accessible to law enforcement through lawful legal process such as court orders and search warrants, even if users attempt to delete content, deactivate accounts, or wipe devices.

Users create X accounts by providing an email address or mobile phone number, though many accounts are operated pseudonymously under aliases or screen names not immediately tied to the user’s real identity. Account profiles may include profile photographs, banners, biographies, pronouns, location fields, website links, verified status

badges, and linked external accounts (such as Google or Apple login credentials). These self-reported profile fields may assist law enforcement in identifying and linking the individual(s) who control a given X account and establishing connections to suspects, co-conspirators, or victims.

X enables users to share a variety of multimedia content, including text posts, photo galleries, short-form video clips, long-form video uploads, and real-time livestreams. Users can interact with posts through likes, reposts (retweets), quote posts, comments, bookmarks, and shares to external platforms. X also supports premium subscription content (“X Premium”) which may allow creators to monetize content through paid subscriber-only posts, exclusive content, and financial transactions. Criminal actors may use these features to promote illegal goods or services, launder illicit proceeds, or engage in fraud schemes using the platform’s commerce capabilities.

In addition to public posting, X allows users to communicate privately via **Direct Messages (DMs)** and encrypted direct messaging features (for accounts that have activated end-to-end encryption). Through my training and experience, I know that Direct Messaging features are frequently exploited by individuals engaged in criminal conduct to coordinate illegal activity, solicit contraband sales, communicate with co-conspirators, plan criminal events, or contact victims in a private setting shielded from public visibility. These private communications may contain text, photographs, videos, emojis, GIFs, external links, location pins, media attachments, and embedded contact information. X maintains detailed server-side logs of these communications, including message content, timestamps, sender/recipient information, deletion logs, encryption status, and metadata.

Beyond messaging, X collects extensive interaction data that may assist law enforcement in documenting criminal conduct, such as:

- Likes, reposts, quote posts, bookmarks, and comments that reflect interests, affiliations, or associations with illegal conduct.
- Poll creation and voting history, including polls related to illicit activity.
- Lists of followers, following, and blocked or muted users which may reveal associations between subjects, co-conspirators, or victims.
- Spaces (audio chat rooms) including session logs, participant lists, live discussion content, and recordings where applicable.
- Community membership records reflecting private group discussions and niche interest circles potentially tied to criminal conspiracies.

In addition to user activity, X retains detailed technical metadata, including:

- IP address logs showing where and when accounts are accessed;
- Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware identifiers, and user-agent strings;
- OAuth authorizations and linked third-party applications connected to external services;

- Push Notification Tokens assigned to specific mobile app installations that may associate multiple accounts to the same physical device;
- Geolocation metadata derived from posted content, device signals, IP-based location inference, and user-submitted location fields;
- Payment records tied to X Premium, subscriptions, monetization payouts, advertisements, and Super Follow or tipping features.

Through my training, experience, and consultation with other investigators, I know that individuals engaged in criminal activity regularly exploit X for a wide range of criminal purposes, including but not limited to:

- **Promotion and advertisement of illegal goods or services**, such as narcotics trafficking, firearms sales, financial fraud schemes, and trafficking in stolen data or personally identifiable information.
- **Coordinating criminal activity** via private messaging, encrypted direct communications, live audio Spaces, or community groups.
- **Financial fraud and laundering**, using monetization features to obscure sources of income, route payments through multiple accounts, or facilitate illegal commerce.
- **Online harassment, exploitation, or intimidation**, targeting victims through threats, doxxing, stalking, or coordinated harassment campaigns.
- **Recruitment into criminal enterprises**, extremist groups, or violent organizations via open or covert content sharing.
- **Post-offense boasting or documentation**, such as posting incriminating photos, videos, or commentary following illegal acts.

Criminal actors often exploit the anonymity X affords by operating multiple pseudonymous accounts, utilizing burner phones, VPNs, anonymization services, and falsified profile information. However, X retains comprehensive backend records including subscriber registration details, linked accounts, device metadata, IP address logs, push notification tokens, financial transaction histories, OAuth integrations, content deletions, and moderation enforcement actions. Even where users delete posts, deactivate accounts, or attempt to obscure identity, these server-side records often remain recoverable to X through lawful legal process.

In my experience, the data maintained by X Corp. provides a critical resource for law enforcement to reconstruct communications, identify criminal networks, recover deleted evidence, corroborate witness statements, and link pseudonymous social media accounts to identified suspects. Because X stores its records on company-controlled servers, this data remains available to law enforcement even if the suspect's physical device has been seized, reset, or wiped. In many instances, search warrants directed to X Corp. represent the only viable means to obtain these records and advance criminal investigations.

For all the reasons outlined above, I believe the requested records maintained by X Corp. related to the identified account(s) will contain evidence, fruits, and instrumentalities of the offenses under investigation.

Additional Considerations for X (Twitter):

X was formerly known as Twitter, but the entire law enforcement is still branded as Twitter (as are some other various parts of the website). This **is** the most current information as of 2025.

X retains some logs only briefly (such as IP addresses). Although the exact time back they retain it is not known, consider the importance of issuing preservation letters if that will be particularly relevant to your investigation.

Any content deleted by users is generally *not available* once it's been deleted.

X does host photographs / videos / Periscope content, but it is oftentimes only hosted *temporarily* and may not always be available. Many X users will host content elsewhere and share it on X, in which case, that multimedia cannot be provided by X.



Summary for Investigators:

Reddit is a large online social media platform built around thousands of user-created discussion communities known as "subreddits." Each subreddit focuses on a specific topic or interest, ranging from news, hobbies, entertainment, or gaming, to highly specialized topics like cryptocurrency, firearms, or niche political ideologies. Users create pseudonymous accounts (no real name required) and can post text, photos, videos, links, or conduct polls. Other users can comment, upvote, or downvote posts, creating community-driven ranking systems where the most popular content rises to the top. Many subreddits are public and searchable, but some are private, invite-only, or moderated with restricted access.

While Reddit is widely used for legitimate conversation and hobbyist communities, offenders often exploit its loose oversight and anonymity for criminal activity. Subreddits have been used for illegal firearms manufacturing discussions, fraud schemes, drug sales, child exploitation, extremist recruitment, and distribution of prohibited content. Direct messaging features allow private conversations between users, and external links may point to off-platform sites where further illegal activity takes place. Despite its reputation as a "discussion forum," Reddit collects significant account, IP, device, and content metadata that can be critical in identifying suspects and building criminal cases.

How to Serve with Legal Process:

Reddit accepts legal process electronically through their law enforcement portal:
<https://legalrequests.reddithelp.com/hc/en-us/requests/new>

Reddit also accepts preservation requests and emergency disclosure requests through the above listed portal.

Location to be Searched:

REDDIT, INC.
C/O Corporation Service Company
2710 Gateway Oaks Drive, Suite 150N
Sacramento, CA 95833

Identify Accounts By:

Reddit accounts can be identified in our legal process by:

- Username (**Easy to identify, should look like u/username**)
- Target Email Address(es)
- Target Phone Number(s)

Items to be Seized:

REDDIT DATA:

To the extent that the information described is within the possession, custody, or control of Reddit, Inc., including any records, files, messages, content, logs, metadata, or deleted materials still available to Reddit, Inc., or preserved pursuant to legal process or internal retention, Reddit, Inc. is required to disclose the following information for the Target Account(s), for the time period of **January 1, 2025 to the date this search warrant is signed**:

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Account usernames, historical usernames, aliases, vanity names, display names, retired handles, alternate spellings, and pseudonyms associated with the Target Account(s);
 - b. Account creation date and time, including associated IP addresses and device identifiers at registration;
 - c. Account deletion date and time, including any linked IP addresses or device identifiers;
 - d. Legal name (if provided), self-reported biographical information, user-submitted pronouns, profile bio text, location fields (hometown, city, country), gender identity, birthdate, and contact information;
 - e. Email addresses associated with the account, including historical changes, prior addresses, and verification status;
 - f. Mobile phone numbers linked to the account, including history of additions, removals, or verifications;
 - g. Profile avatars, photographs, images, or other digital likenesses uploaded as profile content;
 - h. Consent logs, user agreement acceptances, terms of service acknowledgments, privacy policy consents, community guidelines agreements, and timestamped consent history.

2. **Device Information** related to the Target Account(s), including:
 - a. Device identification data including device fingerprints, IMEI, IMSI, MAC addresses, browser types, user-agent strings, device models, platform versions, operating systems, and application version numbers;
 - b. Logs of devices used to access the Target Account(s), including dates, times, session durations, device IDs, and location of logins;
 - c. OAuth integrations, third-party login devices, or external platforms linked via device fingerprinting or hardware signature data.
3. **IP Address Information** for the Target Account(s), to include but not limited to:
 - a. Complete logs of all IP addresses used to register, access, post, message, browse, or otherwise utilize the Target Account(s);
 - b. IPv4 and IPv6 addresses with corresponding timestamps, ports (if available), session start/end times, passive telemetry, app updates, background sessions, and other server-side activity reflecting interaction with Reddit's services.
4. **Linked Accounts & Cross Account Associations** to the Target Account(s), to include:
 - a. Alternate Reddit accounts registered using the same email addresses, phone numbers, device fingerprints, browser identifiers, or shared cookie/session IDs;
 - b. Linked OAuth accounts connected via Google, Apple, Facebook, or other external identity providers;
 - c. Device-based association logs reflecting alternate pseudonymous Reddit accounts likely controlled by the same user or accessed from the same hardware.
5. **Usage Logs, Account Activity and Content** for the Target Account(s), including:
 - a. Full posting history, including original submissions, titles, text posts, media attachments (images, videos, audio), polls, crossposts, awards granted or received, and all metadata including timestamps, geotags, and device identifiers associated with uploaded content;
 - b. Complete comment history, including replies, nested thread participation, upvotes/downvotes received, award information, edit history, deletion logs, timestamps, and content metadata;
 - c. Karma statistics, including total post karma, comment karma, and cumulative karma scoring breakdowns;

- d. Subreddit membership records, including public and private subreddit subscriptions, join dates, invitations sent or received, approvals for restricted communities, removals, and bans issued by moderators or administrators;
- e. Private subreddit participation logs, including subreddit-specific user roles, moderator positions held, invitations issued, membership changes, and moderator action logs;
- f. Direct Messaging content, including private messages, chat messages, group chats, chat room participation, attachments, media files, shared contact cards, emojis, stickers, links, voice notes, and timestamps of all messages sent or received;
- g. Saved content, including bookmarks, favorited posts, saved threads, saved comments, drafts, or archived materials;
- h. Browsing history within Reddit, including subreddit visit history, profile views, saved searches, multireddit creation or curation, trending page interactions, explore content, search queries, hashtags used, trending topic interactions, and explore feed click behavior;
- i. Reports submitted to Reddit for abusive content or moderation reports initiated by the Target Account(s), including reported content IDs, timestamps, rationale provided, and administrative outcomes.
- j. User profile flair, user badges, subreddit-assigned roles, subreddit-specific user titles or honors, and any affiliated visual indicators assigned to the Target Account(s);
- k. Poll voting history for polls participated in by the Target Account(s), including selected poll options, timestamps, and poll metadata;
- l. Subreddit public chat room participation logs, chat room transcripts, chat membership lists, message content, moderation actions within chat rooms, and related metadata;
- m. Internal moderation discussions (modmail threads) including appeals, administrative guidance, investigation threads, and content moderation decisions involving the Target Account(s).

6. **Moderation Logs** for any Subreddits where the Target Account(s) held moderation or administrative privileges, to include:

- a. Full moderation logs reflecting bans issued, users invited, content removals, flair assignments, automoderator rule usage, subreddit rule enforcement, modmail communications, appeal decisions, internal enforcement warnings, administrative interventions, and historical moderator role assignments;

- b. Internal communications between the Target Account(s) and Reddit's Trust & Safety, Admin, or Abuse teams related to appeals, investigations, sanctions, or enforcement actions.

7. Shadowban, Suspension, and Deleted Account Data, including:

- a. Shadowban history applied to the Target Account(s), including flags for suspicious behavior, rule violations, or automated platform sanctions;
- b. Suspension records, content quarantines, moderation escalations, and administrator actions against the Target Account(s);
- c. Deleted user logs retaining orphaned content formerly tied to deleted or suspended accounts, internal account ID references preserved by Reddit following account deletions, and any orphaned content audit trails tied to prior identifiers.

8. Financial, Commercial, and Monetization Data, including:

- a. Reddit Premium membership data, including subscription history, purchase dates, payment methods, and billing records;
- b. Reddit Coins purchases, gift awards, transactions made, coins granted, redeemed, or sent to other users, and coin balances;
- c. Reddit Advertising or promoted content management records including advertising campaign history, targeted demographics, payments, billing addresses, campaign performance metrics, and payment account linkage.

9. Behavioral, Algorithmic, and Personalization Data, including:

- a. Behavioral interest profiles and recommendation data, including subreddit recommendations, trending post interactions, user content affinity scores, community suggestions, content engagement patterns, and machine-learning generated interest clusters;
- b. Audience modeling data reflecting subreddit grouping, trending topic alignment, content ranking signals, and personal algorithmic feed customization.

10. Third Party Application Integrations, including:

- a. Third-party identity providers used during account registration or login (Google, Apple, Facebook, etc.);
- b. List of third-party applications authorized via Reddit OAuth, including timestamps of authorization, permissions granted, scopes, revocation dates, and external data sharing transactions;

- c. Records of automated tools, bots, scraping services, mass posting clients, scheduling software, or external third-party services interacting with the Target Account(s) via API.

11. Security and Account Protection Data, including:

- a. Password change history, password reset logs, recovery attempts, and recovery credentials used;
- b. Two-factor authentication enrollment, trusted device registrations, biometric access credentials (if applicable);
- c. Suspicious login alerts, unauthorized access flags, location mismatch notifications, IP-based anomaly warnings, account compromise reports, or high-risk event flags.

12. Biometric Information (if available), including:

- a. Any biometric identifiers retained or utilized by Reddit related to facial recognition, image hashing, AI content moderation, CSAM detection, or automated illegal content scanning algorithms.

13. Consent, Legal Agreements, and Policy Acknowledgments:, including:

- a. Full record of all user consents, terms of service acceptances, privacy policy agreements, community guideline acceptances, and any opt-in or opt-out selections made by the Target Account(s), including timestamps of consent.

NOTE: This request includes any content, metadata, communications, or account activity that may have been deleted, archived, hidden, or modified but remains recoverable to Reddit, Inc. through internal data retention policies, disaster recovery systems, server-side backups, preservation holds, caching layers, or system-generated metadata repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Reddit is a widely used social media platform operated by Reddit, Inc., headquartered in San Francisco, California. Reddit functions primarily as a collection of user-created communities, known as “subreddits,” where users gather to post content, engage in discussion threads, exchange media, and interact with others around specific topics of interest. Reddit incorporates both public and private community features, extensive

messaging capabilities, moderator-controlled forums, and sophisticated content recommendation systems that build extensive behavioral profiles on its users. Reddit's data is hosted on servers owned and controlled by Reddit, Inc., independent of the user's physical device, and remains accessible to Reddit through lawful legal process, such as search warrants or court orders, even if users attempt to delete or conceal content.

Users create Reddit accounts by providing email addresses and, in some cases, verified phone numbers. Reddit allows users to operate under pseudonyms, usernames, or aliases rather than legal names, and users frequently maintain multiple accounts for different purposes. Account profiles may include avatars, profile photos, biography text, location fields, personal pronouns, gender identity, and linked third-party platforms. Reddit also assigns each account a persistent internal User ID that remains constant even if the username changes. In my experience, this profile and account metadata can assist law enforcement in identifying and linking otherwise anonymous Reddit accounts to known individuals.

Reddit users participate across thousands of public and private subreddits where they can submit original posts, comment on threads, vote on content, assign awards, engage in polls, crosspost to multiple communities, and curate saved content. Posts and comments may include text, images, videos, external links, polls, and attachments. Certain subreddits may restrict membership, require moderator approval, or function as private invite-only communities. Reddit retains detailed logs reflecting this activity, including timestamps, device identifiers, content metadata, awards granted or received, upvotes, downvotes, deletion history, edit logs, moderation actions, and nested conversation threads. This content may provide direct evidence of criminal conduct, establish timelines, corroborate events, and reveal associations between the suspect and co-conspirators.

In addition to public posting, Reddit offers private messaging features, including direct messages, private chats, chat rooms, and multi-user group chats. Through my training and experience, I know that these private communications are often exploited by individuals engaged in criminal activity to conduct conversations related to illegal transactions, grooming behavior, recruitment, financial fraud, or coordination with co-conspirators. These messages may contain text, media attachments, voice notes, emojis, stickers, contact cards, and links to external file storage or communication platforms. Reddit retains extensive records of these private messages, including message content, timestamps, media metadata, device identifiers, deletion logs, and chat room participation records.

Reddit maintains extensive technical, behavioral, financial, and administrative metadata relevant to criminal investigations, including:

- IP address logs associated with account creation, logins, logouts, post submissions, browsing activity, and session connections (including IPv4 and IPv6 formats, ports, and session telemetry);

- Device metadata including browser user-agent strings, operating system versions, application versions, device fingerprints, hardware identifiers, and OAuth integration records;
- Behavioral data including subreddit subscriptions, community engagement, search history, viewed profiles, trending topic interactions, and algorithmically inferred interests;
- Financial transactions related to Reddit Premium subscriptions, Reddit Coins purchases, advertising campaigns, billing addresses, payment methods, and monetization tools;
- Administrative moderation logs reflecting subreddit membership changes, bans, content removals, moderator assignments, appeals, moderator communications (modmail), and rule enforcement actions;
- Reports submitted for abusive content, flagging of illegal material, moderation escalations, enforcement actions by Reddit administrators, and trust & safety intervention logs.

Through my training and experience, I am aware that Reddit is frequently utilized by individuals involved in criminal conduct for a variety of offenses, including but not limited to:

- Child exploitation offenders who use Reddit to locate, groom, and exploit minors through private messages, chat rooms, or invite-only subreddits dedicated to illicit material or grooming behaviors;
- Narcotics traffickers and firearms dealers who promote contraband sales through coded posts, memes, private subreddits, or anonymous message exchanges;
- Organized theft rings, financial fraud actors, and cybercriminals who exchange stolen data, fraud schemes, compromised credentials, hacking tools, or conduct recruitment within closed subreddits or encrypted chat services linked to Reddit;
- Extremist organizations and violent actors who use Reddit to radicalize recruits, promote ideology, distribute propaganda, coordinate group activity, or share operational planning materials.

Criminal actors often exploit Reddit's pseudonymity, burner accounts, VPN usage, encrypted external services, multi-account switching, and private community structures to conceal their identity and activities. However, Reddit's backend systems maintain extensive device logs, content metadata, account linkage data, and behavioral telemetry that may directly associate a suspect to illicit conduct, despite these concealment efforts.

Even when users delete content, Reddit's systems may preserve full or partial records through internal retention policies, preservation holds, archival backups, system logs, orphaned content records tied to deleted accounts, cached storage, and disaster recovery systems. Deletion logs may also reflect attempts to obstruct justice or hide criminal activity.

In my experience, records maintained by Reddit, Inc. serve as a critical investigative resource for reconstructing historical communications, identifying co-conspirators, recovering deleted or hidden evidence, analyzing behavioral patterns, and establishing links between suspects and criminal offenses. Because Reddit stores this data on its own servers independent of a suspect's devices, lawful search warrants served directly to Reddit may be the only means of obtaining this information for evidentiary purposes.

For all of the reasons set forth above, I believe the requested records maintained by Reddit, Inc. related to the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for Reddit:

Reddit is pretty *simple* to use at face value, and a lot of it is accessible via “open source” or undercover accounts. For example, if you look up a user's profile on Reddit, you can publicly see: Communities they are active in, their past posts in any subreddit (except private ones) and comments they've made on posts. Users can **not** make their profiles private or hide this information. However, it won't reveal posts in *private subreddits* which tends to be where criminal activity occurs.

Regarding IP addresses, Reddit only retains them for **100 days** before they are automatically purged.

When a Reddit user deletes their account, it is instantly deleted (there is no “30 day window” like many other platforms). Deleted accounts cannot be re-activated. Reddit acknowledges that even when a user account is deleted, some information is retained.

Summary for Investigators:

Kik is a mobile messaging application owned by MediaLab.ai, Inc., widely used for real-time text messaging, image and video sharing, group chats, voice messages, and live video communication. Unlike many other messaging apps, Kik does not require users to register with a verified phone number — instead, accounts are typically tied to a username, email address, and optional display name. This low barrier to entry makes Kik especially attractive to users who wish to remain anonymous or use multiple pseudonymous accounts. Kik supports both private one-on-one messaging and large public or private group chats organized around common interests. Users can easily share photos, videos, external links, and attachments directly within chats, as well as initiate live video calls within conversations.

Because of its anonymity and youth-oriented user base, **Kik has become a frequent platform for criminal exploitation, particularly in child sexual exploitation, sextortion, human trafficking, and distribution of CSAM (Child Sexual Abuse Material).** Offenders may approach minors in public groups before moving conversations into private chats where grooming and exploitation occur. Kik maintains certain server-side data available to law enforcement under legal process, which may include account registration details, IP address logs, device information (including push tokens), group memberships, chat content, attachments, timestamps, and metadata. This data can assist investigators in identifying suspects, locating victims, documenting the scope of exploitation, and reconstructing communications even when suspects attempt to delete conversations.

How to Serve with Legal Process:

Kik accepts legal process electronically through their law enforcement portal:
<https://medialablawenforcementhelp.zendesk.com/hc/en-us/requests/new>

Kik also accepts preservation requests and emergency disclosure requests through the above listed portal.

Location to be Searched:

MediaLab
Attention: Legal
1222 6th Street
Santa Monica, CA 90401

Identify Accounts By:

Kik accounts can be identified in our legal process by:

- Username
- Target Email Address(es)

Items to be Seized:

KIK MESSENGER DATA:

To the extent that the information described is within the possession, custody, or control of MediaLab.ai Inc. (operator of Kik Messenger), including any records, files, messages, logs, metadata, or deleted content still available to MediaLab.ai Inc., or preserved through legal process, **MediaLab.ai Inc. is required to disclose the following information for the Target Account(s), for the period of January 1, 2025 to the present:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account usernames, display names, historical username changes, screen names, vanity names, aliases, and retired handles associated with the Target Account(s);
 - b. Kik User ID (internal unique account identifier assigned by Kik);
 - c. Account registration date and time, including IP address and device information at time of registration;
 - d. Email addresses linked to the account, including verification status, historical addresses, and prior changes;
 - e. Mobile phone numbers linked to the account, including verification status, historical changes, and prior numbers;
 - f. Profile photographs, avatars, Bitmojis, or custom graphics used as profile images;
 - g. Profile biography text, status messages, website links, or self-reported information entered into the user profile;
 - h. Linked external accounts or integrations authorized via Kik Messenger;
 - i. User's birthdate (if provided);
 - j. User's location information (if available).
2. **Device Information** related to the Target Account(s), including:
 - a. Device identifiers including device fingerprints, IMEI, IMSI, MAC addresses, hardware IDs, browser user-agent strings, device models, operating system versions, and application version numbers;

- b. Push Notification Tokens (Push Tokens) assigned to devices used to access the account, including any Apple Push Notification Service (APNS) tokens, Google Firebase Cloud Messaging (FCM) tokens, or other device-specific push identifiers;
 - c. Device connection history reflecting logins, session activity, and devices used to access Kik Messenger services.
- 3. **IP Address Information** for the Target Account(s), to include but not limited to:
 - a. Complete logs of all IP addresses used to register, log in, or access the Target Account(s), including passive telemetry and background session data;
 - b. IPv4 and IPv6 addresses with corresponding timestamps, port numbers (if available), and session duration records.
- 4. **Linked Accounts & Cross-Account Associations** to the Target Account(s), to include:
 - a. Alternate Kik accounts registered using shared email addresses, phone numbers, device fingerprints, browser identifiers, or linked session cookies;
 - b. Device-based association logs reflecting additional pseudonymous Kik accounts accessed from the same hardware.
- 5. **Account Activity & Logs** for the Target Account(s), including the following:
 - a. Friend/contact lists showing friends added, blocked users, pending requests, and removals;
 - b. Login activity, failed login attempts, password resets, and recovery logs;
 - c. Account suspension records, abuse reports filed by or against the account, flagged content, moderation actions, and administrative account interventions;
 - d. Search history, contact discovery logs, group discovery activity, and invitation records;
 - e. Notifications, alerts, or in-app system messages transmitted to or from the account.
- 6. **Messaging & Content Records** for the Target Account(s), including:
 - a. Full direct message and group chat content (text, emojis, attachments, stickers, voice notes, GIFs, or multimedia files), for any content still stored or preserved by Kik;

- b. Group chat membership records, including group names, creation dates, invite codes, group administrator roles, participants lists, and timestamps of user joins/leaves;
- c. Media attachments, including photos, videos, audio files, and associated metadata (timestamps, device data, geolocation where applicable).

7. Payment or Commercial Transaction Data (if applicable), including:

- a. Payment records for in-app purchases, premium features, promoted chats, or any financial activity linked to the account, including transaction histories and linked payment processors.

8. Security and Account Protection Data, including:

- a. Two-factor authentication enrollment (if enabled), trusted device logs, security tokens, and backup/recovery credentials;
- b. Password change history, reset attempts, and account recovery event logs;
- c. Login anomaly alerts, location mismatch flags, unauthorized access warnings, and compromise reports.

9. Deleted, Archived, and Preserved Content, including any deleted, archived, expired, or preserved messages, content, or metadata that remain recoverable via MediaLab.ai Inc.'s internal data retention systems, server backups, caching infrastructure, legal holds, or disaster recovery repositories.

NOTE: This request specifically includes any content, metadata, and communications that may have been deleted, archived, modified, or hidden but remains accessible through Kik's internal storage, caching, disaster recovery, or backup systems.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Kik Messenger is a mobile-based messaging platform operated by MediaLab.ai Inc. Kik is widely used by individuals seeking to communicate via text messaging, media sharing, group chats, and other interactive features. Kik allows users to create pseudonymous accounts that are not directly tied to legal names, allowing individuals to operate under screen names, aliases, or self-created usernames. Kik accounts are primarily associated with mobile phone devices, although registration typically requires only an email address, username, and date of birth. Many Kik users intentionally avoid providing true identifying

information, which can make attribution of accounts to real-world individuals difficult without legal process. The data maintained by Kik is hosted on company-controlled servers and remains accessible to MediaLab.ai Inc. via lawful process such as search warrants and court orders.

Kik accounts may include self-reported subscriber information such as usernames, email addresses, date of birth, profile pictures, avatar images, bios, display names, and linked device information. Each account is assigned a unique User ID internally tracked by Kik's servers. Users often change screen names frequently, and may operate multiple Kik accounts using separate email addresses or mobile devices. These accounts are often linked to specific mobile devices through push notification tokens, device identifiers, IP addresses, and app version telemetry, which may provide law enforcement with evidence to attribute devices to specific accounts.

Kik supports both private one-on-one messaging and group chats, which may include text-based conversations, photo sharing, video clips, stickers, emojis, GIFs, audio messages, and external hyperlinks. Based on my training and experience, these private communications are frequently utilized by individuals involved in criminal activity to facilitate illegal conduct. Kik maintains extensive records related to these communications, including message metadata, timestamps, sender/recipient identifiers, IP logs, device data, and, in some cases, content that has not yet been deleted by either party at the time of preservation or production.

In addition to text and media messages, Kik allows users to create group chats that serve as ongoing chat rooms involving multiple participants. Group chats may persist for extended periods of time, allowing suspects to engage in long-term conversations with co-conspirators, distribute illicit materials, advertise criminal services, or recruit additional individuals for criminal activity. Kik may retain records of group membership history, participant identifiers, join/leave logs, and moderation activities conducted by group administrators.

Kik retains extensive device, network, and security metadata related to user accounts that can aid in criminal investigations. This includes IP address logs for all logins, device identifiers such as IMEI and MAC addresses, push notification tokens assigned to specific devices, app version data, login sessions, geographic information inferred from IP geolocation, and device platform details. Even when individuals attempt to conceal their identity by using burner emails, VPNs, or multiple accounts, Kik's server-side data may allow investigators to identify patterns of account usage that tie multiple accounts to the same physical device or user.

Based upon my training, experience, and consultation with other investigators, I am aware that Kik Messenger has been widely utilized by individuals engaged in serious criminal conduct, including but not limited to:

- Child exploitation offenses, including grooming, solicitation of minors,

production and distribution of CSAM (Child Sexual Abuse Material), and trafficking of explicit imagery;

- Narcotics trafficking networks coordinating sales, advertising drug availability, negotiating pricing, and arranging delivery or pickup locations through private chat messages or group chats;
- Financial fraud schemes utilizing Kik to recruit accomplices, launder money, coordinate identity theft rings, or distribute stolen financial credentials;
- Recruitment efforts by organized criminal enterprises or violent organizations using Kik's group chat features to organize, recruit, and coordinate illegal activity.

Because Kik allows rapid message deletion, account switching, and anonymous use, suspects may delete or modify content prior to law enforcement contact. However, MediaLab.ai Inc. retains server-side metadata, account identifiers, device linkage data, IP address logs, message metadata, and sometimes content that has not yet expired or been deleted. Deleted content may still be recoverable through preservation requests, server-side retention policies, caching, and disaster recovery backups.

In my experience, records maintained by MediaLab.ai Inc. may provide essential evidence that documents suspect communications, establishes criminal associations, links devices to accounts, identifies co-conspirators, corroborates victim statements, and reconstructs events critical to this investigation. Because this data exists independently of any seized device, legal process directed to MediaLab.ai Inc. is often the only means to recover this evidence and advance the investigation.

For these reasons, I believe that the requested records maintained by MediaLab.ai Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for Kik Messenger:

Kik Messenger has a law enforcement specific FAQ section of their website that has some useful information: <https://medialablawenforcementhelp.zendesk.com/hc/en-us/sections/4404983297819-Kik-FAQ>

KIK Messenger is really heavily used by young kids and teenagers, so it is unfortunately highly favored by child predators. Also, CSAM material is often exchanged on Kik (they had over 114,000 CyberTip reports in 2024).

Particularly with Kik Messenger, we strongly recommend a preservation request. When an account is banned or deleted, data is *wiped* immediately. This results, unfortunately, in a lot of potential lost evidence.



Summary for Investigators:

Discord is an online platform originally built for gamers to communicate while playing video games, but it has grown into a massive multi-purpose chat service used by people for all kinds of communities and interests. Users can join or create private or public “servers,” which function like group chat rooms. Inside each server are channels that can be text-based (for chatting, posting images, links, or files) or voice-based (for live audio conversations or video chats). Many gaming groups use Discord to talk to each other while playing, organize teams, share game strategies, or just socialize outside of the game itself.

Beyond gaming, Discord is widely used by hobby groups, clubs, influencers, study groups, businesses, and even some criminal actors because of its private nature. Many servers are invite-only, with customizable privacy settings, moderation tools, and even bots that automate tasks or restrict access. Unlike more public social media platforms, Discord often feels like a closed community where users can control who sees what, making it attractive for both legitimate communities and people attempting to avoid detection.

How to Serve with Legal Process:

Discord accepts legal process electronically through the **Kodex** provider portal:
<https://app.kodexglobal.com/discord/signin>

Discord also accepts preservation requests, emergency disclosure requests, content reports, account takedown requests, and questions through the above listed portal.

Location to be Searched:

DISCORD, INC.
444 De Haro St, Suite 200
San Francisco, CA 94107

Identify Accounts By:

Refer to the following Discord webpage on how to identify User ID(s), Server ID(s), Message ID(s) and Channel ID(s) while using Discord: <https://support.discord.com/hc/en-us/articles/206346498-Where-can-I-find-my-User-Server-Message-ID>

Items to be Seized:

DISCORD DATA:

To the extent that the information described is within the possession, custody, or control of Discord, Inc., including any messages, records, files, logs, or information that have been deleted but are still available to Discord, Inc., or have been preserved pursuant to a request, Discord, Inc. is required to disclose the following information for the Target Account(s). All of the following records, ranging from the time period of **January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Full legal name, screen name, user ID number (UID), Discord tag, username, and all username change history, including prior aliases, vanity names, retired handles, and alternate spellings associated with the account;
 - b. Date of birth and any age verification processes applied to the account;
 - c. Email addresses associated with the account, including all changes, updates, or deletions over time;
 - d. Mobile phone numbers linked to the account, including historical changes, deletions, and recovery contacts;
 - e. Profile photographs, avatars, digital likenesses, banners, and any “About Me” profile text fields;
 - f. Linked external accounts, including any connected via OAuth, Google, Apple ID, Xbox Live, PlayStation Network, Steam, Epic Games, Spotify, Twitch, or other authorized third-party platforms;
 - g. Linked payment methods, financial accounts, subscription history, Discord Nitro purchases, Nitro Boost activity (including server boosts and transfer logs), billing addresses, and transaction history related to subscriptions, upgrades, or digital purchases;
 - h. Participation records in Discord's Hypesquad program or other Discord community affiliation programs;
 - i. Consent acknowledgments, terms of service acceptances, privacy policy consents, community guidelines agreements, safety notices, and opt-in/opt-out logs with timestamps.
2. **Device Information** related to the Target Account(s), including:
 - a. Device identification records, including but not limited to: IMEI, IMSI, MAC addresses, device IDs, hardware fingerprints, serial numbers, and system configuration identifiers;

- b. Complete device access logs showing all devices used to access the account, including platform type (mobile, desktop, web), client version, browser user-agent strings, OS versions, device manufacturer, model, and firmware versions;
 - c. Session activity logs reflecting all login attempts, successful logins, logouts, session durations, and cross-device sync activity.
- 3. **IP Address Information** for the Target Account(s), to include but not limited to:
 - a. Full logs of all IPv4 and IPv6 addresses used to register, access, modify, or interact with the account, including IP addresses tied to message transmission, voice calls, video streams, content uploads, background app telemetry, and push notification activity;
 - b. Port numbers associated with IP address logs, where available.
- 4. **Linked Accounts & Cross Account Associations** to the Target Account(s), to include:
 - a. Alternate Discord accounts managed or operated by the same user/device via shared phone numbers, email addresses, IP addresses, device fingerprints, browser sessions, cookies, OAuth tokens, or hardware identifiers;
 - b. Any detected linked Discord accounts flagged internally for policy circumvention, grooming behavior, multi-account evasion, or ban evasion risk signals;
 - c. Accounts linked via Discord's Account Linking Services or Meta Account Center integrations (if applicable).
- 5. **Server Participation and Group Memberships**, including:
 - a. Complete records of all servers created, joined, owned, administered, or moderated by the Target Account(s), including server IDs, names, creation dates, ownership transfers, and deletion history;
 - b. Server channel structures, including voice channels, text channels, private channels, locked channels, and invite-only groups;
 - c. Full server audit logs including role assignments, permission modifications, administrative actions, bans, mutes, kicks, join/leave events, and moderation history related to the Target Account(s);
 - d. Server invite links created or used by the Target Account(s), including invite metadata, invite usage logs, expiration dates, invite tracking codes, and invite sharing activity;

- e. Friends list, blocked users, pending friend requests, ignored friend requests, server membership lists, and mutual server associations.
- 6. Message Content and Communication Logs, including:**
- a. Direct Messages (DMs), private group chats, and all message threads involving the Target Account(s), including message content, attached media, timestamps, message IDs, sender/recipient IDs, channel IDs, reactions, and pinned messages;
 - b. All message edits, deletions, or recalled message versions, including deletion timestamps and message modification logs;
 - c. File attachments shared via messages, including photographs, videos, GIFs, documents, audio files, and embedded links;
 - d. Metadata related to shared voice notes, audio messages, contact cards, calendar invites, or embedded third-party content sent via Discord messaging platforms.
- 7. Voice, Video, Streaming & VOIP Session Logs, including:**
- a. Voice call logs, group calls, audio room sessions, and multi-user conference sessions, including participant lists, call durations, connection timestamps, and session metadata;
 - b. Video call sessions, screen-sharing activity, streaming sessions (Go Live), broadcast metadata, participants, viewer counts, connection durations, and timestamps;
 - c. Audio stream capture logs associated with high-risk flagged sessions if preserved by Discord for Trust & Safety enforcement purposes.
- 8. Deleted, Archived, or Preserved Content, including:**
- a. Recently deleted messages, files, and media preserved under Discord's internal backup systems, preservation holds, audit logs, and disaster recovery archives;
 - b. System-generated cache files, temporary backups, or disaster recovery data accessible to Discord's internal systems but not visible to end-users;
 - c. Deletion logs reflecting message deletions, account deletions, server deletions, or mass content purges, including timestamps, administrator IDs, or API-triggered deletions.
- 9. Internal Safety Enforcement & Machine Learning Classifications, including:**
- a. Internal safety classification tags assigned by Discord's automated moderation systems (including but not limited to flags for CSAM, child

- grooming, narcotics sales, firearms trafficking, hate speech, terrorist content, violent extremism, or financial fraud indicators);
- b. Internal behavioral safety scores, grooming detection signals, anomaly scoring, or policy violation flagging algorithms applied to the Target Account(s);
- c. Moderation appeals, user safety reports, and Trust & Safety case file histories tied to content moderation actions or reported abuse cases.

10. Third Party Application Integrations and OAuth Apps, including:

- a. List of third-party apps, bots, automation tools, scheduling services, server management bots, moderation bots, or integrations authorized via OAuth tokens or API access;
- b. Authorization timestamps, revocation logs, permission levels granted to third-party integrations, and data exchange records with external applications or platforms.

11. System Activity and Diagnostic Logs, including:

- a. Browser and client crash logs, system diagnostic reports, internal bug reporting logs, device error reporting, and telemetry data collected by Discord from client applications;
- b. Referral URLs, web beacons, pixel trackers, single-pixel gifs, cookies, and session analytics metadata captured during app usage;
- c. System uptime, synchronization records, data consistency logs, and metadata retention events related to storage of content for the Target Account(s).

12. Biometric Information (if available), including:

- a. Facial recognition templates, machine-learning derived biometric identifiers, facial mapping templates, or any experimental Discord safety technologies employing biometric data models.

13. Security and Account Protection Data, including:

- a. Two-factor authentication enrollment records, registered security keys, recovery code generation, biometric authentication tokens (if applicable);
- b. Account recovery emails, trusted contacts, trusted devices, alternate phone numbers, and backup recovery pathways;
- c. Suspicious login notifications, geolocation mismatch alerts, anomalous access flags, account compromise detections, brute force prevention systems, and unusual access warnings;

- d. Password reset history, recovery attempts, and associated security events.

14. Customer Support Records, Trust & Safety Correspondence, and Administrative Logs, including:

- a. Records of any communications between Discord staff and the Target Account(s), including correspondence with customer support, Trust & Safety reports, moderation enforcement notices, appeals, compliance department communications, and law enforcement liaison interactions;
- b. Support ticket metadata, case closure records, response time logs, and moderation escalation chains pertaining to complaints involving the Target Account(s).

15. Consent and Legal Agreement History, further described as all user agreements, updated Terms of Service acceptances, community guidelines agreements, privacy policy acknowledgments, age verification attestation, and opt-in/opt-out consent records, including timestamps of consent actions.

NOTE: This request includes any records, messages, or content previously deleted, archived, purged, or modified by the account holder but still recoverable through Discord, Inc.'s internal data retention policies, disaster recovery systems, preservation holds, caching servers, machine learning training archives, or server-side backup infrastructure, whether as full content, partial logs, metadata, snapshots, or reconstructed system-generated records.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Discord is a popular social media and communication platform operated by Discord Inc., headquartered in San Francisco, California. Discord offers a wide range of features allowing its users to communicate through text, voice, video, and file sharing across private direct messages, group chats, and user-managed servers. The data maintained by Discord is hosted on servers owned and controlled by Discord Inc., independent of any user's personal device. Information retained by Discord remains accessible through lawful legal process, such as search warrants or court orders, potentially even if users delete content or attempt to wipe devices.

Users create Discord accounts by providing email addresses and, in some cases, verified mobile phone numbers. Accounts are often operated under pseudonyms, screen names, or numeric identifiers known as Discord "User IDs." Discord allows users to maintain

multiple accounts, sometimes using alternate identities or burner email accounts. User profiles may include avatars, profile photos, status messages, custom bios, linked external social media profiles (such as Twitch, YouTube, Spotify, Xbox Live, Steam, and PayPal), and self-reported biographical information.

Discord servers function as customizable chat communities created and controlled by users. Each server may contain numerous text channels, voice channels, video rooms, and administrative roles that grant certain users moderation or content control privileges. Server owners and moderators can create invitation-only servers, restrict access to specific channels, or configure servers with privacy settings that limit visibility to non-members. These servers may serve legitimate purposes but are frequently exploited by criminal actors to create private communication hubs shielded from public oversight.

Users can communicate privately through direct messages (DMs) and group DMs, which support text conversations, file attachments (including images, videos, documents, and voice notes), links to external storage services, and embedded media. Based on my training and experience, I know that Discord's private messaging features are commonly exploited by individuals engaged in criminal conduct for communications by offenders.

Discord maintains extensive logs of user activity that may assist law enforcement in criminal investigations, including:

- Direct Message content, group chats, and file attachments transmitted via text, voice, or multimedia formats;
- Files shared in private servers, including photographs, videos, voice recordings, and external links directing to cloud storage services containing illicit content;
- Voice chat and video session metadata, including timestamps, participants, session durations, and device connection information;
- Administrative logs reflecting server membership history, channel creation or deletion, role assignments, bans, kicks, user promotions or demotions, and moderation actions taken by administrators or bots;
- Deletion logs reflecting when messages, files, or entire servers are deleted or modified, including associated timestamps;
- Search queries, server browsing history, invited servers, server join dates, and user discovery activities performed on Discord's platform.

In addition to content and communication data, Discord maintains comprehensive technical and account metadata, including:

- IP address logs reflecting all account logins, logouts, and session connections (provided in IPv4 and IPv6 formats where available);
- Device metadata including browser user-agent strings, app version numbers, operating system versions, and device platform information;

- OAuth-based third-party integrations such as Spotify, YouTube, Steam, Xbox, Google, PayPal, and other services linked to Discord profiles;
- Session telemetry logs capturing device fingerprints, session durations, location approximations based on IP geolocation, and backend network telemetry;
- Payment transaction records related to Discord Nitro subscriptions, including linked payment methods, billing addresses, financial account identifiers, transaction histories, and payment processor metadata (Stripe, PayPal, Apple Pay, etc.).

Through my training and experience, I am aware that Discord is frequently utilized by individuals involved in criminal conduct for a variety of offenses, including but not limited to:

- Child exploitation offenders who use Discord to locate, groom, and exploit minors through private direct messages, invite-only servers, and encrypted file sharing of illicit content;
- Narcotics traffickers who coordinate distribution operations, advertise drug sales through coded messages or visual media, and facilitate transactions via external payment services;
- Organized theft rings and financial fraud actors who recruit co-conspirators, plan operations, and exchange stolen personal identifying information, account credentials, or compromised financial data within private servers;
- Hacking and cybercrime communities who share malicious software, hacking tools, credential dumps, stolen databases, and exploit techniques within private Discord communities.

Criminal actors often leverage Discord's privacy features, including server-specific permissions, pseudonymous accounts, disappearing messages, burner email registration, VPN access, and anonymization tools, making them difficult to identify through open-source investigations alone. However, Discord's server-side infrastructure maintains substantial records that can directly identify users, devices, co-conspirators, and criminal conduct through the data elements described above.

Even if content is deleted by the suspect, Discord's internal systems may retain partial or full records through archival backups, preservation holds, system logs, cached storage, and disaster recovery mechanisms. Deletion timestamps may also reflect attempts to obstruct justice or conceal evidence.

In my experience, records maintained by Discord Inc. serve as a critical resource for law enforcement to reconstruct historical communications, uncover the scope of criminal networks, identify otherwise anonymous users, recover deleted evidence, and establish direct links between criminal actors and illegal activity. Because Discord's servers retain this information independently of any seized physical device, search warrants served directly to Discord Inc. may be the only available means to obtain this evidence and further the investigation.

For these reasons, I believe that the requested records maintained by Discord Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Summary for Investigators:

YouTube is a widely used online video-sharing platform **owned by Google**. Users can create personal channels where they upload and share videos that may include tutorials, product demonstrations, entertainment content, educational material, or personal vlogs. In addition to full-length videos, YouTube has introduced newer short-form video features called YouTube Shorts, which are vertical videos generally under 60 seconds, similar in style to TikTok and Instagram Reels. Shorts are designed for rapid content consumption and are heavily promoted through algorithm-driven recommendation feeds, making them a popular tool for viral content, quick advertisements, or brief tutorials.

Beyond standard video uploads, YouTube offers livestreaming, community posts, Stories (for eligible creators), channel memberships, and monetization options through YouTube Partner Program, advertising revenue, and fan-funded features like Super Chats or Super Thanks. Creators can engage directly with viewers through comment sections, live chat during streams, and embedded links in video descriptions. YouTube tracks extensive user activity, including watch history, likes, comments, subscriptions, search queries, and viewing habits, which may assist investigators in identifying subjects, patterns of behavior, financial activity, and potential criminal conduct conducted or promoted through the platform.

How to Serve with Legal Process:

Google (YouTube) accepts legal process and preservation letters electronically through their law enforcement portal: <https://lers.google.com>

Google accepts emergency disclosure requests through the following web form (new as of March 2025): <https://requestrecords.google.com/forms/edr>

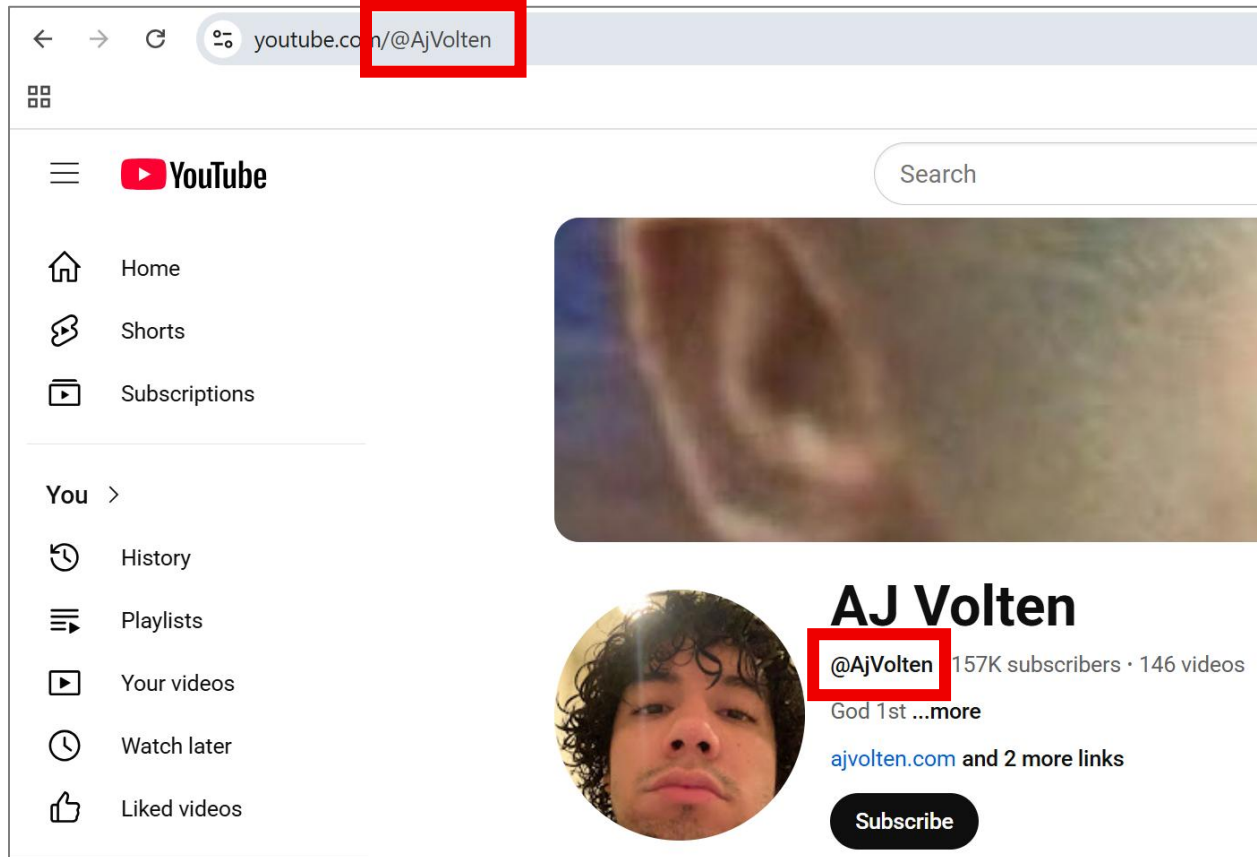
Location to be Searched:

GOOGLE, LLC.
1600 Amphitheatre Parkway
Mountain View, CA 94043

Identify Accounts By:

YouTube accounts can be targeted / identified in our legal process by:

- Username **(See below)**
- Target Email Address(es)
- Target Phone Number(s) *(May or may not work)*
- URLs of profiles or uploaded videos



Items to be Seized:

YOUTUBE DATA:

To the extent that the information described is within the possession, custody, or control of YouTube, LLC (a subsidiary of Google LLC), including any messages, records, files, logs, metadata, or deleted materials still available to YouTube, LLC, or preserved pursuant to legal process or internal retention, YouTube is required to disclose **the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information for the Target Account(s)**, including but not limited to:
 - a. Account usernames, historical usernames, channel names, display names, vanity URLs, retired handles, pseudonyms, and alternate spellings associated with the Target Account(s);
 - b. Google Account identifiers (Gmail addresses, Google IDs, YouTube Channel IDs, Creator IDs);
 - c. Account creation date and time, including associated IP addresses, device identifiers, and registration metadata;
 - d. Account deletion or suspension date and time, including any associated IP addresses or device identifiers;
 - e. Self-reported biographical data, profile descriptions, about-me sections, pronouns, profile avatars, photographs, location fields, gender identity, birthdate, relationship status, and contact information (if provided);
 - f. Email addresses associated with the account, including historical changes, recovery addresses, and verification status;
 - g. Mobile phone numbers linked to the account, including history of additions, removals, or verifications;
 - h. Linked alternate accounts under shared Google Account control (multiple channels under a single Google user);
 - i. Consent logs, terms of service acceptances, privacy policy agreements, community guidelines acceptances, and timestamped consent records;
 - j. Recovery email addresses, phone numbers, and secondary contacts associated with account recovery;
 - k. Account suspension, reinstatement, appeals, policy strikes, warning histories, and enforcement actions maintained by YouTube Trust & Safety.
2. **Device Information** related to the Target Account(s), including:

- a. Device identifiers such as IMEI, IMSI, MAC addresses, hardware IDs, browser user-agent strings, device fingerprints, device models, and platform operating systems;
 - b. Logs of devices used to access the Target Account(s), including login dates, times, session durations, and device connection histories;
 - c. OAuth integrations and external sign-ins via Google, Apple, or third-party identity providers;
 - d. Application version numbers and installed app metadata for mobile, TV, or browser-based access;
 - e. Session persistence tokens, cookie identifiers, backend session continuity tokens, or device binding records used to track sessions across devices, even if VPN or anonymization tools were used.
3. **IP Address Information** for the Target Account(s), to include but not limited to:
- a. Complete logs of all IP addresses used to access, log into, stream from, upload to, or otherwise interact with the account, including app background sessions, telemetry signals, API interactions, content uploads, live broadcasts, and passive background activity;
 - b. IP addresses provided in IPv4 and IPv6 format with port information (where available), timestamps, session durations, and geolocation approximations.
4. **Linked Accounts** to the Target Account(s), to include:
- a. Facebook, Google, Apple, or other external identity providers linked via OAuth;
 - b. Alternate YouTube channels controlled under the same Google Account umbrella;
 - c. Device-based associations reflecting likely pseudonymous or burner accounts accessed via shared hardware, browser fingerprints, cookie data, or IP overlap;
 - d. YouTube Family Group memberships, payment organizers, family sharing subscriptions, and shared billing relationships.
5. **Usage Logs, Account Activity and Content** related to the Target Account(s), including:
- a. Complete video posting history, including uploaded videos, public posts, unlisted videos, private videos, archived videos, abandoned drafts, scheduled future posts, premieres, or preloaded media awaiting publication;

- b. Shorts uploads (published, drafts, and staged uploads);
- c. Live stream events, including scheduled live streams (past, canceled, or future), completed LIVE recordings, participant rosters, chat logs, live stream metadata, timestamps, viewer metrics, gift transactions, and archived content;
- d. Duet-style collaborations (if applicable), split-screen interviews, or collaborative content via live guests or multi-hosting features;
- e. Community tab posts, polls, questions, scheduled posts, canceled community updates, and drafts of future community posts;
- f. Full comment history including video comments, replies, pinned comments, edited comments, deleted comments, timestamps, and upvote/downvote history;
- g. Live Chat Replay logs associated with live streams, including full real-time chat, moderator actions, deleted chat messages, blocked participants, and timestamps;
- h. Private messages (if applicable), creator-to-viewer communications, and interactions in Community spaces;
- i. Saved content including playlists, watch later lists, favorites, bookmarks, saved searches, or multichannel collections;
- j. Search history across YouTube, including video searches, channel searches, hashtags, trending page interaction, and personalized explore feed click behavior;
- k. Administrative enforcement logs reflecting content moderation flags, community guideline strikes, copyright claims, takedowns, removals, and appeals initiated by or against the Target Account(s);
- l. Reports submitted by the Target Account(s) against other users or content, including timestamps, report rationale, and moderation outcomes;
- m. Draft uploads, partially uploaded media, or staged content existing on YouTube backend systems that was never finalized;
- n. Scheduled premieres, abandoned live events, or unpublished livestreams queued for future activation but not executed;
- o. Unlisted sharing URLs and direct private distribution links active or generated by the Target Account(s).

6. YouTube TV (Live TV Streaming Service) Subscriber and Usage Data (if applicable):

- a. YouTube TV subscription enrollment history, including subscription start and cancellation dates, trial periods, membership tiers, channel package selections, and add-on subscriptions;
- b. Billing records, payment history, payment methods, and financial transaction data associated with YouTube TV service under the Target Account(s);
- c. Household Family Group sharing records, including invited household members, linked family accounts, and account sharing activity;
- d. Viewing history logs, including live TV channels watched, DVR (Cloud DVR) recordings, program recording history, watch time logs, playback history, start/stop timestamps, and skip/fast-forward metadata;
- e. Search history specific to YouTube TV content (e.g., search queries for shows, movies, or channels inside the YouTube TV interface);
- f. Location data used for regional channel availability and local programming rights (geo-fencing data, IP-based region assignment, and device location signals);
- g. Advertising engagement history tied to personalized ad targeting shown within YouTube TV service;
- h. Parental controls, restricted content flags, blocked channels, content filtering preferences, and household-level viewing restrictions applied.

7. Financial, Commercial, and Monetization Data for the Target Account(s), including:

- a. YouTube Partner Program (YPP) enrollment, monetization eligibility audits, revenue generation summaries, earnings reports, and payouts;
- b. Super Chat, Super Stickers, channel memberships, fan funding contributions, and supporter payment transaction logs;
- c. Advertising revenue history, linked AdSense accounts, billing addresses, linked financial institutions, tax ID data, payment processor records, and refund or chargeback histories;
- d. Affiliate marketing clickthrough logs where outbound tracking was applied to video descriptions containing monetized external partner links;
- e. Brand sponsorship disclosures, FTC labeling metadata, branded content partnership tools, sponsorship history, and brand campaign management records.

8. Algorithmic, Behavioral, and Personalization Data for the Target Account(s), including:

- a. Algorithmic personalization data reflecting content recommendations, viewing history, watch time metrics, content affinity scores, interest clusters, trending topics, channel suggestions, and behavioral targeting profiles;
- b. Audience modeling data including interest-based targeting, audience segmentation assignments, and inferred ideological alignment profiles;
- c. Trending interaction profiles, hashtag usage clusters, and content interest patterns generated by YouTube recommendation algorithms;
- d. Content sensitivity flags, algorithmic risk assessments, and moderation tags identifying controversial content, high-risk categories (firearms, drug sales, child safety violations, violence), or pending enforcement review.

9. Third Party Application Integrations, including:

- a. OAuth-authorized external applications, mobile integrations, and third-party service connections authorized by the Target Account(s);
- b. Authorization timestamps, granted permission scopes, revocation dates, and external data sharing records;
- c. Automated third-party tools, bots, scraping services, API automation clients, mass posting software, scheduling clients, or externally linked analytics services interacting with YouTube's API infrastructure on behalf of the Target Account(s).

10. Security and Account Protection Data, including:

- a. Password change history, recovery attempts, password reset logs, and recovery credentials;
- b. Two-factor authentication enrollment, trusted device registrations, security key registrations, and backup authentication factors;
- c. Suspicious login alerts, IP-based anomaly flags, account compromise notifications, login mismatch warnings, or backend security telemetry indicating unauthorized access attempts;
- d. Account compromise case investigations, incident management logs, and internal Trust & Safety security flags.

11. Biometric Information (if available), further described as facial recognition templates, biometric verification records, AI-generated moderation hash comparisons, or machine-learning derived biometric data related to content moderation, child safety detection, or CSAM flagging systems utilized by YouTube.

12. **Consent and Legal Agreement History**, further described as all user agreements, terms of service acceptances, privacy policy acknowledgments, content guideline acceptances, monetization policy consents, community policy enrollments, and timestamped records of consent history.

NOTE: This request encompasses any data described above that may have been deleted, archived, modified, hidden, or otherwise concealed but remains accessible through YouTube's internal data retention systems, preservation holds, backup servers, caching infrastructure, disaster recovery processes, and system-generated metadata repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

YouTube is a global video sharing, livestreaming, and content distribution platform operated by Google LLC, a subsidiary of Alphabet Inc., headquartered in Mountain View, California. YouTube offers a wide variety of features that allow users to upload, share, stream, and monetize video content; interact with other users; conduct livestream broadcasts; communicate privately through certain messaging features; and build extensive personal profiles and behavioral data histories. YouTube also offers paid subscription services such as YouTube Premium, YouTube Music, YouTube TV (live television streaming), and other monetization tools for content creators. All data maintained by YouTube is hosted on Google-controlled servers and remains accessible through lawful legal process such as search warrants or court orders, even in cases where users attempt to delete or modify content.

YouTube accounts are generally tied to a broader Google Account, which may include subscriber information such as legal name, email address, phone number, recovery contacts, and billing information. YouTube channel profiles may include usernames, channel names, avatars, profile photographs, banner images, custom biography text, external website links, social media cross-promotions, and other self-reported information. Through my training and experience, I am aware that YouTube profile data can assist investigators in identifying users, uncovering aliases, documenting financial activity, and establishing associations with co-conspirators.

YouTube allows users to upload and distribute video content in various formats, including standard videos, YouTube Shorts (short-form vertical videos), livestream broadcasts, and community posts containing text, images, polls, and external links. Uploaded content may include detailed metadata such as upload timestamps, device identifiers, IP addresses, location information, video descriptions, hashtags, tagged collaborators, closed captioning, viewer comments, and engagement metrics including

likes, dislikes, shares, reposts, and interaction history. YouTube retains records of both public content and unlisted/private videos, as well as historical versions of deleted or modified uploads. Based on my training and experience, uploaded video content frequently contains direct and indirect evidence of criminal activity, including visual depictions of contraband, participation in criminal acts, financial promotion of illegal services, coded messaging, or the recruitment of co-conspirators.

YouTube's livestreaming features allow users to broadcast real-time video and interact with viewers via live chat, super chats (paid highlighted comments), livestream gifting, and monetization tools. YouTube retains comprehensive records of livestream session logs, including full chat histories, gift transactions, timestamps, participant identities, stream recording archives, and financial earnings generated through live broadcasts. Through my training and experience, I am aware that livestreaming is frequently utilized by criminal actors to promote illicit activity, solicit financial support, recruit accomplices, or broadcast criminal conduct in real time.

In addition to public content, YouTube users may communicate through private channel comments, direct message functions (legacy or limited), live chat threads, or external links embedded within video descriptions or community posts. These communications may contain critical evidence of planning, coordination, recruitment, solicitation, or post-offense boasting.

YouTube maintains extensive behavioral and recommendation data that reflects a user's interaction patterns on the platform. This includes:

- Search history, viewed videos, watch time logs, subscription activity, playlist curation, saved content, personalized feed curation, and algorithmically inferred content interests;
- Engagement with promoted content, advertisements, targeted marketing, brand partnerships, and sponsorship programs;
- Interaction histories with other users through comments, likes, polls, pinned messages, and community posts;
- Advertising profiles reflecting inferred demographic data, behavioral targeting segments, purchase interests, political leanings, location targeting, and ad clickthrough history.

In addition to the public YouTube platform, some users may subscribe to YouTube Premium or YouTube TV, which allow for ad-free video access, original content subscriptions, live television streaming, DVR usage, and paid channel memberships. YouTube TV in particular retains records of household accounts, shared family profiles, billing records, DVR recording histories, channel package selections, regional location-based programming, live viewing history, and associated payment methods, all of which may provide critical location-based and financial evidence.

Beyond content and behavioral data, YouTube retains detailed technical and network metadata associated with account activity, including:

- IP address logs reflecting all account access, streaming sessions, uploads, deletions, and search activity;
- Device identifiers such as IMEI, MAC address, browser user-agent strings, app version numbers, and device fingerprints;
- OAuth-based third-party integrations linking YouTube accounts to other services such as Google Pay, AdSense, Patreon, affiliate marketing platforms, or other monetization partners;
- Location data derived from IP address geolocation, device telemetry, location permissions, and Wi-Fi proximity data.

Through my training and experience, I am aware that criminal actors often utilize YouTube for a variety of illegal conduct, including but not limited to:

- Narcotics trafficking organizations advertising products or money laundering schemes through coded videos or livestreams;
- Firearms trafficking suspects demonstrating illegal firearm modifications, manufacturing guides, or offering private party sales through video tutorials or livestream Q&A sessions;
- Child exploitation offenders uploading, sharing, or soliciting sexually exploitative material through coded community groups, restricted sharing links, or private video channels;
- Extremist groups and violent organizations using livestreams, comment sections, and video uploads to promote recruitment, coordinate violent acts, or disseminate propaganda;
- Financial fraud schemes including investment scams, pyramid schemes, cryptocurrency fraud, or romance scams promoted through sponsored video content.

Criminal actors frequently leverage YouTube's privacy settings, including private or unlisted videos, pseudonymous channel names, limited comment moderation, and external monetization partnerships to obscure their identity and insulate their illegal operations. However, YouTube's internal systems retain extensive archived data including subscriber registrations, financial transaction logs, IP address records, location-based access logs, device metadata, behavioral profiling, monetization earnings, advertising partnerships, and historical versions of uploaded or deleted content that may remain accessible through lawful legal process.

Even where content has been deleted, modified, or hidden from public view, YouTube may retain full or partial archival copies through server-side backups, preservation holds, disaster recovery systems, or cached metadata repositories. Deletion logs and modification timestamps may also provide evidence of obstruction, consciousness of guilt, or efforts to destroy incriminating evidence.

In my experience, records maintained by Google LLC and YouTube serve as a critical investigative resource to identify suspects, recover deleted content, document financial gain, establish networks of co-conspirators, and prove direct participation in criminal acts. Because YouTube servers retain this information independently of any seized physical device, search warrants served directly to Google LLC are often the only means to obtain this evidence and further the investigation.

For these reasons, I believe that the requested records maintained by YouTube/Google LLC concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for YouTube:

Because YouTube is owned by Google, YouTube is a “service” offered by them ***linked to their Google account login***. Although the example language above is very YouTube specific, I **strongly recommend** combining this warrant with other Google Services linked to the same account. Why limit yourself with just YouTube content when you could also ask Google for their Android Device Information, Phone Backups, Google Web & Search Activity, Google Drive content, Google Photos content, email content, and more?

There are numerous websites and applications for downloading YouTube videos on an “open source” type basis without writing legal process: Be careful, many are loaded with viruses and malware. The tool I recommend is **4K Video Downloader** (linked in your student portal). Also, I don’t personally consider an open source video download to hold the same evidential value as a video obtained directly from YouTube in response to a search warrant, because that comes with a *Certificate of Authenticity* and we are getting it directly from the source using appropriate legal process – but I also recognize sometimes a video downloaded using an open source tool can be sufficient for a case.

Although YouTube appears “public facing,” don’t underestimate *how much MORE DATA* you can get through a search warrant! When uploading videos, users can set them to private (so they won’t appear on their profile and can’t be found publicly) or accessible only if users have the link. Also, many YouTube accounts have “drafts” (or videos that have not yet been published). With a warrant, you will get that!



Summary for Investigators:

Tinder is one of the most widely-used dating, casual sex, and social networking apps in the world, owned by Match Group. Users create profiles using photographs, biographical text, and preferences such as gender identity, sexual orientation, and relationship interests. The app's core feature is its "swipe" system, where users swipe right to express interest or left to pass on profiles shown to them based on geographic proximity. If both users swipe right, a match is formed, allowing private messaging, photo sharing, voice notes, and even video chats directly within the app.

Tinder has also added features like Photo Verification (biometric selfie verification), Explore for interest-based matching, and Top Picks that curate potential matches based on user behavior. Tinder collects detailed information including precise location data (GPS, IP-based, Wi-Fi triangulation), device identifiers, communication logs, swiping history, search filters, behavioral algorithms, financial transaction records, and security logs. Due to its pseudonymous nature and privacy settings, Tinder is sometimes exploited by offenders for criminal purposes, but its robust server-side storage retains extensive records that are highly valuable in criminal investigations.

While the language contained below is *specific* to Tinder, it can be broadly applicable to most dating or casual sex applications (*there are MANY*), however investigators should take notice to determine other features those applications may have which aren't covered in the below exemplar language and be sure to add them.

How to Serve with Legal Process:

Tinder accepts legal process and preservation letters electronically through their law enforcement portal: <https://app.kodexglobal.com/match-group/signin>

Location to be Searched:

TINDER, LLC.
Attn: Legal Department
PO Box 25458
Dallas, TX 75225

Identify Accounts By:

Tinder accounts can be targeted / identified in our legal process by:

- Username **(See below)**
- Target Email Address(es)
- Target Phone Number(s) *(May or may not work)*

Items to be Seized:

TINDER DATA:

To the extent that the information described is within the possession, custody, or control of Match Group, LLC (parent company of Tinder), including any records, messages, files, logs, metadata, deleted or archived information, or preserved pursuant to legal process, Match Group, LLC is required to disclose the following information for the Target Account(s), for the time period of **January 1, 2025 through the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Tinder usernames, historical username changes, display names, vanity names, alternate handles, aliases, and retired usernames;
 - b. Account creation date, time, registration IP address, device identifiers, and geolocation data at registration;
 - c. Registered email addresses, prior addresses, verification status, and any historical changes;
 - d. Mobile phone numbers linked to the account, including prior phone numbers, verification logs, and deletion records;
 - e. Date of birth, gender, sexual orientation, gender identity, pronouns, ethnicity (if provided), languages spoken, relationship preferences, and self-reported demographic details;
 - f. Biography text, personal interests, education, employment, location fields (hometown, city, country), and profile tags (such as lifestyle interests, hobbies, or "Passions");
 - g. External social media handles or accounts linked via profile, including Instagram, Spotify, Snapchat, Apple ID, Facebook, or Google OAuth connections;
 - h. Uploaded photographs, profile photos, video introductions, video profiles, avatars, photo verification selfies, and video loops used in profile displays;

- i. Consent records, user agreement acceptance logs, privacy policy acknowledgments, community guideline consents, and any timestamped consent history or opt-in logs.
2. **Device Information** related to the Target Account(s), including:
- a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware IDs, and app installation IDs;
 - b. Browser types, user-agent strings, platform versions, app version numbers, operating system versions, and language settings;
 - c. Complete device access logs showing active and passive connections, device changes, session durations, and timestamps.
3. **IP Address Logs** for the Target Account(s), to include but not limited to:
- a. Comprehensive logs of all IPv4 and IPv6 addresses used to register, access, browse, or interact with the Target Account(s), including login IPs, content interaction IPs, background app activity, and geolocation approximations;
 - b. Port information associated with all IP logs, where available.
4. **Linked Accounts & Cross Account Associations** to the Target Account(s), to include:
- a. Third-party accounts linked via OAuth, including but not limited to Facebook, Apple ID, Google, Instagram, Snapchat, Spotify, and YouTube;
 - b. Device-based associations to any additional Tinder accounts registered or accessed via shared hardware, device fingerprints, or cookies;
 - c. Match Group-linked profiles cross-registered using the same email address, phone number, payment credentials, or device (including Hinge, OkCupid, Match.com, Plenty of Fish, and other affiliated brands).
5. **Usage Logs, Account Activity, and Content History**, including:
- a. Full match history, including swipes (likes/dislikes), super likes, boosts, rewinds, blocks, rejections, passes, unmatched accounts, and match date timestamps;
 - b. Message content for all conversations, including one-on-one chats, group chats (if applicable), text, voice messages, video messages, GIFs, attachments, images, emojis, links, file transfers, stickers, and timestamps for sent/received messages;
 - c. Deleted message content, unmatched conversation data, and deletion logs, including timestamps of edits or deletions;

- d. Profile discovery logs, including swipe deck presentation order, exposure counts, explore/discover page activity, search filters applied, profile boost exposure, trending profiles, and Incognito Mode usage history;
- e. Geolocation history based on active app sessions, passive background tracking, GPS coordinates, Wi-Fi triangulation, Bluetooth beacons, IP-based geolocation, and third-party location services integrations;
- f. In-app calling and video chat session logs, including timestamps, call durations, participants, and call connection metadata;
- g. Verification selfie images and machine-learning templates used for identity verification processes ("Photo Verification" feature), including verification pass/fail results, timestamps of submission, and verification enforcement records;
- h. Full "Explore" tab engagement, including content viewed, Top Picks interaction history, Tinder Loop or Video Feature activity, and promotional feature engagement;
- i. Safety features and moderation tools used by the Target Account(s), including "Does This Bother You?" reporting, report abuse submissions, "Safety Center" usage, and user-initiated content flags.

6. App Purchase, Subscription, and Financial Data, including:

- a. Subscription purchase history including Tinder Plus, Tinder Gold, Tinder Platinum, or any premium upgrade tiers;
- b. Payment records, payment methods used, subscription upgrade/downgrade logs, refunds, chargeback history, free trial usage, promotional credits, receipts, and payment processor identifiers;
- c. Super Like purchases, Boost purchases, subscription benefits usage logs, and payment account linkages.

7. Moderation, Safety, and Enforcement Records, including:

- a. User-generated reports against other users, reports submitted against the Target Account(s), safety team investigations, administrative enforcement actions, account warnings, bans, suspensions, or shadow bans;
- b. Internal moderation logs including blocked content, quarantined photos, abusive behavior flags, policy violation detections (e.g., fraud, catfishing, sexual exploitation, scams), and enforcement outcome records;
- c. Law enforcement preservation requests, subpoena history, emergency disclosure requests, and legal compliance records relating to the Target Account(s).

8. Security and Account Protection Records, including:

- a. Password change history, recovery attempts, password reset logs, and device authentication events;
- b. Two-factor authentication enrollment, security key registration, trusted device list, suspicious login warnings, location mismatch alerts, account compromise notifications, and high-risk flagging events.

9. Biometric and Image Verification Data, including:

- a. Selfie verification templates and facial recognition metrics generated for identity verification;
- b. Machine-learning generated facial recognition data tied to Photo Verification enforcement systems.

10. Consent, Legal Agreements, and User Policy Logs, including a complete history of terms of service acceptance, privacy policy agreements, opt-ins, opt-outs, profile disclosures, and community guideline acceptance logs with timestamp metadata.

NOTE: This request includes any records, content, metadata, or account activity that may have been deleted, archived, modified, or otherwise concealed but remains recoverable to Match Group, LLC through internal backup systems, disaster recovery policies, preservation holds, system-level logs, and server-side data repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Tinder is a widely-used online dating, casual sex, and social networking application owned and operated by Match Group, LLC. Tinder allows individuals to create personal profiles, view other users' profiles, engage in private messaging, conduct live video and voice calls, and interact based on proximity, shared interests, and mutual consent. Tinder's application is accessible through mobile devices, web browsers, and integrated third-party platforms. Data maintained by Tinder is stored on servers controlled by Match Group, LLC, independently of the user's personal device. This server-side storage allows information to remain accessible through lawful legal process, such as search warrants or court orders, even if a suspect deletes content from their local device.

Users create Tinder accounts by registering with mobile phone numbers and/or email addresses. Profiles generally include photographs, biographical text, gender identity, sexual orientation, relationship interests, geographic location, and optional external social

media links such as Instagram, Snapchat, Spotify, or Apple Music. Tinder utilizes facial recognition technology and selfie verification features ("Photo Verification") to verify a user's identity and confirm the authenticity of uploaded profile photos. This biometric verification generates machine-learning templates that may help confirm the identity of individuals controlling specific accounts.

The core functionality of Tinder involves swiping through user profiles based on geographic proximity, where users may "like" or "pass" on other users. When both users express mutual interest, Tinder creates a match, allowing private messaging and other interactive features. Users may also engage in video chats, voice calls, send photos, emojis, GIFs, links, audio recordings, and participate in video-based introductions. Tinder maintains detailed logs of these communications, including message content, timestamps, device metadata, deletion logs, and related engagement metrics.

In addition to private messaging, Tinder collects extensive interaction and behavioral data through features such as Top Picks, Explore tab, Super Likes, Boosts, Swiping metrics, trending profile interactions, and mutual interests. Tinder tracks all profile exposure data, swiping decisions, explore page behaviors, search filters, profile views, profile boosts, and curated interest-based recommendations delivered to the user. This information can reveal patterns of behavior, relationship-building activity, search intent, and suggest connections between users.

Tinder also maintains extensive location-based data tied to account activity. Location data may include GPS coordinates, IP-based geolocation, Wi-Fi triangulation, Bluetooth beacon proximity, and session-level tracking, even when the app is running in background mode. This may place a user at a specific location at a particular time, which is critical for criminal investigations involving offenses occurring at specific places.

Tinder maintains subscription and financial data for users who upgrade to premium services (Tinder Plus, Gold, Platinum), purchase Boosts or Super Likes, or engage in other in-app financial transactions. This includes purchase histories, billing addresses, payment methods, refunds, and chargeback disputes. These financial records may assist law enforcement in identifying suspects or establishing digital fingerprints linking multiple accounts or devices to a single offender.

In addition to subscriber and communication data, Tinder preserves extensive account protection, moderation, and safety records. This includes password reset logs, two-factor authentication records, suspicious login notifications, compromised account warnings, and safety feature usage, such as Tinder's in-app reporting tools, "Safety Center," user abuse reports, and enforcement actions for community guideline violations.

Because Tinder accounts may be accessed across multiple devices and may use pseudonyms or fake photographs, individuals engaged in criminal conduct often utilize Tinder to conceal their true identity. However, Tinder's centralized server infrastructure preserves critical records that allow investigators to recover deleted messages, link

multiple accounts via device identifiers or payment records, and confirm the true identity of users through biometric verification data, IP address logs, and third-party OAuth associations.

In my experience, these records maintained by Match Group, LLC serve as an essential evidentiary resource for reconstructing historical communications, identifying offenders, corroborating victim statements, and documenting the full scope of criminal conduct committed through the Tinder platform.

For all the reasons described above, I believe the requested records maintained by Match Group, LLC related to the identified Tinder account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.



Summary for Investigators:

Bumble is a location-based dating and social networking app that allows users to create personal profiles featuring photographs, biographical information, interests, and lifestyle preferences. Unlike some dating platforms, Bumble's core feature gives female users the option to initiate conversations when a match occurs, particularly in heterosexual matches. Users swipe right to express interest and left to dismiss, with mutual interest resulting in a match. In addition to dating, Bumble also offers "Bumble BFF" for finding platonic friendships and "Bumble Bizz" for networking. Users can link their profiles to external social media accounts such as Instagram or Spotify, upload multiple profile photos, and provide verified identity credentials such as phone numbers, email addresses, and optional photo verifications.

Bumble collects and maintains extensive data on user activity, including swiping history, match history, chat transcripts, video call logs, blocked/unmatched user lists, payment records (for subscription features), location data, IP addresses, device identifiers, and search filters used. In criminal investigations, Bumble records can help establish connections between suspects and victims, reveal grooming behaviors, document timelines, and corroborate statements regarding when and how contact was initiated. Even if users delete messages, unmatched with others, or attempt to alter profiles after an offense, Bumble's server-side retention may preserve deleted data accessible via legal process.

How to Serve with Legal Process:

Bumble accepts legal process and preservation letters electronically through their law enforcement portal: <https://app.kodexglobal.com/bumble/signin>

Location to be Searched:

BUMBLE TRADING LLC.
1105 West 41st Street
Austin, Texas 78756

Identify Accounts By:

Bumble accounts can be difficult to identify in our legal process because public facing profiles don't display any unique identifiers (usernames, user IDs, contact information), which presents some challenges for us.

Bumble asks that investigators, within our legal process, provide **the account name** (IE: John Smith) **and** one of the following:

- Unique User ID
- Associated Email Address(es)
- Associated Phone Number(s)

Here are a few ways we can work through this issue:

1. Write for the victim's account first. For the victim to identify their User ID, they can go into their *settings* within the Bumble application, scroll to the bottom and double tap the Bumble logo (this will reveal their Bumble ID). Bumble's records that you obtain via search warrant from the victim's account will have communications content, and unique identifiers for people they are communicating with.
2. Alternatively, we recommend providing Bumble with the victim's account information and a screenshot of the suspect's profile. IE: "The Bumble account with the name 'John Smith,' which has been communicating with the victim's account (User ID: xxxx). A screenshot of the target profile for 'John Smith' is attached and incorporated below."

Bumble is relatively helpful for law enforcement so don't fret, just provide them as much information as possible to help them identify the correct account.

Items to be Seized:

BUMBLE DATA:

To the extent that the information described is within the possession, custody, or control of Bumble, Inc., including any records, files, messages, content, logs, metadata, or deleted materials still available to Bumble, Inc., or preserved pursuant to legal process or internal retention, **Bumble, Inc. is required to disclose the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account usernames, display names, vanity names, aliases, alternate spellings, retired usernames, profile handles, and pseudonyms;

- b. Account creation date and time, including IP addresses and device identifiers at registration;
- c. Email addresses associated with the account, including verification status, historical changes, and prior addresses;
- d. Mobile phone numbers linked to the account, including verification status, historical changes, and deletions;
- e. Legal name, date of birth, gender, gender identity, pronouns, sexual orientation, relationship status, self-reported biographical information, hometown, residence city, employment information, education history, languages spoken, and religious/political affiliations (if provided);
- f. Profile photographs, profile videos, avatars, Bitmojis, or digital likenesses uploaded by the user;
- g. Consent logs, including terms of service acceptances, privacy policy agreements, community guidelines acceptances, and timestamped records of user acknowledgments;
- h. Verified identity documentation (if provided), including government-issued ID verification or facial recognition verification data;
- i. Linked social media accounts or external app integrations authorized by the user.

2. **Device Information** related to the Target Account(s), including:

- a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware IDs, and app installation IDs;
- b. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
- c. Browser types, user-agent strings, platform versions, app version numbers, operating system versions, and language settings;
- d. Complete device access logs showing active and passive connections, device changes, session durations, and timestamps.

3. **IP Address Logs** for the Target Account(s), to include but not limited to:

- a. Comprehensive logs of all IPv4 and IPv6 addresses used to register, access, browse, or interact with the Target Account(s), including login IPs, content interaction IPs, background app activity, and geolocation approximations;
- b. Port information associated with all IP logs, where available.

4. **Linked Accounts & Cross Account Associations** to the Target Account(s), to include:
 - a. Other Bumble or affiliated accounts created using the same device fingerprints, email addresses, phone numbers, browser identifiers, cookies, or OAuth credentials;
 - b. Device-based associations between the Target Account(s) and other pseudonymous accounts accessed from the same hardware or app installation.

5. **Usage Logs, Account Activity, and Content History**, including:
 - a. Full profile content, including all versions of uploaded bios, profile captions, personal interests, hobbies, tags, favorite music integrations, or Spotify-linked content;
 - b. Swipe history, including records of profiles liked, super-liked, passed, rewound, matched, or unmatched, with associated timestamps and profile identifiers;
 - c. Match history, including all individuals matched with, match initiation timestamps, match expiration timestamps, and removal or unmatched actions;
 - d. Full message history for all matched contacts, including text messages, emojis, GIFs, voice notes, photos, videos, external links, file attachments, stickers, and timestamps;
 - e. Block lists, unmatched users, reported accounts, or accounts flagged for inappropriate behavior by the Target Account(s);
 - f. Report logs submitted against the Target Account(s), including the content of reports, reasons for reports, timestamps, review decisions, and moderator notes;
 - g. Saved media, uploaded private photos (including blurred or “photo unlock” content), subscription-based premium content shared, or private albums;
 - h. Video chat records, including session metadata, timestamps, duration, participants, and technical logs of video call sessions;
 - i. Boosts, Spotlight usage, profile promotion purchases, and purchase history related to app-based premium features;
 - j. Account changes including profile edits, photo uploads/removals, privacy setting changes, deletion requests, and deactivation/reactivation logs;
 - k. Search history, keyword searches, filter use (distance, age range, gender preferences, intent preferences), and behavioral interaction logs influencing match algorithms.

6. **App Purchase, Subscription, and Financial Data**, including:
 - a. Purchase history for Bumble Boost, Bumble Premium, Spotlight, SuperSwipe, or other monetized services, including purchase dates, subscription renewals, cancellations, payment method details, billing addresses, and financial account identifiers;
 - b. Payment processor records (Stripe, PayPal, Apple Pay, Google Pay, etc.) linked to the Target Account(s);
 - c. Refund requests, chargebacks, or disputed transactions.
7. **Behavioral, Algorithmic, and Personalization Data**, including:
 - a. a. User interest profiles, match suggestion algorithms, behavioral learning data, swipe tendencies, interaction patterns, and recommendation data used to refine feed delivery for the Target Account(s);
 - b. b. Content personalization data derived from machine-learning analysis of profile activity, message behavior, and app usage.
8. **Moderation, Safety, and Enforcement Records**, including:
 - a. User-generated reports against other users, reports submitted against the Target Account(s), safety team investigations, administrative enforcement actions, account warnings, bans, suspensions, or shadow bans;
 - b. Internal moderation logs including blocked content, quarantined photos, abusive behavior flags, policy violation detections (e.g., fraud, catfishing, sexual exploitation, scams), and enforcement outcome records;
 - c. Law enforcement preservation requests, subpoena history, emergency disclosure requests, and legal compliance records relating to the Target Account(s).
9. **8. Third-Party Integrations**, including:
 - a. List of authorized third-party apps connected to the Target Account(s);
 - b. Historical records of granted permissions, scopes of data sharing, revocations, and OAuth transactions.
10. **Security and Account Protection Records**, including:
 - a. Password change logs, password reset requests, recovery attempts, and multi-factor authentication enrollment;
 - b. Device security keys, trusted devices, recovery email addresses, and backup contacts;

- c. Suspicious login alerts, unauthorized access notifications, location mismatch warnings, or high-risk anomaly detections.

11. Biometric and Image Verification Data, including:

- a. Selfie verification templates and facial recognition metrics generated for identity verification;
- b. Machine-learning generated facial recognition data tied to Photo Verification enforcement systems.

12. Consent, Legal Agreements, and User Policy Logs, including a complete history of terms of service acceptance, privacy policy agreements, opt-ins, opt-outs, profile disclosures, and community guideline acceptance logs with timestamp metadata.

NOTE: This request includes any records, content, metadata, or account activity that may have been deleted, archived, modified, or otherwise concealed but remains recoverable to Bumble LLC. through internal backup systems, disaster recovery policies, preservation holds, system-level logs, and server-side data repositories.

Affidavit Language:

Based upon my training, experience, consultation with other investigators, and information obtained during this investigation, I believe the following to be true:

Bumble is a popular online dating and social networking application operated by Bumble, Inc., headquartered in Austin, Texas. Bumble is primarily a mobile-based platform designed to facilitate romantic connections, friendships, and professional networking. It is one of the most widely used dating apps in the United States and internationally. Bumble allows users to create detailed personal profiles, communicate privately with other users, and engage in various forms of multimedia interaction. The data maintained by Bumble is stored on servers controlled by Bumble, Inc., independent of any user's personal device. Information retained by Bumble remains accessible through lawful legal process such as search warrants or court orders, even if the user deletes or modifies data from within the application.

To establish an account on Bumble, users are required to provide certain personal identifiers, including a verified mobile phone number and/or email address. Users create profiles that may include photographs, biographical information, gender identity, sexual orientation, pronouns, date of birth, employment details, educational background, interests, hobbies, and location data. Many users link external accounts such as Spotify or Instagram to supplement their profiles, and may undergo identity verification steps that involve uploading photographs or facial recognition submissions for verification badges.

Bumble collects and retains extensive subscriber records that may assist law enforcement in confirming the identity of users and linking accounts to physical individuals involved in criminal activity.

Bumble facilitates communication through private one-on-one messaging between users who have matched. In addition to standard text messaging, Bumble supports sharing photos, videos, voice notes, emojis, GIFs, file attachments, links, contact information, and external social media handles. These private message exchanges are often used to coordinate in-person meetings, exchange sensitive information, and arrange financial transactions. In my training and experience, individuals involved in criminal activity regularly utilize dating applications like Bumble as a covert method of initiating illegal communications, including trafficking, fraud schemes, and sexual exploitation.

Bumble maintains extensive activity logs that are valuable to criminal investigations. These include complete swipe history (likes, super likes, passes, rewinds), match history, match initiation and unmatch timestamps, and complete chat histories for all connections. Bumble also retains data related to video calls conducted within the platform, including session metadata, participants, and timestamps. Users may also create private albums and upload locked photographs which require mutual consent to unlock, sometimes used to share sensitive or illicit content privately between matched parties.

Bumble collects extensive device metadata, including IP address logs, device fingerprints, user-agent strings, push notification tokens, and browser data tied to each account session. This information may allow law enforcement to directly link accounts to specific devices, physical locations, or multiple accounts operated by the same suspect. Bumble also retains search and filter data reflecting user preferences (e.g., location radius, age range, gender filters, intent filters), which may provide insight into patterns of victim targeting or geographic focus areas for criminal activity.

Bumble's monetization features include subscription-based services such as Bumble Boost, Bumble Premium, SuperSwipes, Spotlight promotions, and in-app purchases that enhance user visibility and match opportunities. Bumble maintains detailed financial records of these transactions, including payment methods, processor data, billing addresses, refunds, and chargeback history. Financial records may reflect ongoing revenue streams or traceable financial ties to illicit conduct.

Even if content is deleted by the user, Bumble may preserve data through its internal archival, retention, or preservation systems, including deleted account logs, chat deletion records, content modification timestamps, and audit trails. Deleted content and account deletion logs may provide evidence of efforts to obstruct justice, conceal criminal activity, or destroy evidence.

Through my training and experience, I am aware that Bumble may serve as a significant digital repository of evidence in criminal investigations by preserving a detailed history of a suspect's communications, financial transactions, movement patterns, victim

targeting, and behavioral preferences. Because Bumble's servers retain this information independent of a suspect's physical device, legal process served directly to Bumble, Inc. is often the only means by which law enforcement can recover historical evidence critical to the investigation.

For all of the reasons set forth above, I believe that the requested records maintained by Bumble, Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of violations under investigation.

Summary for Investigators:

Hinge is a popular dating and relationship-oriented social media platform owned by Match Group, the same parent company that operates Tinder, Match.com, and other major dating apps. Unlike traditional swipe-based dating apps, Hinge markets itself as a "relationship app" designed to encourage more serious or intentional connections. Users create detailed profiles that include photos, self-written prompts, lifestyle preferences, interests, political views, religious beliefs, and various personal identifiers. Hinge's algorithm uses this information, along with location data, to suggest compatible matches nearby. Users can "like" specific parts of another user's profile and initiate conversations directly, leading to private messaging threads that are not visible to any other users or moderators.

While many users utilize Hinge for its intended purpose, the platform has increasingly been exploited by offenders seeking to identify, target, and meet potential victims. Private messaging allows suspects to communicate extensively, exchange personal information, and arrange in-person meetings outside of the app's oversight. Hinge maintains detailed server-side records, including message histories (even for unsent messages), voice notes, photos exchanged in chat, call logs, IP address history, device identifiers, financial payment data, and subscription history. This data is critical for law enforcement investigations into sexual assault, stalking, human trafficking, and other offenses where suspects use dating platforms to access vulnerable victims.

How to Serve with Legal Process:

Hinge accepts legal process and preservation letters electronically through their law enforcement portal: <https://app.kodexglobal.com/match-group/signin>

Location to be Searched:

HINGE, INC.
8750 N. Central Expy, Ste 1400
Dallas, Texas 75231

Identify Accounts By:

- Name and Screenshot of Profile
- Username / User ID
- Phone Number
- Email Address

Items to be Seized:

HINGE DATA:

To the extent that the information described is within the possession, custody, or control of Hinge, Inc., including any records, files, messages, content, logs, metadata, or deleted materials still available to Hinge, Inc., or preserved pursuant to legal process or internal retention, **Hinge, Inc. is required to disclose the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account usernames, display names, historical usernames, vanity names, aliases, retired handles, alternate spellings, and pseudonyms;
 - b. Full name as reported by user, date of birth, gender, pronouns, sexual orientation, relationship preferences, ethnicity, religion, political views, education history, occupation, employer, and all self-reported biographical information;
 - c. Account creation date and time with associated IP address and device information;
 - d. Account deletion date and time, including associated IP addresses and deletion requests;
 - e. All email addresses associated with the account, including historical changes, verification statuses, and prior addresses;
 - f. Mobile phone numbers linked to the account, including verification status, additions, removals, or changes;
 - g. Linked external social media accounts (e.g., Instagram, Facebook, Snapchat, Spotify, etc.);
 - h. Photographs, videos, or other profile media uploaded or linked by the user, including all historical profile photo versions;
 - i. Photo verification status, facial recognition submissions, or selfie authentication records;
 - j. Consent and legal agreement records including privacy policy consents, terms of service agreements, and community guidelines acknowledgments with associated timestamps.
2. **Device Information** related to the Target Account(s), including:
 - a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware IDs, and app installation IDs;
 - b. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);

- c. Browser types, user-agent strings, platform versions, app version numbers, operating system versions, and language settings;
 - d. Complete device access logs showing active and passive connections, device changes, session durations, and timestamps.
- 3. **IP Address Logs** for the Target Account(s), to include but not limited to:
 - a. Comprehensive logs of all IPv4 and IPv6 addresses used to register, access, browse, or interact with the Target Account(s), including login IPs, content interaction IPs, background app activity, and geolocation approximations;
 - b. Port information associated with all IP logs, where available.
- 4. **Linked Accounts & Cross Account Associations** to the Target Account(s), to include:
 - a. Other Hinge or affiliated accounts created using the same device fingerprints, email addresses, phone numbers, browser identifiers, browser sessions, cookies, IP overlaps, linked contact data, or OAuth credentials;
 - b. Social media integrations or linked third-party OAuth logins associated to the Target Account(s);
 - c. Device-based associations between the Target Account(s) and other pseudonymous accounts accessed from the same hardware or app installation;
 - d. Internal system identifiers used by Match Group to associate accounts across owned platforms (e.g., Tinder, Match.com, OkCupid, Plenty of Fish, etc.).
- 5. **Usage Logs, Account Activity, and Content History**, including:
 - a. Complete match history including all mutual matches, one-sided likes, skips, passes, and undo actions, including timestamps and associated profile data of matched parties;
 - b. Full chat history and messaging content, including text conversations, voice messages, photos, videos, emojis, GIFs, and stickers exchanged between users;
 - c. Call logs including in-app video calls, voice calls, call durations, participant identifiers, timestamps, and connection metadata;
 - d. Deleted messages, unmatches, unmatched users, message deletion history, and corresponding deletion timestamps;

- e. Blocked user lists, reports filed, abuse reports submitted, or users reported by or against the Target Account(s);
- f. “Standouts,” “Prompts,” and profile answers, including all historical edits and responses;
- g. User swiping and interaction behavior, including swiping tendencies, preferences, and behavioral scoring utilized for algorithmic matching and recommendation algorithms;
- h. Saved searches, search filters applied, and interest or compatibility criteria;
- i. Behavioral logs reflecting usage patterns, app navigation behavior, content engagement metrics, time spent on profiles, and algorithmic scoring data generated by Hinge.

6. App Purchase, Subscription, and Financial Data, including:

- a. Hinge Preferred subscription history, billing records, payment methods, payment processor metadata, and any stored financial account information linked to the account;
- b. Purchase history of premium features such as “Boosts,” “Roses,” or other monetized services offered by Hinge;
- c. Transaction logs, refunds, chargebacks, and payment disputes tied to the Target Account(s).

7. Behavioral, Algorithmic, and Personalization Data, including:

- a. User interest profiles, match suggestion algorithms, behavioral learning data, swipe tendencies, interaction patterns, and recommendation data used to refine feed delivery for the Target Account(s);
- b. Content personalization data derived from machine-learning analysis of profile activity, message behavior, and app usage.

8. Moderation, Safety, and Enforcement Records, including:

- a. User-generated reports against other users, reports submitted against the Target Account(s), safety team investigations, administrative enforcement actions, account warnings, bans, suspensions, or shadow bans;
- b. Internal moderation logs including blocked content, quarantined photos, abusive behavior flags, policy violation detections (e.g., fraud, catfishing, sexual exploitation, scams), and enforcement outcome records;
- c. Law enforcement preservation requests, subpoena history, emergency disclosure requests, and legal compliance records relating to the Target Account(s).

9. Security and Account Protection Records, including:

- a. Password change logs, password reset requests, recovery attempts, and multi-factor authentication enrollment;
- b. Device security keys, trusted devices, recovery email addresses, and backup contacts;
- c. Suspicious login alerts, unauthorized access notifications, location mismatch warnings, or high-risk anomaly detections.

10. Biometric and Image Verification Data, including:

- a. Selfie verification templates and facial recognition metrics generated for identity verification;
- b. Machine-learning generated facial recognition data tied to Photo Verification enforcement systems.

11. Consent, Legal Agreements, and User Policy Logs, including a complete history of terms of service acceptance, privacy policy agreements, opt-ins, opt-outs, profile disclosures, and community guideline acceptance logs with timestamp metadata.

NOTE: This request includes any records, content, metadata, or account activity that may have been deleted, archived, modified, or otherwise concealed but remains recoverable to Hinge, Inc. through internal backup systems, disaster recovery policies, preservation holds, system-level logs, and server-side data repositories.

Affidavit Language:

Based upon my training, experience, consultation with other investigators, and information obtained during this investigation, I believe the following to be true:

Hinge is a popular online dating application and social networking service owned and operated by Match Group, Inc. Hinge is designed to facilitate connections between users through algorithmic matchmaking, mutual interests, location proximity, and shared biographical traits. The application is available via mobile devices, web browsers, and integrated third-party platforms. Hinge maintains user account data, communications, and profile information on servers controlled by Match Group, Inc., independent of any user's personal device. This information is accessible to law enforcement via lawful legal process, such as search warrants or court orders, even in cases where content may have been deleted, hidden, or modified by the user.

Users create Hinge accounts by providing a valid mobile phone number or third-party authentication credentials such as Google, Apple, or Facebook. Users may optionally supply a wide range of personal information to populate their dating profiles, including full name, date of birth, gender, sexual orientation, relationship preferences, religion, ethnicity, educational history, employment details, political views, pronouns, and self-written biographical prompts. Profiles also include user-submitted photographs and videos, many of which are verified through facial recognition selfie submissions to ensure authenticity. Users often link external social media platforms such as Instagram or Spotify to their Hinge accounts.

Through its core features, Hinge allows users to view profiles of others within geographical proximity or matching algorithmic preferences, and initiate connections by “liking” specific photos, videos, or profile prompts. When two users mutually express interest, they form a match and are permitted to communicate via private messaging features within the app. These conversations may include text messages, voice recordings, photos, videos, GIFs, emojis, stickers, and links. Hinge also offers in-app voice and video call capabilities, allowing matched users to conduct private calls directly through the application. Hinge retains extensive records of message histories, media attachments, timestamps, deletion logs, call histories, and user interaction metrics associated with each match.

Hinge maintains detailed activity logs related to user behavior, including:

- Mutual matches, likes, passes, skips, and rejections;
- Message history, including deleted conversations, unmatched contacts, and timestamps of communication attempts;
- Call logs for voice and video sessions;
- Profile browsing behavior, saved searches, swipe patterns, preferences, and behavioral scoring metrics;
- Reports filed by or against the user for misconduct, abuse, or harassment;
- Content takedown requests and moderation actions initiated by Hinge’s Trust & Safety team.

Hinge also retains comprehensive account metadata including:

- IP address logs reflecting all account activity, including registration, logins, logouts, messaging sessions, and profile updates;
- Device identification data including device IDs, IMEI, IMSI, MAC addresses, hardware fingerprints, user-agent strings, and application versioning;
- OAuth-based third-party integrations, social media linkage records, and system identifiers used by Match Group to associate multiple accounts across their owned platforms;
- Subscription records for premium features such as “Hinge Preferred,” “Roses,” or Boost purchases, along with complete financial records tied to payments, refunds, disputes, and billing histories.

Through my training and experience, I know that Hinge is regularly used by individuals involved in criminal activity, including but not limited to:

- Sexual assault investigations involving suspects who initiate contact with victims through dating applications;
- Human trafficking operations where offenders exploit dating platforms to identify, groom, and recruit vulnerable victims;
- Fraud schemes where suspects misrepresent themselves for financial gain, romance scams, or identity theft;
- Stalking, harassment, and coercive control where suspects use Hinge's messaging and voice features to maintain unwanted or criminal contact with victims.

Criminal actors may attempt to conceal their identities by using pseudonyms, false profile information, burner phone numbers, VPN services, or anonymized payment methods. However, Hinge's extensive server-side records provide law enforcement with critical evidence to identify suspects, document patterns of behavior, corroborate victim reports, and reconstruct deleted or modified communications essential to criminal investigations.

Because Hinge stores user data remotely, law enforcement may be unable to fully recover this evidence from seized physical devices alone. Obtaining these records directly from Match Group, Inc., via lawful process, may be the only available means to obtain complete historical evidence relevant to this investigation.

For these reasons, I believe that the requested records maintained by Hinge and Match Group, Inc. concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.



Summary for Investigators:

Grindr is a location-based dating and social networking application primarily marketed toward LGBTQ+ users, with a particular emphasis on gay, bisexual, transgender, and queer men. Users create profiles using display names, profile photos, short biographies, and limited self-reported information such as age, gender identity, and relationship preferences. The platform operates primarily via mobile devices, leveraging real-time GPS data to show users a list of nearby accounts, ranked by proximity. Grindr's chat feature allows users to exchange direct messages, photographs, and videos. Some users may also link external social media profiles or third-party apps to their Grindr profile. While marketed as a dating or hookup app for consenting adults, law enforcement regularly encounters Grindr being misused by offenders to locate underage victims who have misrepresented their age during registration.

Grindr retains limited historical data compared to many other platforms. While the platform does not store message content long-term, it does maintain critical subscriber information such as email addresses, linked phone numbers, device information (including device ID, IMEI, and user-agent strings), payment history for premium accounts (Grindr XTRA or Grindr Unlimited), and IP address logs reflecting login activity and approximate location. Because Grindr profiles are pseudonymous and can be created with minimal identity verification, investigators often rely on these technical metadata logs, payment details, and device-based account linkages to identify offenders and corroborate investigative leads. Its proximity-based matching system and embedded geolocation features also present investigative opportunities to correlate suspect movements, victim proximity, or identify potential witnesses.

How to Serve with Legal Process:

Grindr accepts legal process and preservation letters electronically through their law enforcement portal: <https://app.kodexglobal.com/grindr/signup>

Location to be Searched:

Grindr, LLC. (*Hereinafter referred to as "Provider"*)
C/O Telos Legal Corp.
9450 SW Gemini Dr, PMB 73938
Beaverton, OR 97008

Identify Accounts By:

- User ID
- Phone Number
- Email Address

Grindr claims they need a “Support Code or Device ID” to locate an account and produce data and the only way for investigators to obtain this is by possessing the user’s device. They used to provide a “how to” page for law enforcement on how to locate these unique identifiers, but it is now offline. In reviewing past warrants to Grindr, they historically have responded to requests by email or phone number.

Items to be Seized:

GRINDR DATA:

To the extent that the information described is within the possession, custody, or control of Grindr LLC (or its parent company), including any records, files, or metadata retained internally or preserved pursuant to legal process, **Grindr LLC is required to disclose the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account username, display name, and user ID;
 - b. Registered email address (including historical changes if available);
 - c. Registered mobile phone number (including historical changes if available);
 - d. Profile photograph(s) or avatar(s) currently associated with the account;
 - e. Account creation date and timestamp;
 - f. Account deletion date and timestamp (if applicable);
 - g. Account consent logs, including terms of service acceptance, privacy policy acknowledgments, and timestamped acceptance history.
2. **Device Information** related to the Target Account(s), including:
 - a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware IDs, and app installation IDs;
 - b. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
 - c. Browser types, user-agent strings, platform versions, app version numbers, operating system versions, and language settings;
 - d. Complete device access logs showing active and passive connections, device changes, session durations, and timestamps.

3. **IP Address Logs** for the Target Account(s), to include but not limited to:
 - a. Comprehensive logs of all IPv4 and IPv6 addresses used to register, access, browse, or interact with the Target Account(s), including login IPs, content interaction IPs, background app activity, and geolocation approximations;
 - b. Port information associated with all IP logs, where available.
4. **Financial & Payment Records**, including:
 - a. Subscription history for premium services (e.g. Grindr XTRA, Grindr Unlimited), including purchase dates, billing addresses, payment methods, transaction records, and payment processor identifiers.
5. **Content or Activity Logs / Records of Account Usage** related to the target account preserved or retained by Grindr, LLC., including:
 - a. Complete message content for all private chats, including sender, recipient, timestamps, message text, photos, videos, voice notes, GIFs, emojis, stickers, links, and any media shared via chat;
 - b. Match history, including connection requests, accepted matches, rejections, blocks, favorites, and user interactions (with dates/times);
 - c. Profile views, who viewed the Target Account's profile, and when;
 - d. Search history and browsing activity within the app;
 - e. User distance calculations and proximity logs generated by Grindr's location algorithm (distance-based matching logs, not exact coordinates unless preserved);
 - f. Likes, favorites, taps, flames, or other reaction-based activity;
 - g. History of blocked, unfriended, muted, and unblocked accounts.
6. **Moderation, Safety, and Enforcement Records**, including:
 - a. User-generated reports against other users, reports submitted against the Target Account(s), safety team investigations, administrative enforcement actions, account warnings, bans, suspensions, or shadow bans;
 - b. Internal moderation logs including blocked content, quarantined photos, abusive behavior flags, policy violation detections (e.g., fraud, catfishing, sexual exploitation, scams), and enforcement outcome records;
7. **Third-Party Integrations**, including:
 - a. List of authorized third-party apps connected to the Target Account(s);

- b. Historical records of granted permissions, scopes of data sharing, revocations, and OAuth transactions.

8. Security and Account Protection Records, including:

- a. Password change logs, password reset requests, recovery attempts, and multi-factor authentication enrollment;
- b. Device security keys, trusted devices, recovery email addresses, and backup contacts;
- c. Suspicious login alerts, unauthorized access notifications, location mismatch warnings, or high-risk anomaly detections.

9. Consent, Legal Agreements, and User Policy Logs, including a complete history of terms of service acceptance, privacy policy agreements, opt-ins, opt-outs, profile disclosures, and community guideline acceptance logs with timestamp metadata.

NOTE: This request includes any deleted, archived, hidden, restricted, or modified content, metadata, or communications that may remain accessible to Grindr through internal retention policies, archival systems, backup infrastructure, disaster recovery storage, or preservation holds initiated pursuant to legal process.

GRINDR DATA:

To the extent that the information described is within the possession, custody, or control of Grindr LLC (or its parent company), including any records, files, or metadata retained internally or preserved pursuant to legal process, **Grindr LLC is required to disclose the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. Subscriber Information for the Target Account(s), to include:

- a. Account username, display name, and user ID;
- b. Registered email address (including historical changes if available);
- c. Registered mobile phone number (including historical changes if available);
- d. Profile photograph(s) or avatar(s) currently associated with the account;
- e. Account creation date and timestamp;
- f. Account deletion date and timestamp (if applicable);
- g. Account consent logs, including terms of service acceptance, privacy policy acknowledgments, and timestamped acceptance history.

2. Device Information related to the Target Account(s), including:

- a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware IDs, and app installation IDs;
 - b. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
 - c. Browser types, user-agent strings, platform versions, app version numbers, operating system versions, and language settings;
 - d. Complete device access logs showing active and passive connections, device changes, session durations, and timestamps.
3. **IP Address Logs** for the Target Account(s), to include but not limited to:
- a. Comprehensive logs of all IPv4 and IPv6 addresses used to register, access, browse, or interact with the Target Account(s), including login IPs, content interaction IPs, background app activity, and geolocation approximations;
 - b. Port information associated with all IP logs, where available.
4. **Financial & Payment Records**, including:
- a. Subscription history for premium services (e.g. Grindr XTRA, Grindr Unlimited), including purchase dates, billing addresses, payment methods, transaction records, and payment processor identifiers.
5. **Content or Activity Logs / Records of Account Usage** related to the target account preserved or retained by Grindr, LLC., including:
- a. Complete message content for all private chats, including sender, recipient, timestamps, message text, photos, videos, voice notes, GIFs, emojis, stickers, links, and any media shared via chat;
 - b. Match history, including connection requests, accepted matches, rejections, blocks, favorites, and user interactions (with dates/times);
 - c. Profile views, who viewed the Target Account's profile, and when;
 - d. Search history and browsing activity within the app;
 - e. User distance calculations and proximity logs generated by Grindr's location algorithm (distance-based matching logs, not exact coordinates unless preserved);
 - f. Likes, favorites, taps, flames, or other reaction-based activity;
 - g. History of blocked, unfriended, muted, and unblocked accounts.
6. **Moderation, Safety, and Enforcement Records**, including:

- a. User-generated reports against other users, reports submitted against the Target Account(s), safety team investigations, administrative enforcement actions, account warnings, bans, suspensions, or shadow bans;
 - b. Internal moderation logs including blocked content, quarantined photos, abusive behavior flags, policy violation detections (e.g., fraud, catfishing, sexual exploitation, scams), and enforcement outcome records;
7. **Third-Party Integrations**, including:
- a. List of authorized third-party apps connected to the Target Account(s);
 - b. Historical records of granted permissions, scopes of data sharing, revocations, and OAuth transactions.
8. **Security and Account Protection Records**, including:
- a. Password change logs, password reset requests, recovery attempts, and multi-factor authentication enrollment;
 - b. Device security keys, trusted devices, recovery email addresses, and backup contacts;
 - c. Suspicious login alerts, unauthorized access notifications, location mismatch warnings, or high-risk anomaly detections.
9. **Consent, Legal Agreements, and User Policy Logs**, including a complete history of terms of service acceptance, privacy policy agreements, opt-ins, opt-outs, profile disclosures, and community guideline acceptance logs with timestamp metadata.

NOTE: This request includes any deleted, archived, hidden, restricted, or modified content, metadata, or communications that may remain accessible to Grindr through internal retention policies, archival systems, backup infrastructure, disaster recovery storage, or preservation holds initiated pursuant to legal process.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Grindr is a mobile-based social networking and dating application primarily marketed toward members of the LGBTQ+ community. It is operated by Grindr LLC, headquartered in West Hollywood, California. Unlike many traditional social media platforms, Grindr emphasizes proximity-based interaction, connecting users based on their geographic location relative to one another using device-based GPS and location

services. Grindr allows users to create profiles, upload photographs, engage in private messaging, and search for nearby users based on real-time distance estimates.

To create an account, users must register with a valid email address and may also link a mobile phone number. Profiles typically contain a username, display name, profile photographs, a brief biography, and user-selected demographic details such as age, gender identity, sexual orientation, or personal preferences. Users may update their profile information, photographs, and privacy settings at any time. Some users subscribe to paid premium services such as Grindr XTRA or Grindr Unlimited, allowing for expanded functionality, search filters, and profile visibility.

Grindr provides private messaging features that allow users to send text messages, images, audio files, location pins, and other media directly to other users. However, based on my training and experience, as well as information provided by Grindr LLC in response to law enforcement inquiries, I am aware that Grindr does not retain long-term message content or media once messages have been delivered between users. Unlike some other platforms, Grindr's communication is largely device-to-device with minimal long-term server-side storage of chat content. Nevertheless, Grindr does maintain key subscriber, registration, and transactional metadata that may assist law enforcement in identifying account holders and devices associated with criminal activity.

Grindr retains certain server-side information, including:

- Account registration information, including email address, phone number, user ID, profile names, and account creation timestamps;
- Device identifiers (IMEI, IMSI, MAC address, device ID, user-agent strings, app version, and operating system details) logged at account creation or most recent logins;
- IP address logs at registration and most recent login sessions, including timestamps and ports (if available);
- Subscription history for premium services, including billing addresses, payment methods, payment processors (e.g. Apple Pay, Google Pay, Stripe), and transaction records;
- Consent logs related to privacy policies, terms of service agreements, and user acknowledgments.

In my training and experience, Grindr is regularly utilized by offenders for various types of criminal activity including sexual assaults, child exploitation, prostitution-related offenses, fraud, extortion, harassment, and violent targeting of victims based on protected class status. Criminal actors often exploit Grindr's real-time location features, pseudonymous profiles, limited public oversight, and disappearing message capabilities to identify and engage with victims. Due to the limited nature of content retention on Grindr's servers, obtaining subscriber registration data, IP address logs, device metadata, and payment history from Grindr LLC may be critical to identifying suspects,

corroborating victim statements, establishing jurisdiction, tying physical devices to online activity, and demonstrating intent or premeditation in criminal investigations.

Even in cases where content has been deleted by the suspect or is no longer retrievable from the user's physical device, Grindr's centralized account registration records, IP address history, device identifiers, and subscription transactions may serve as valuable evidence to further the investigation.

For these reasons, I believe that the requested records maintained by Grindr LLC concerning the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for Grindr:

Grindr produces *very limited* information for law enforcement compared to other dating applications. It's worth noting that Grindr states:



We do not store users' chat messages (text, pictures, and location). Chat messages are sent directly from device to device, and are not stored on our servers. A user's chat messages are kept on his device for up to 30 days then they are automatically cleared; the user can also manually clear chat history on his device. We do not store changes or historical data, we only have the information as of the last time the user set it or last signed on.

You'll see in the example language we've still included content. Given that Grindr routinely makes CyberTip reports, it appears they *must* have access to some content under certain circumstances.

Summary for Investigators:

OnlyFans is a subscription-based social media platform primarily used for adult content, where creators share photos, videos, and live streams with paying subscribers. While originally intended as a general content monetization platform, OnlyFans has become closely associated with sexually explicit material, with many creators producing pornography or customized content for individual subscribers. Users create accounts using email addresses and usernames, often using pseudonyms or stage names. Creators can interact privately with subscribers through direct messaging, sell custom content, host live streaming events, and accept tips or paid requests. OnlyFans manages payment processing, subscriber billing, and creator payouts, requiring financial information such as linked bank accounts or payment cards to receive funds.

From an investigative perspective, OnlyFans maintains significant backend data useful to law enforcement, including account registration details, IP address logs, device identifiers, financial records, banking details, payout histories, and full messaging histories between creators and subscribers. This platform has increasingly been exploited by offenders involved in human trafficking, prostitution, sexual exploitation, fraud, and extortion. Victims may be coerced into producing content while traffickers control the financial accounts, communications, and payouts. In cases involving minors or coerced victims, OnlyFans' backend data can be critical for identifying controlling parties, locating victims, tracking financial proceeds of illegal activity, and documenting patterns of exploitation over time.

How to Serve with Legal Process:

OnlyFans accepts legal process, including preservation requests and emergency requests, electronically through their law enforcement form:

<https://onlyfans.com/legalinquiry>

Location to be Searched:**Fenix International Limited dba OnlyFans**

Attn: Law Enforcement Relations
9th Floor, 107 Cheapside
London EC2V 6DN

Note: OnlyFans is based out of London (UK) but they **will** comply with US legal demands (without an MLAT or other hoops to jump through) and are actually relatively law enforcement friendly. The challenge you may encounter is whether or not your courts have the authority to (or are willing) to issue a warrant to be served in the UK.

Identify Accounts By:

OnlyFans accounts can be targeted / identified in our legal process by:

- Username
- Profile URL
- Email address
- Legal name
- Telephone number
- Billing address
- Credit card information (must include first six and last four numbers of the credit card, dates and times of suspected transactions, and the legal name of the account holder)

Items to be Seized:

ONLYFANS DATA:

To the extent that the information described is within the possession, custody, or control of OnlyFans (operated by Fenix International Limited), including any records, files, messages, content, logs, metadata, payment information, or deleted materials still available to OnlyFans or preserved pursuant to legal process or internal retention policies, **OnlyFans is required to disclose the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Account username(s), display names, profile names, historical username changes, vanity URLs, and pseudonyms;
 - b. Legal name(s) provided during account creation or payment verification processes;
 - c. Birthdate, age verification documents, government-issued identification submitted for Know Your Customer (KYC) compliance or age verification;
 - d. Account creation date and time, including IP address, device identifiers, and geolocation data captured at registration;
 - e. Email address(es) associated with the account, including historical changes and verification status;
 - f. Mobile phone number(s) associated with the account, including history of additions, removals, or verification;
 - g. Profile photographs, avatars, or other images used in the profile;

- h. Self-reported biography or “About Me” profile text, linked social media accounts (Twitter, Instagram, TikTok, etc.), external website links, or business links provided in profile information;
 - i. IP addresses associated with account deletions, suspensions, or terminations;
 - j. Consent records, terms of service acceptances, privacy policy acknowledgments, community guidelines acceptances, and timestamped consent history.
- 2. **Device Information** related to the Target Account(s), including:
 - a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, hardware IDs, and app installation IDs;
 - b. Push notification tokens (including APNs tokens, Firebase tokens, and any other push token identifiers);
 - c. Browser types, user-agent strings, platform versions, app version numbers, operating system versions, and language settings;
 - d. Complete device access logs showing active and passive connections, device changes, session durations, and timestamps.
- 3. **IP Address Logs** for the Target Account(s), to include but not limited to:
 - a. Comprehensive logs of all IPv4 and IPv6 addresses used to register, access, browse, or interact with the Target Account(s), including login IPs, content interaction IPs, background app activity, and geolocation approximations;
 - b. Port information associated with all IP logs, where available.
- 4. **Linked Accounts & Cross Account Associations** to the Target Account(s), to include:
 - a. Social media accounts linked to OnlyFans profiles, including Twitter, Instagram, TikTok, or any OAuth-connected services;
Any external identity verification services or identity providers used to verify account holder identity.
- 5. **Account Usage, Activity Logs, Content & Communications**, including:
 - a. All published content posted by the Target Account(s), including photos, videos, livestream recordings, captions, stories, highlights, scheduled posts, drafts, archives, hidden media, locked content, and geotagged content;

- b. Direct Message (DM) content including full chat histories, timestamps, media attachments (photos, videos, audio), emojis, stickers, gifts, voice notes, links, and sent/received messages between creators and subscribers;
- c. Live stream session logs, including full video recordings (if archived), participants, chat logs, timestamps, viewer lists, gift transactions, and monetization records associated with live broadcasts;
- d. Content deletion logs, edits, or media removal history, including deletion timestamps;
- e. Saved media, archived content, or private collections maintained by the Target Account(s);
- f. Subscriber lists, followers, subscription history, subscriber join/leave timestamps, and audience engagement logs;
- g. Creator-subscriber interaction logs, including messaging history, custom requests, pay-per-view (PPV) content sales, tip requests, locked message transactions, media unlock history, and sales logs for custom content;
- h. Gifted subscription history, promotions, and discount codes issued;
- i. Content monetization records, including content pricing, purchase history, pay-per-view purchases, subscription fees collected, and custom paid content agreements;
- j. Internal moderation logs reflecting policy violations, reported content, community guideline enforcement, and administrative sanctions;
- k. Reports of abusive content, copyright violations, and third-party reports submitted concerning the Target Account(s);
- l. Browsing history within OnlyFans, including user search queries, profile views, trending content interaction, and promoted content engagement.

6. Financial Transaction Records, including:

- a. Linked bank accounts, routing numbers, account holder names, and financial institution information;
- b. Payment processor records, payout logs, disbursement amounts, held balances, suspended payouts, pending payouts, and frozen funds;
- c. Purchase history for all payments made to the Target Account(s), including subscriber purchases, pay-per-view purchases, tip transactions, and donations received;
- d. Credit card and debit card information provided by subscribers or buyers;
- e. Third-party payment processor identifiers including (but not limited to) Paxum, Wise, or other OnlyFans payment integration services.

7. **Behavioral, Algorithmic, and Personalization Data**, further described as recommendation algorithms, suggested content feed behavior, viewer engagement patterns, content category assignments, audience modeling, user interaction profiles, and trending affinity groups.
8. **Moderation, Safety, and Enforcement Records**, including:
 - a. User-generated reports against other users, reports submitted against the Target Account(s), safety team investigations, administrative enforcement actions, account warnings, bans, suspensions, or shadow bans;
 - b. Internal moderation logs including blocked content, quarantined photos, abusive behavior flags, policy violation detections (e.g., fraud, catfishing, sexual exploitation, scams), and enforcement outcome records;
 - c. Law enforcement preservation requests, subpoena history, emergency disclosure requests, and legal compliance records relating to the Target Account(s).
9. **Third-Party Integrations**, including:
 - a. List of authorized third-party apps connected to the Target Account(s);
 - b. Historical records of granted permissions, scopes of data sharing, revocations, and OAuth transactions.
10. **Security and Account Protection Records**, including:
 - a. Password change logs, password reset requests, recovery attempts, and multi-factor authentication enrollment;
 - b. Device security keys, trusted devices, recovery email addresses, and backup contacts;
 - c. Suspicious login alerts, unauthorized access notifications, location mismatch warnings, or high-risk anomaly detections.
11. **Biometric and Image Verification Data**, including:
 - a. Biometric verification records used for identity verification (facial recognition, facial scans, selfie-based ID verification data, and government ID scans used for compliance verification);
 - b. KYC verification document scans, facial mapping data, and extracted document metadata.
12. **Consent, Legal Agreements, and User Policy Logs**, including a complete history of terms of service acceptance, privacy policy agreements, opt-ins, opt-

outs, profile disclosures, and community guideline acceptance logs with timestamp metadata.

NOTE: This request includes any deleted, archived, hidden, restricted, or modified content, metadata, or communications that may remain accessible to OnlyFans through internal retention policies, archival systems, backup infrastructure, disaster recovery storage, or preservation holds initiated pursuant to legal process.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

OnlyFans is a content subscription platform operated by Fenix International Limited. It allows users, often referred to as "creators," to monetize original content by offering it directly to paying subscribers ("fans") in exchange for subscription fees, pay-per-view charges, or tips. The platform has grown to include a wide variety of content, including—but not limited to—adult material, fitness instruction, influencer content, entertainment, and personal fan interactions. The data maintained by OnlyFans is hosted on servers controlled by the company and remains accessible through lawful legal process such as search warrants or court orders, even if content has been deleted or removed by the user.

Users create OnlyFans accounts by providing personal information including email addresses, verified mobile phone numbers, and government-issued identification for age verification, financial compliance, and Know Your Customer (KYC) requirements. Creators may link their OnlyFans profiles to external social media accounts such as Twitter, Instagram, TikTok, or other platforms to promote content or cross-market to subscribers. Subscriber information may include usernames, display names, pseudonyms, profile photographs, linked social media handles, payment details, linked financial institutions, device information, and extensive account metadata. This profile and registration information can assist law enforcement in identifying individuals responsible for particular accounts, confirming account ownership, and establishing associations with suspects, co-conspirators, or victims.

OnlyFans allows users to post various forms of multimedia content including photographs, videos, audio files, livestreams, scheduled content drops, and private custom content that can be monetized on a per-view basis. This content may include metadata such as upload timestamps, geolocation tags, payment transaction data, and device identifiers that are valuable for evidentiary purposes. In addition to public or subscriber-facing content, OnlyFans provides private messaging functions through which creators and subscribers can exchange messages, images, audio, video, links, and payment requests directly. These direct messages often serve as private negotiation

channels for financial arrangements, custom content sales, or other transactions which may be relevant to criminal investigations.

OnlyFans maintains extensive financial records associated with each account. Creators receive payouts through linked bank accounts or third-party payment processors, while subscribers submit payments through credit cards or payment apps. These financial records may provide critical evidence of monetary transactions linked to criminal activity, including money laundering, fraud, prostitution, human trafficking, extortion, or other illicit financial gain.

In addition to user-generated content and financial transactions, OnlyFans retains comprehensive device metadata, session logs, IP address histories, device fingerprints, security event logs, and suspicious activity alerts which may establish a suspect's identity, location, and device access patterns. The company also maintains records of content deletions, edits, moderation actions, and account suspensions which may demonstrate intent to conceal evidence or obstruct investigations.

Based on my training and experience, I am aware that individuals engaged in various criminal activities may use OnlyFans for the following purposes:

- To advertise or solicit prostitution, human trafficking, or sexual exploitation activities under the guise of “custom content” sales or subscription-based access;
- To facilitate money laundering by structuring illicit proceeds through subscription payments, tips, or payout disbursements;
- To produce or distribute unlawful explicit content, including underage sexual exploitation material or non-consensual pornography;
- To arrange illicit financial transactions masked as legitimate subscription payments, affiliate programs, or influencer marketing partnerships;
- To communicate privately with potential co-conspirators, recruiters, or customers through the platform’s internal messaging features.

Even when suspects delete content, OnlyFans may retain archived content, backups, device logs, account activity, deleted media metadata, and preservation logs. These records are often critical for identifying participants, proving financial transactions, recovering deleted evidence, documenting the full scope of criminal enterprise, and demonstrating a suspect’s planning, intent, and actions.

Because OnlyFans maintains these records on its own servers, independent of any physical device seized from a suspect, the records described herein are often only obtainable through lawful legal process directly served to OnlyFans. For these reasons, I believe that the requested records maintained by OnlyFans concerning the Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for OnlyFans:

Most investigators have heard of OnlyFans – while it is a paywall or subscription based content delivery service for *anything*, it's heavily utilized for explicit photographs / videos and the sale of amateur pornography. From an investigator's standpoint – we see it utilized for the sale of homemade or amateur CSAM (although OnlyFans' strict age verification requirements *does* limit this substantially). It's not uncommon to encounter Human / Sex Trafficking victims producing content *for their trafficker*, who runs OnlyFans accounts for the victim(s) to generate passive income. It's also not uncommon to see *money laundering* through OnlyFans – it's easy to create fake “subscriber” profiles and make fraudulently obtained money look “legitimately” earned through an OnlyFans account (without the records to disprove this, of course).

As mentioned earlier, OnlyFans is based in the United Kingdom. While they do comply fully with US legal process without requiring MLATs or other hoops to jump through, the issue many investigators (particularly local / state) have encountered is the question: Do my court(s) have the authority to issue legal process to a company in the UK? One workaround we've seen is that an argument could be made that it is *served* electronically (via email) in the US – likely within the jurisdiction of the court. But, we won't provide any legal advice. Consult with your local prosecutors or attorney staff to figure out the best way to approach this.

OnlyFans keeps incredible records, frankly some of the best we see with social media productions. They keep *meticulous* records. All content, messages, financial data, is extremely comprehensive.

Regarding identification verification, OnlyFans requires that users who sell content or make money provide tax documents, identity verification documents, photographs, address verification documents, and more. It can be incredibly fruitful with a search warrant.

Regarding financial records, OnlyFans keeps *meticulous* financial records of every penny that moves through their platform: Whether it is passive financial transactions (subscriptions to paywall content), money sent directly for private requests, or “gifts” or “tips” that may be proffered by a subscriber to a content creator.

OnlyFans typically produces records within 14 days.



Summary for Investigators:

Cash App is a widely used peer-to-peer mobile payment service operated by Block, Inc. (formerly known as Square, Inc.). It allows users to send and receive money quickly using a mobile device or computer. Users create accounts tied to unique “\$Cashtags,” email addresses, or phone numbers. Once an account is set up, funds can be transferred instantly between users, linked to bank accounts, debit cards, or even converted into Bitcoin through built-in cryptocurrency functionality. Cash App also offers a physical Cash Card debit card that users can use to make purchases or withdraw funds from ATMs. Many transactions on Cash App occur within seconds, with very limited verification, making it an attractive tool for both legitimate personal use and for criminal actors seeking to quickly move funds.

Because of its speed, ease of use, and limited identity verification, Cash App is frequently exploited in financial crimes. Criminal suspects often use it for schemes involving fraud, identity theft, check scams, drug trafficking, and money laundering. Suspects can easily create multiple accounts using different Cashtags, often with burner phone numbers or fake email addresses, to move money between various parties or to conceal their identity. While the platform appears anonymous on the surface, Cash App retains extensive backend records, including account registration details, linked bank accounts, device identifiers, IP address histories, Bitcoin transaction logs, push tokens, and communications with customer support, all of which can provide critical investigative leads through lawful search warrants.

How to Serve with Legal Process:

CashApp accepts legal process (including **seizure orders**) and preservation letters electronically through their law enforcement portal:

<https://squareup.request.csdisco.com/us/form>

For exigent requests, email lawenforcement@squareup.com and request their Emergency Disclosure Request Form to start the process.

Location to be Searched:

BLOCK, INC.

Attn: Law Enforcement Response Team
1955 Broadway, Suite 600
Oakland, California 94612

Identify Accounts By:

CashApp accounts can be targeted / identified in our legal process by:

- Cashtag (**\$username**)
- Target Email Address(es)
- Target Phone Number(s) *(May or may not work)*
- “Cash Card” debit card number *(Usually not necessary since the Cashtag is usually printed on the physical card)*

Items to be Seized:

CASHAPP DATA:

To the extent that the information described is within the possession, custody, or control of Block, Inc. (formerly Square, Inc., operator of Cash App), including any records, files, transactions, metadata, communications, system logs, and deleted or archived data recoverable via preservation or internal retention systems, Block, Inc. is required to disclose **the following information for the Target Account(s), for the period of January 1, 2025 to the present:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Full legal name(s) provided at registration or account updates;
 - b. Account usernames, \$Cashtag handles, historical handle changes, aliases, and display names;
 - c. Linked email addresses (current and historical), verification status, and modification timestamps;
 - d. Linked mobile phone numbers (current and historical), verification status, and modification timestamps;
 - e. Date and time of account creation with originating IP address and device information;
 - f. Date, time, and details of any account deletion, closure, deactivation, suspension, freezing, or reinstatement events;
 - g. Profile photographs, avatars, Bitmoji or emoji icons, public profile bios, custom status messages, and any self-reported information submitted by the user;
 - h. Linked identification documents (such as government-issued photo IDs) submitted for identity verification (Know Your Customer - KYC compliance);
 - i. Social Security Number (SSN), Taxpayer Identification Number (TIN), or Employer Identification Number (EIN) if provided;

- j. Date of birth, gender, mailing address(es), prior addresses, billing addresses, or shipping addresses provided for cards or payments, submitted by the CashApp customer, or obtained through customer verification methods utilized by Block, Inc.;
 - k. Linked bank accounts, credit cards, debit cards, or financial institution account numbers used for funding, withdrawal, or card transactions, to include full account unredacted card and/or account numbers and issuing banks (if available);
 - l. Any consent logs, legal policy acknowledgments, Terms of Service agreements, Privacy Policy agreements, opt-ins/opt-outs, arbitration agreements, or marketing consent records.
2. **Device Information** related to the Target Account(s), including:
- a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, mobile device IDs, app instance IDs, and push notification tokens (push tokens);
 - b. Operating system versions, application versions, user-agent strings, browser types, platform versions, hardware models, and network types;
 - c. All device logs reflecting usage of the Cash App mobile app, desktop web app, or authorized third-party integrations;
 - d. Device location telemetry (if collected during device registration, app launches, transactions, or fraud monitoring).
3. **IP Address Information** for the Target Account(s), to include but not limited to:
- a. All IPv4 and IPv6 addresses used to access, log into, log out of, or utilize the Target Account(s), including passive telemetry, session start/end timestamps, background sync activity, fraud scoring sessions, and device activity;
 - b. Port data where available;
 - c. IP geolocation approximations derived from network activity.
4. **Payment Transaction Records** for the Target Account(s), including:
- a. Comprehensive transaction history of all peer-to-peer payments, payment requests, payment cancellations, reversals, voids, refunds, failed transactions, and successful transfers;
 - b. Complete sender and recipient information for all transactions, including counterparties' \$Cashtags, names, handles, linked emails, or phone numbers;

- c. Full payment note contents, memos, text messages, emojis, hashtags, links, attachments, or supplemental messages attached to any transaction;
- d. Timestamps, transaction IDs, status updates, and payment source/destination account identifiers (linked banks, debit cards, credit cards, and stored balance accounts);
- e. Cash App Pay merchant transactions, QR code purchases, external vendor payments, and in-store purchase records via Cash App QR services.

5. Bitcoin and Digital Asset Activity for the Target Account(s), including:

- a. Bitcoin wallet activity including purchase, sale, deposit, withdrawal, conversion, and transfer history;
- b. Blockchain transaction IDs, external wallet addresses, blockchain confirmations, and internal ledger records;
- c. Linked custody wallet addresses controlled by Cash App's platform;
- d. Account identity verification records required for digital asset compliance (e.g., "Know Your Customer" documentation specific to Bitcoin services);
- e. Limit increases, compliance flags, suspicious activity reports, and elevated monitoring thresholds related to digital asset activity.

6. Cash Card / Debit Card Activity for the Target Account(s), including:

- a. Issuance records for any Cash Card (physical or virtual) tied to the account, including full or partial card numbers, expiration dates, CVV codes, activation timestamps, shipping addresses, and delivery tracking records;
- b. Full Cash Card transaction history, including merchant names, MCC (Merchant Category Codes), purchase locations, declined transactions, and refunds;
- c. Card freeze, replacement, suspension, lost/stolen reports, and re-issuance logs;
- d. Any Boost discounts, merchant promotional offers, or partner offers activated or redeemed through Cash Card transactions.

7. Business Accounts and Commercial Activity for the Target Account(s), including:

- a. Business profile registrations, Business EIN numbers, or merchant agreements attached to the Target Account(s);

- b. Business transaction logs reflecting invoices sent, payment requests, or payment acceptance under Cash App for Business functionality;
- c. Business fee assessments, payment limits, transaction processing records, and merchant account audit logs.

8. Contact Discovery and Social Graph Data, including:

- a. Uploaded contacts, imported address books, or synced phonebook records submitted by the user for payment discovery purposes;
- b. Contact recommendation data including people suggested by algorithmic matching;
- c. Records of other Cash App users discovered, searched for, or invited by the Target Account(s).

9. Risk Management, Fraud Detection, and Compliance Monitoring Logs, including:

- a. a. Automated fraud scoring data, risk flags, device mismatch alerts, location mismatch detections, and high-risk transaction pattern records;
- b. b. Suspicious Activity Reports (SARs), compliance reviews, OFAC (Office of Foreign Assets Control) screenings, sanctions list checks, or elevated monitoring triggers;
- c. c. Security event logs reflecting unusual activity patterns, multiple device access flags, or login anomalies.

10. Security and Account Protection Data, including:

- a. Password reset history, security PIN changes, recovery attempts, and credential recovery actions;
- b. Two-factor authentication enrollment, trusted device logs, biometric authentication (if applicable), security questions/answers;
- c. Account compromise reports, location mismatch warnings, unauthorized access flags, failed login attempt records, and high-risk event flags;
- d. Records of device locking, remote access revocations, and any security holds applied to the account.

11. Customer Support and Internal Communications, including:

- a. All customer support tickets, user-submitted support requests, internal correspondence with Cash App representatives, chat transcripts, emails, and communications initiated by the Target Account(s);

- b. Compliance investigation communications, dispute resolution records, chargeback processing, refund requests, or fraud investigations.

12. Consent and Legal Agreement History, further described as records of user consent to Cash App's Terms of Service, Privacy Policies, Arbitration Agreements, E-Sign consent, and opt-in/opt-out selections including timestamps of acceptance.

NOTE: This request includes any data, content, or account activity that may have been deleted, archived, modified, or partially retained but remains recoverable to Block, Inc. via internal data retention policies, disaster recovery systems, server-side backups, preservation holds, or system-generated metadata repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Cash App is a mobile payment service operated by Block, Inc. (formerly Square, Inc.), headquartered in San Francisco, California. Cash App allows users to send and receive peer-to-peer payments, conduct financial transactions, invest in stocks or Bitcoin, engage in banking services, and utilize a wide variety of features facilitating the transfer and storage of funds. All user data maintained by Cash App is stored on servers controlled by Block, Inc. and is accessible through lawful legal process such as search warrants, subpoenas, or court orders.

Individuals create Cash App accounts by providing a variety of subscriber information, including their legal names (or aliases), unique Cashtag usernames, verified mobile phone numbers, email addresses, and links to external financial accounts or payment instruments. Based on my training and experience, I know that Cash App allows individuals to associate multiple bank accounts, debit cards, or credit cards for the purpose of funding or receiving transfers. Some users may employ pseudonyms, burner phone numbers, or unverified information when creating Cash App profiles to obscure their true identity.

Cash App provides a wide range of transactional functionality, including:

- Peer-to-peer transfers of funds between users via Cashtags, phone numbers, email addresses, or QR codes;
- Cash App debit card (Cash Card) issuance, enabling physical spending of funds linked to the Cash App balance;
- Direct deposit capabilities for payroll, government benefits, or tax refunds directly

into Cash App accounts;

- Bitcoin purchases, sales, and transfers facilitated within the app;
- Stock trading and investing accounts managed directly through Cash App;
- Business profiles allowing commercial sales, service transactions, and payments for goods or services.
- In addition to transaction records, Cash App maintains extensive logs of account access, including:
 - IP addresses associated with account logins, transactions, and device connections;
 - Device metadata including device IDs, app version numbers, browser user-agents, platform data, and session telemetry;
 - Login timestamps, account creation and deletion logs, password changes, security event logs, and multi-factor authentication records;
 - Linked external accounts, including bank account routing and account numbers, debit and credit card numbers, and external payment providers.

Through my training and experience, I am aware that Cash App is commonly used by individuals engaged in criminal activity to transfer proceeds from illegal conduct. This includes narcotics trafficking, fraud, financial scams, identity theft, prostitution, money laundering, and organized retail theft schemes. Due to its widespread adoption, limited verification requirements, rapid transfer capabilities, and accessibility across mobile platforms, Cash App provides criminal actors with a readily accessible mechanism to transfer funds, conceal financial trails, and avoid traditional banking oversight.

Criminal subjects may utilize multiple Cashtag accounts simultaneously, link or unlink financial accounts strategically, employ virtual phone numbers or VOIP accounts for registration, or rely on networked criminal associates to circulate funds through multiple accounts to obscure the true source or destination of illicit proceeds. However, Cash App maintains comprehensive financial audit trails, account activity logs, device and network metadata, subscriber information, transaction histories, payment instrument linkage data, and security logs that can assist law enforcement in identifying the true parties involved, mapping financial flows, identifying coconspirators, and tracing criminal proceeds.

Even if suspects delete their Cash App accounts, remove linked financial instruments, or attempt to anonymize transactions, Block Inc. retains historical transactional data, account creation metadata, audit logs, and compliance reporting records which remain accessible through lawful process. These records may be essential for reconstructing financial patterns, documenting proceeds of criminal conduct, and establishing a nexus between illicit activity and financial gain.

For these reasons, I believe the records maintained by Block, Inc. related to the identified Cash App account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

Additional Considerations for CashApp:

CashApp keeps incredible records – they are produced as spreadsheets that can easily be sorted or filtered using basic excel functions and tools. *If you aren't too Excel savvy*, check out “Cash Crawler” in the tools section of this manual or your student portal.

CashApp also keeps verification documents. This includes “selfies” uploaded by users and photographic IDs. Because CashApp handles digital money, they are required to abide by pretty stringent verification requirements and recordkeeping requirements.

Expect delays in the production of your records if this isn't a serious case involving life or death. For typical property crimes or fraud, we are seeing about 40-60 day production times. For more serious cases, particularly if you note them when completing the submission form (IE: Child Exploitation, Sales of Fentanyl to Juveniles, Homicide / Armed & Dangerous Suspect, etc.) you will likely receive records in *a few days*. If time is of the essence, I'd consider reaching out to their law enforcement email (lawenforcement@squareup.com) and request they escalate your production.

Seizure orders are typically processed very quickly if you choose “seizure order” when uploading your legal process. See the court orders / seizure language for additional information. Seizing money from suspect's CashApp accounts is *easy*.

Final note – **Sutton Bank** is technically the issuer for CashApp debit cards (CashCards). This is an important thing to remember. For example, if a suspect were to use his debit card at a POS station before committing a shooting in the parking lot – and you obtained records for the POS system – you may end up writing a warrant to Sutton Bank who is going to direct you to write your warrant to CashApp. You'll get there, but it'll take time.



Summary for Investigators:

Venmo is a popular mobile payment application owned by PayPal that allows users to send and receive money directly from their smartphones. Venmo links to users' bank accounts, debit cards, or credit cards, and allows them to transfer funds instantly between individuals using email addresses, phone numbers, or usernames. Unlike traditional banking apps, Venmo incorporates a social component — users can include short descriptions, emojis, or comments with each payment, which are often visible to friends or the public unless privacy settings are adjusted. Many users treat Venmo like a hybrid between a payment service and a casual social feed.

While Venmo was originally designed for personal payments between friends or family, it is frequently exploited by criminals for various forms of financial fraud. Because transactions occur quickly, often without face-to-face contact, and payment notes can be vague or coded, suspects may use Venmo to launder money, facilitate scams, or move proceeds from fraudulent activity with minimal scrutiny. Venmo maintains detailed records of account activity, transactions, device access, IP addresses, linked financial accounts, and payment disputes, all of which can provide critical evidence for law enforcement investigations into fraud, theft, or organized criminal activity.

How to Serve with Legal Process:

Venmo is owned by PayPal. PayPal accepts legal process (including **seizure orders**) and preservation letters electronically through their law enforcement portal:

<https://safetyhub.paypal.com>

Exigent requests are also handled through the above, very user-friendly portal.

Location to be Searched:

PAYPAL HOLDINGS, INC.

Attn: Global Investigations Team
2211 North First Street
San Jose, California 95131

Identify Accounts By:

PayPal (Venmo) accounts can be targeted / identified in our legal process by:

- Account Number (*Likely won't have*)
- Email Address
- Username
- Transaction ID
- Bank (routing number and full account number)
- Credit/Debit Card
- SSN
- Phone Number

Items to be Seized:

VENMO DATA:

To the extent that the information described is within the possession, custody, or control of PayPal, Inc. (Venmo's parent company), including any records, files, messages, content, logs, metadata, or deleted materials still available to PayPal, Inc., or preserved pursuant to legal process or internal retention, PayPal, Inc. is required to disclose **the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include:
 - a. Legal name(s) associated with the account;
 - b. Venmo username(s), display names, vanity handles, historical username changes, retired aliases, and pseudonyms;
 - c. Account registration date and time, including IP addresses and device identifiers captured at creation;
 - d. Verified email address(es), including history of changes, additions, or deletions;
 - e. Verified mobile phone number(s), including verification timestamps, changes, or deletions;
 - f. Physical mailing address(es) or billing addresses associated with the account;
 - g. Linked social media accounts, including Facebook, Google, Apple ID, or other OAuth-based identity providers;
 - h. Profile photographs, avatars, Bitmoji-style icons, or any profile image submitted by the user;
 - i. Consent logs, terms of service acceptances, privacy policy agreements, user agreement acknowledgments, and timestamped acceptance records.

2. **Device Information** related to the Target Account(s), including:
 - a. Device identifiers including IMEI, IMSI, MAC addresses, device fingerprints, user-agent strings, operating system versions, app versions, and browser versions;
 - b. Logs of all devices used to access the account, including device types, model numbers, platform information, and connection histories;
 - c. Push notification tokens registered to any device used by the Target Account(s);
 - d. Device-based location telemetry captured during app usage or login sessions.
3. **IP Address Information** for the Target Account(s), to include but not limited to:
 - a. Full logs of all IP addresses associated with any login, transaction, session activity, app use, web access, or background telemetry;
 - b. IP addresses provided in IPv4 and IPv6 formats with associated timestamps, session durations, and port numbers (if available)..
4. **Linked Financial Account Information**, including:
 - a. Linked bank account information, including routing and account numbers, account holder names, financial institutions, verification dates, and transaction authorizations;
 - b. Linked debit card or credit card numbers, expiration dates, billing addresses, cardholder names, verification history, and changes made to linked payment methods.
5. **Transaction History and Usage Activity** for the Target Account(s), including:
 - a. Complete transaction logs, including sent payments, received payments, payment requests, reversals, refunds, chargebacks, cancellations, and disputes;
 - b. Transaction metadata, including amounts, timestamps, counterparties (payer/payee details), transaction descriptions, notes, emojis, hashtags, and social feed visibility (public, friends-only, or private);
 - c. Transaction status (completed, failed, canceled, reversed, held, disputed, or pending);
 - d. Group payment transactions, shared payments, or split bills;
 - e. Push token logs related to real-time transaction notifications or alerts;
 - f. Saved payment requests, recurring payment setups, subscriptions, or scheduled payments linked to the Target Account(s);

- g. Funding source details for each transaction, including originating accounts or cards used for specific payments.
- 6. **Social and Community Activity** for the Target Account(s), including:
 - a. Public feed posts, social feed visibility settings, profile privacy preferences, and audience settings for each transaction;
 - b. Comment threads on transactions, including comments, replies, mentions, tags, emojis, reactions, and timestamps;
 - c. Contact lists or friend lists, including Facebook-linked friends, imported phonebook contacts, and friend connections established through Venmo's discovery features;
 - d. Records of users blocked, unfriended, removed, or restricted by the Target Account(s);
 - e. Invitations sent to other users or pending contact requests.
- 7. **Risk Management, Fraud Detection, and Compliance Monitoring Logs**, including:
 - a. Automated fraud scoring data, risk flags, device mismatch alerts, location mismatch detections, and high-risk transaction pattern records;
 - b. Suspicious Activity Reports (SARs), compliance reviews, OFAC (Office of Foreign Assets Control) screenings, sanctions list checks, or elevated monitoring triggers;
 - c. Security event logs reflecting unusual activity patterns, multiple device access flags, or login anomalies.
- 8. **Security and Account Protection Data**, including:
 - a. Password change history, password reset logs, recovery attempts, failed login attempts, and recovery credentials used;
 - b. Two-factor authentication enrollment, trusted devices, backup codes, and biometric authentication logs (if applicable);
 - c. Suspicious login alerts, geolocation mismatch flags, fraud detection flags, high-risk account alerts, compromised account notifications, and account lockouts.
- 9. **Customer Support and Internal Communications**, including:
 - a. All communications between the Target Account(s) and Venmo/PayPal customer support, fraud teams, or trust & safety teams;
 - b. Support ticket histories, investigation notes, appeals, dispute resolutions, and administrative actions related to suspicious transactions or fraud

investigations.

10. **Third Party Integrations and Authorized Applications**, including any records of third-party apps connected to Venmo accounts via OAuth authorization, including timestamps of authorization, permissions granted, scopes, revocation dates, and data sharing transactions.

11. **Preservation, Recovery, and Deleted Data**, further described as records of any content, transactions, or accounts deleted, hidden, archived, or disabled but recoverable through internal retention policies, preservation holds, backup systems, or cached storage mechanisms maintained by Venmo or PayPal.

NOTE: This request includes any data, content, or account activity that may have been deleted, archived, modified, or partially retained but remains recoverable to PayPal via internal data retention policies, disaster recovery systems, server-side backups, preservation holds, or system-generated metadata repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Venmo is a widely used mobile payment application owned and operated by PayPal, Inc. Venmo allows users to conduct peer-to-peer financial transactions, transfer funds between linked bank accounts or debit cards, split payments, request money, and maintain ongoing transaction histories. Unlike traditional banking services, Venmo integrates social media-style features into its platform, allowing users to publicly share transaction notes, emojis, hashtags, and payment activity in a real-time social feed viewable by others. The data maintained by Venmo is hosted on servers owned and controlled by PayPal, Inc., independent of any user's physical device, and is accessible to PayPal, Inc. through lawful process such as search warrants or court orders.

Venmo users establish accounts by providing personal identifying information, including full legal names, email addresses, mobile phone numbers, mailing addresses, and linked financial accounts such as checking accounts, debit cards, or credit cards. Each account is associated with a unique Venmo username, display name, and profile image. Users may link their Venmo account to other platforms, including Facebook, Google, or Apple, allowing additional cross-referenced identifying data. Through my training and experience, I am aware that Venmo retains extensive subscriber records including account registration dates, IP address logs, device metadata, phone verification records, and social media connections, which may assist law enforcement in identifying account holders, establishing financial activity, and tracing funds.

Venmo provides multiple interactive features that generate significant records relevant to criminal investigations, including:

- Transaction histories reflecting all funds sent or received, including amounts, transaction descriptions, payment notes, emojis, hashtags, and audience visibility settings (public, friends-only, or private);
- Contact lists, friend connections, and discovery features that allow investigators to identify the financial contacts and peer associations of suspects;
- Linked bank accounts, debit cards, or credit cards providing full account and routing numbers used to fund or withdraw money from Venmo accounts;
- Transaction metadata including timestamps, IP addresses, geolocation data, device IDs, and funding source details tied to each financial transfer;
- Customer service records, including dispute resolutions, fraud alerts, support tickets, and internal risk assessment flags.

Through my training and experience, I am aware that Venmo is routinely used by individuals engaged in criminal activity for various offenses, including narcotics trafficking, financial fraud, money laundering, identity theft, organized theft rings, and online scams. Because Venmo allows for the rapid and discreet transfer of funds using only usernames or contact information, suspects are often able to facilitate illegal financial transactions without needing traditional banking relationships. In many cases, criminal actors will structure payments, utilize multiple accounts, recruit unwitting intermediaries, or leverage Venmo's casual transaction notes to disguise the true nature of the activity. Even when transactions appear to be coded or innocuous, Venmo retains full transactional logs, payment requests, messaging history, and device information that allow investigators to reconstruct financial flows, identify conspirators, and trace proceeds of criminal activity.

Venmo also maintains extensive security logs, including password reset histories, failed login attempts, two-factor authentication enrollments, device recognition logs, push notification token records, and suspicious login alerts that can further corroborate suspect identities or link physical devices to financial transactions. While criminal actors may attempt to conceal their identity through the use of burner phones, pseudonymous usernames, or VPNs, Venmo's server-side records — including IP address logs, device fingerprints, funding sources, and OAuth-linked accounts — often allow investigators to overcome these concealment tactics.

In my experience, records maintained by PayPal, Inc. (Venmo) serve as a critical evidentiary resource for law enforcement, particularly in financial fraud investigations where quickly tracing the flow of illicit funds is essential. Even if a suspect's phone or computer is seized, reset, or wiped, Venmo's centralized records remain accessible through lawful legal process. The records maintained by PayPal, Inc. may provide the only comprehensive historical view of a suspect's financial activities, associations, and criminal conduct.

For these reasons, I believe that the requested records maintained by PayPal, Inc. related to the identified Venmo account(s) will contain evidence, fruits, and instrumentalities of violations under investigation.

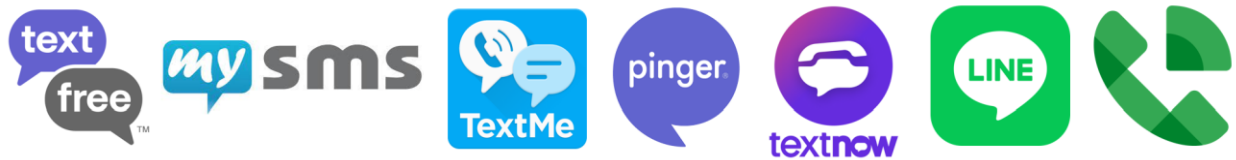
Additional Considerations for Venmo:

Venmo keeps good records, not quite the same caliber as CashApp, but still incredibly useful. Venmo records are produced as spreadsheets that can easily be sorted or filtered using basic excel functions and tools.

Venmo also may have verification documents. This includes “selfies” uploaded by users and photographic IDs. Venmo typically doesn’t include them in search warrant productions, even if requested. If they are useful for your case and you requested them in your warrant, and did not receive them, email lawenforcement@paypal.com for assistance in obtaining them.

Seizure orders are typically processed very quickly if you choose “seizure order” when uploading your legal process. See the court orders / seizure language for additional information. Seizing money from suspect’s Venmo accounts is easy.

TEXT MESSAGING APPLICATIONS / VOIPS



Preface / Author's Note:

There are an overwhelming number of text messaging and VOIP applications available today, many of which operate in similar ways. No single platform stands out as being universally more common for criminal use, as offenders may utilize virtually any application to facilitate illegal activity. Rather than attempting to provide individualized legal language for each service, this guide offers generalized affidavit and search warrant language that can serve as a foundation applicable to most text messaging and VOIP platforms.

However, investigators must recognize that each application may vary significantly in its features, the types of data it collects, its data retention practices, and how it responds to legal requests from law enforcement. Therefore, it is essential that investigators familiarize themselves with the specific service being targeted and review any available law enforcement guidance or compliance documentation provided directly by the platform.

For additional guidance on identifying the specific text messaging or VOIP application associated with a phone number — particularly when routing information leads to providers such as Bandwidth.com or Inteliquent — investigators should refer to the **“VOIP / Texting App Quick Reference Guide”** available in the GBG Consulting, LLC. student portal.

Summary for Investigators:

Standalone texting applications such as TextNow, TextFree, Pinger, Sideline, Burner, and others allow users to obtain a phone number not tied to a traditional cellular subscription. These apps provide VOIP-based texting, calling, and voicemail services over Wi-Fi or mobile data, enabling users to create multiple phone numbers, often anonymously, using only an email address or basic registration information. These apps are widely exploited by criminals seeking to avoid detection, maintain disposable communication channels, or compartmentalize criminal communications (for example: drug trafficking, fraud schemes, harassment, child exploitation, or prostitution-related activity). Because these applications are internet-based, they are often used even without an active cellular plan, making them popular for burner devices, tablets, or secondary phones.

Many suspects utilize standalone text messaging and VOIP applications such as **TextNow, TextFree, Sideline, Pinger, Hushed, and similar services** because they believe these platforms offer them greater anonymity. These applications allow users to generate phone numbers quickly without requiring a traditional cellular carrier, physical SIM card, or lengthy account verification. As a result, offenders often believe they are using a number that cannot be easily traced back to them. In many cases, they view these services as a free or inexpensive alternative to purchasing physical “burner” phones, allowing them to maintain multiple disposable numbers while avoiding the cost and exposure associated with purchasing new devices.

However, in practice, these applications often collect and retain detailed subscriber records, registration data, IP address logs, device identifiers, and—in many cases—extensive message content. Unlike major cellular carriers who may only retain limited text message content (or none at all), these third-party text apps frequently store full chat histories, attachments, call logs, and other metadata on their servers for extended periods, especially when users do not actively delete their content. As such, legal process served directly to these providers may yield highly valuable investigative evidence that might otherwise be unavailable through standard carrier records. In some cases, these platforms may retain more actionable content than what law enforcement can obtain from the suspect's wireless carrier, providing full conversations, contact lists, media files, and IP-based location data that directly identify and implicate suspects.

How to Serve with Legal Process:

Check the search.org ISP list for information on how to serve the specific application you are looking at with legal process, information on the location to be searched for your warrant, and for law enforcement information and guides.

Identify Accounts By:

Typically, when writing to Texting Apps and VOIPs, you’ll be writing for it by **phone number**. For many applications though, you may also be able to write to the application by email address or other unique identifiers.

Items to be Seized:

VOIP / TEXT MESSAGING APPLICATION DATA:

To the extent that the information described is within the possession, custody, or control of the provider, including any records, files, logs, content, metadata, or deleted materials still available to the provider or preserved pursuant to legal process or internal retention policies, **the provider is required to disclose the following information for the Target Account(s), for the time period of January 1, 2025 to the date this search warrant is signed:**

1. **Subscriber Information** for the Target Account(s), to include by way of example (but not limited to) the following items:
 - a. Account username(s), handles, screen names, display names, or vanity names associated with the account(s);
 - b. Full legal name (if provided), aliases, nicknames, and self-reported identifiers;
 - c. Account creation date and time, including IP address and device identifiers at time of registration;
 - d. Account deletion date and time (if applicable), including any linked IP addresses or device identifiers;
 - e. Mobile phone number(s) linked to the account, including all historical phone numbers previously used;
 - f. Email address(es) associated with the account, including historical email changes, verification status, and prior addresses;
 - g. Any profile photo, avatar, or profile image associated with the Target Account(s);
 - h. Date of birth, gender, location (if self-reported), time zone, language preferences, or other demographic data;
 - i. Payment, billing, or subscription records if premium services were utilized, including payment methods, billing addresses, and financial account identifiers;
 - j. Consent logs, user agreement acceptances, terms of service agreements, privacy policy acceptances, community guidelines acceptances, and any timestamped consent history.
2. **Device Information** related to the Target Account(s), including:
 - a. Device identifiers including IMEI, IMSI, MAC address, device ID, hardware IDs, or device fingerprints;
 - b. Logs of all devices associated with, linked to, or accessing the account(s), including device connection histories;
 - c. Browser user-agent strings, operating system versions, application versions, and platform identifiers captured at login;
 - d. Push Notification Tokens registered to any devices linked to the account.
3. **IP Address Logs & Records, including:**
 - a. Complete logs of all IP addresses used to register, access, utilize, message, call, or otherwise operate the Target Account(s);

- b. IP addresses provided in both IPv4 and IPv6 format, including associated port information where available;
 - c. Session connection timestamps, session durations, passive telemetry, and app update activity.
- 4. **Account Linking and Cross-Account Associations** for the Target Account(s), to include:
 - a. Accounts registered using shared email addresses, phone numbers, device fingerprints, browser identifiers, cookies, or shared session IDs;
 - b. OAuth integrations and external accounts linked via Google, Apple, Facebook, or other third-party login providers;
 - c. Internal linkage or association logs indicating additional accounts likely operated by the same user or device.
- 5. **Usage Logs, Activity, Communications, and Content** for the Target Account(s), including:
 - a. Full message content of all inbound and outbound messages, including text messages, multimedia messages (MMS), photos, videos, voice notes, files, attachments, emojis, stickers, GIFs, and embedded links;
 - b. Message metadata including message IDs, timestamps, sender/recipient information, delivery status, read receipts, deletion flags, and editing history;
 - c. Complete call history, including inbound/outbound calls, timestamps, durations, participant identifiers, call status, and any associated metadata;
 - d. Voicemail content, voice memos, voice recordings, and audio files transmitted through the service;
 - e. Saved, archived, or draft content not transmitted but stored within the account;
 - f. Contact lists uploaded, synced, or stored within the account(s), including saved names, phone numbers, emails, and address book integrations;
 - g. Call logs and messaging logs associated with any third-party VoIP services integrated into the account platform (if applicable);
 - h. Deletion logs reflecting messages, files, calls, or media that have been deleted, including timestamps of deletion events;
 - i. User reports, abuse complaints, moderation flags, or administrative actions taken on the Target Account(s).
- 6. **Location Data**, if retained, including IP-based location approximations, GPS coordinates, Wi-Fi proximity, Bluetooth beacons, or other geolocation data

collected or inferred through device usage, login activity, or background app processes.

7. Security and Account Protection Data, including:

- a. Password change history, password reset logs, recovery attempts, and recovery credentials;
- b. Two-factor authentication enrollment, trusted devices, recovery codes, or biometric authentication credentials (if applicable);
- c. Security alerts, login anomaly notifications, device mismatch flags, suspicious login alerts, or compromised account warnings.

8. Third Party Integrations (if applicable), including:

- a. List of authorized third-party apps connected to the Target Account(s);
- b. Permission scopes granted to third-party apps, timestamps of authorization and revocation, and data shared between apps.

9. Consent and Legal Agreements, including all versions of Terms of Service, Privacy Policies, User Agreements, or Community Guidelines consented to by the Target Account(s), with associated timestamped logs.

NOTE: This request includes any information described above that may have been deleted, modified, or archived but remains accessible to the provider through internal backups, system retention, disaster recovery processes, preservation holds, or metadata repositories.

Affidavit Language:

Based upon my training, experience, and consultation with other investigators, as well as information obtained during this investigation, I believe the following to be true:

Text Messaging and VOIP (Voice Over Internet Protocol) applications are widely used communication platforms which allow users to create telephone-like accounts that operate independent of traditional cellular service providers. These services allow users to obtain telephone numbers, send and receive text messages, place or receive phone calls, and communicate through multimedia messaging over internet-based infrastructure. Many of these platforms are accessible via mobile apps, desktop applications, or web-based portals, and operate without the need for users to possess an active mobile carrier subscription. The data maintained by these providers is hosted on remote servers, owned and operated by the companies themselves, and remains accessible through lawful legal process, such as search warrants or court orders.

Users typically create accounts by providing an email address and/or phone number, though many applications allow registration using pseudonyms, burner emails, or other non-verified information. Account identifiers may include user-selected screen names, display names, and assigned telephone numbers issued by the provider. These applications often attract users who seek anonymity, cost savings, or convenience by allowing them to obtain temporary or multiple phone numbers without purchasing burner phones or contracting with cellular carriers. However, despite the perceived anonymity, providers often retain detailed subscriber information, account activity logs, IP address histories, and device identifiers capable of linking suspects to their true identities and devices.

In addition to basic messaging, most VOIP/Texting applications allow for multimedia messaging features, including the ability to send photographs, videos, voice recordings, location pins, GIFs, and other attachments. Many platforms also support group chats, file transfers, voicemail recordings, and allow integration with a user's existing contact lists, further extending the user's communication network. Law enforcement investigations have frequently revealed that suspects engaged in criminal activity utilize these applications to communicate with co-conspirators, arrange transactions, recruit participants, or coordinate illicit conduct while believing their activity is concealed behind disposable phone numbers or pseudonymous accounts.

In my training and experience, these providers routinely maintain detailed technical records that may assist law enforcement in criminal investigations, including:

- Complete logs of inbound and outbound text messages, calls, and multimedia messages, including timestamps, message content, sender and recipient information, and associated metadata;
- Call logs including call durations, participants, timestamps, call types (inbound/outbound), and any associated voicemail content;
- IP address histories showing locations where accounts were accessed, including passive telemetry, app sessions, background activity, and device logins;
- Device identifiers including IMEI, IMSI, MAC addresses, user-agent strings, app versions, device fingerprints, and operating system data;
- Contact lists uploaded or synced from the user's mobile device, including names, phone numbers, and email addresses;
- Third-party app integrations, if authorized by the user, which may reveal additional cross-platform linkages to external services;
- Payment or subscription records if the user engaged in premium services or upgraded features;
- Content deletion logs and audit trails indicating when users attempted to delete or modify account data or communications;
- Security logs showing password resets, two-factor authentication enrollments, login anomalies, account recovery efforts, or unauthorized access flags.

Even if users attempt to delete content, many of these providers retain records through internal backups, preservation holds, disaster recovery systems, or system-generated metadata repositories. These retained records may preserve critical evidence of criminal activity, even after users believe messages have been deleted or accounts deactivated.

In my experience, the records maintained by these third-party Text Messaging and VOIP providers often serve as a vital investigative resource for identifying suspects, corroborating witness statements, reconstructing timelines, recovering deleted evidence, identifying financial transactions, and mapping criminal networks. Because these records are maintained directly by the service providers and not stored solely on a suspect's physical device, lawful process served directly to these companies is often the only means of obtaining this historical evidence.

For these reasons, I believe that the requested records maintained by the provider related to the identified Target Account(s) will contain evidence, fruits, and instrumentalities of the violations under investigation.

OTHER SOCIAL MEDIA PLATFORMS: WHAT TO DO

At this point, we've covered many of the major platforms that law enforcement most commonly encounters in criminal investigations. However, technology constantly evolves, and there will always be cases involving niche, emerging, or lesser-known applications that aren't included in this guide. Investigators may encounter new platforms, foreign-based services, or specialty apps tied to specific subcultures or criminal communities. For that reason, it's critical that investigators develop the skills to become subject matter experts in *any* application they encounter.

Why Do I Need to Become an Expert?

First and foremost, remember that an “expert” is somebody who knows more than the average person, in the eyes of the court. If a majority of the population knows *nothing* about “that application,” and you know enough to confidently talk about it, you **are** an expert. We need to be “experts” for the purpose of:

- Effectively writing legal process (knowing *what* to ask for, specifically);
- Explaining the social media platform within your warrant affidavits;
- Understanding the data you get back;
IE: If an application like Snapchat has a feature called “Memories” and you get back files titled “Memories,” if you didn’t know what a memory was, you’d have no idea what exactly you were looking at and why the platform has it.
- Testifying on your social media evidence.

Resources to Learn About An Application:

- **Visit the Platform’s Website**
Most social media platforms will have a website which breaks down various features of the platform and can provide you some basic information to further your knowledge on the platform.
- **Visit the Platform’s Law Enforcement Webpage (if available)**
Many social media platforms have webpages specifically for law enforcement seeking information. Try a Google search for “[Platform Name] Law Enforcement Information” or you may find it linked from Search.org’s ISP list (see below).
- **Review the Platform’s Law Enforcement Guide (if available)**
Many social media platforms have PDF guides intended for law enforcement that aren’t distributed publicly. These may be available from a Google search for “[Platform Name] Law Enforcement Guide,” Search.org, or KLoing (see below).
- **Check the Platform’s Privacy Policy**
Nearly every social media platform will have a privacy policy. It’ll be long and

wordy, but it will also likely list out all the data they collect about their users. If the platform is collecting this data, we can likely obtain it through legal process.

- **Search.org's ISP List** (<https://www.search.org/resources/isp-list/>)
A valuable resource which can give you some basic information on various platforms and providers, specifically how they accept legal process, how to address your legal process and serve them, and oftentimes information on what they may or may not be able to provide you. They also have a large collection of law enforcement guides from various platforms.
- **Check KLove's Law Enforcement Forum** (<https://groups.io/g/kloving>)
An unbelievably useful resource for law enforcement (verified LE or civilian staff only). Within the files section you'll find thousands of templates, including an entire section packed full of law enforcement guides.
- **Check the NDCAC Website** (<https://ndcac.fbi.gov/le-portal>)
Another incredibly useful resource accessible through LEEP for verified law enforcement personnel. They have a breakdown of *a ton* of social media applications with a lot of valuable information for investigators.
- **Conduct Online Research**
There are many guides, websites, and YouTube videos that can introduce you to an application and show you the various features. Try a Google or YouTube search for "how to use [platform name]," you'll be surprised how much information is out there and accessible to you.
- **Talk to Somebody Who Uses It**
If you're working a victim case and the crime occurred after the victim communicated with the suspect on [insert platform name here], *who better* to teach you about the application than your victim? Instead of just saying "Oh, they communicated on [platform]" and following up with your own research – if you don't know anything about it, start asking questions. "What is [platform]? How do you use it? What features does it have? Can you *show me*?"
- **Download the Application**
There's no better way to learn about an application than actually downloading it yourself and messing around with it. Create a fake profile, have your partner do the same, and spend some time trying out the various features. Now, you don't only have "training" but you have "experience" and you can tell a judge and a jury that you've actually used the application before. This will give you a newfound sense of confidence with most applications you're unfamiliar with.

By taking the above-described steps, you'll establish your training and experience with nearly *any* social media platform and be prepared to write your first legal process to it.

What Should I Ask for in my Search Warrant?

A common question – “Okay, so I’ve become an expert, but now I’m trying to write a warrant and I don’t know what to ask for?”

You are likely *not* the first investigator to write a search warrant for *that platform*. If the language isn’t included within this guide and you don’t have any templates from other investigators, check **KLoving’s Law Enforcement Forum**. There are *thousands* of templates available there. And if you can’t find one, **make a post** and ask. More than likely, somebody (or multiple investigators) will gladly send you a template to work from.

If that doesn’t work, and you can’t find a template elsewhere (NDCAC, other sources), **you may have to craft your own.**

When writing a search warrant for an application you’re not familiar with, reference their law enforcement guides or privacy policies to identify information the provider(s) likely possess that you may want to ask for.

Effective Use of AI: I respect that some investigators aren’t “on board” with ChatGPT or similar AI tools – but *this* is something AI is very good at. You could prompt ChatGPT to help you write a search warrant to [PLATFORM] and it will give you a starting point to work off. Be aware, ChatGPT will oftentimes write warrant language that may leave out important features to your case, or it may say things that aren’t *entirely* accurate in affidavit language, so be sure to double check anything AI generated and avoid “copy and pasting.” There *is* a way to *ethically* use AI – but don’t over rely on it.

COURT ORDERS: SOCIAL MEDIA PEN REGISTERS

Pen Registers (*Pen Register / Trap Trace, abbreviated PRTT*) are useful tools with the “big 3” social media platforms: Facebook, Instagram, and Snapchat. Some other providers may be capable of installing *some form* of pen register, and many provides cannot. A great resource to use to get more information on PRTTs and your targeted platform is NDCAC.

A social media PRTT is *different* than what we receive from cellular providers, but the **concept** is the same – a PRTT produces data for us, *prospectively (in the future)*, on an ongoing basis. Here’s what we may get with a social media PRTT:

- Changes to Accounts / Subscriber Information
- Message Headers (Who are target is messaging?) **without content**
- IP Address Logs (All captured IP addresses from account activity)
- Account Activity (Posts, Story Posts, Snaps, Etc.) **without content**

These will be produced every 15-30 minutes, depending on the provider. Essentially you’ll get an email with a data production you can download to review.

A social media PRTT, particularly to Snapchat (and Facebook on a more substantially limited scale) can also provision **location data** if your target has location services enabled. You’ll get an email every 15-30 minutes with your target’s location. *Imagine getting an email every 30 minutes with where your target has been the last 30 minutes from Snapchat.*

California Pen Registers & Location Data Issue:

It’s worth noting that California Penal Code § 638.52(c), the authority for issuing PRTTs, specifically states “a pen register or trap and trace device **does not include** any device or process used **to obtain the contents of a communication or to obtain the location of an individual or device.**” Yet, social media providers won’t typically respond to “ping” warrants and will require a PRTT be installed to provision location data.

Here’s the workaround: Your court order will be a combination of a PRTT, as authorized by Penal Code § 630, *and* a prospective location data (tracking) warrant, as authorized by Penal Codes §§ 1524(a)(12), 1534. **This works.**

Court Orders for PRTT Installation:

IT IS ORDERED that, in compliance with **California Penal Codes §§ 638.50–638.59**, **[PROVIDER]** is to install a Pen Register / Trap Trace Device on the target account(s), and produce **the following data**, on an ongoing basis **every 15 minutes**, for a period of **60 days**:

- Changes to subscriber information (usernames, phone numbers, emails, etc.);
- Records or Logs of IP addresses and ports used to access the account;
- Message headers (not content) such as to/from usernames, timestamps;
- Device/session identifiers and push tokens;
- Records of account activity (not content).

IT IS FURTHER ORDERED that, in compliance with **California Penal Codes §§ 1524(a)(12) and 1534**, **[PROVIDER]** shall provide close to real-time **location data** on an ongoing basis, every 15 minutes, for a period of 30 days, including:

- GPS coordinates or geolocation data;
- Wi-Fi/cell tower-based location;
- All other available location metadata within any log or record.

California Requirements:

California Penal Code language also requires we include the following within the orders:

This request complies with **California Penal Code § 638.52**, which provides:

"An application for a court order authorizing or approving the installation and use of a pen register or a trap and trace device shall be made in writing under oath or equivalent affirmation by a peace officer and shall include the identity of the peace officer making the application and the identity of the law enforcement agency conducting the investigation."

As required by § 638.52(b), the following are provided:

- **Peace Officer:** Detective [Your Full Name], [Badge #];
- **Law Enforcement Agency:** [Full Agency Name, Division, Address];
- **Identity of Subject (if known):** "[USERNAME]", believed to be operated by [FULL NAME], DOB [DOB];
- **Nature and Purpose of Investigation:**
Investigation into violations of [e.g., H&S §11351 – Possession for Sale of a Controlled Substance]. The social media account "[USERNAME]" is used to coordinate criminal activity, including narcotics sales, by obscuring user identity and enabling encrypted messaging.

- **Statement of Offense:**
Violations include [Primary Offense – e.g., H&S §11351], [Optional: PC §182 (Conspiracy), PC §136.1 (Witness intimidation), etc.]
- **Certification (PC § 638.52(d)):**
"I certify that the information likely to be obtained by the installation and use of the pen register and trap and trace device is relevant to an ongoing criminal investigation."

Affidavit Language for Social Media PRTT:

This is just an example. You'll want to tailor this to your investigation and whatever social media platform you are targeting (IE: Snapchat, Facebook, etc.).

Based on my training and experience, I know that social media platforms maintain metadata and routing information related to user communications, which can be obtained via a court-authorized pen register and trap and trace order pursuant to California Penal Code §§ 638.50–638.59. While the traditional concept of a pen register involves the collection of phone numbers dialed or received, in the context of social media and encrypted messaging services, this typically includes non-content information such as IP addresses used to access the account, timestamps of logins and logouts, session identifiers, and metadata regarding communications sent and received, such as the usernames or handles of other users contacted and the times those messages were exchanged.

Social media providers generally comply with pen register/trap and trace orders by furnishing connection logs and routing metadata in real or near-real time. These records do not contain the content of messages or media shared but are crucial in identifying a suspect's location, access patterns, communication frequency, and potential co-conspirators.

Based on my training and experience, this information is often the only available method to track anonymous users who operate through usernames or app-specific identifiers instead of phone numbers. In prior investigations, pen register data from social media platforms has provided key leads in identifying suspects, establishing probable cause, and locating devices in use.

This request is limited to metadata and routing information and does not seek the content of communications. The information requested is consistent with the permissible scope of a pen register and trap and trace device under California law.

It's difficult to provide an effective template for these because *every jurisdiction* handles them a little differently. I suggest using this sample language and working with your local prosecutors or attorney staff to craft a social media PRTT that works best for you.

COURT ORDERS: SEIZURES FROM P2P PAYMENT APPS

We won't get into the legal authorities to seize money (asset forfeiture, criminal profiteering, restitution, etc.) because it varies from state to state and what you're specifically investigating – that's something you'll want to work with your prosecutors on.

Instead, let's look at the technicalities of seizing money from Peer to Peer Payment Applications like CashApp, Venmo, PayPal, or even online banks.

It is **EASY** to seize money from P2P Payment Applications. Consider whether you want to:

- **Freeze** the money (lock down the account so it can't be moved), review the records, and then follow up with a seizure warrant, **or**
- **Seize** the money immediately.

If you want to **FREEZE** the money, insert the following orders into your legal process:

IT IS ORDERED that **[PROVIDER]** is to **FREEZE AND HOLD ALL FUNDS** currently held in the target account(s). The provider shall place said funds into a separate account which prevents access by the suspect(s) in this investigation, or utilize reasonable methods to preserve the funds and restrict access to the account by account holders.

IT IS FURTHER ORDERED that the seized funds in the target account(s) **SHALL NOT** be released until a court order is received directing the release or disposition of the funds. Any questions may be directed to **[INSERT NAME / CONTACT INFO]**.

If you want to **SEIZE** the money, insert the following orders into your legal process:

IT IS ORDERED that **[PROVIDER]** shall immediately identify and disclose to law enforcement the total balance of funds, credits, cryptocurrency holdings, or other monetary assets currently maintained in the account.

IT IS ORDERED that **[PROVIDER]** is hereby directed to fully liquidate, transfer, and remit the total balance of all seized funds, up to the full amount available, directly to the following seizing law enforcement agency for placement into a law enforcement seizure account, pending further disposition:

[AGENCY CONTACT INFO HERE]

Typically, these platforms will send you a Cashier's Check. It's **that easy** (usually).

COURT ORDERS: OUT OF STATE WARRANTS TO CA

A majority (but certainly not all) the social media providers we deal with regularly are based in California, yet law enforcement agencies in the other 49 states will likely need records or data from these providers at some point.

Most platforms will produce the data without issue, *however*, some platforms may object or refuse to comply on the grounds of jurisdiction. They may challenge whether or not your court has the authority to issue a warrant to an out of state corporation. **Take Life360 for example:** They routinely refuse to comply with legal process from law enforcement agencies outside of California.

California Penal Code § 1524.2(c)(1):

Penal Code Text: “A California corporation that provides electronic communication services or remote computing services to the general public, when served with a warrant issued by another state to produce records that would reveal the identity of the customers using those services, data stored by, or on behalf of, the customer, the customer’s usage of those services, the recipient or destination of communications sent to or from those customers, or the content of those communications, shall produce those records as if that warrant had been issued by a California court.”

What It Means: Any social media or technology provider operating in California (the definition of “electronic communication services” is very broadly defined in Penal Code 1546) are required, by state law, to comply with out of state warrants “as if it were issued by a California court. So, arguably, **this shouldn’t be an issue**. Even if you are not a California peace officer, if you’re writing to a California provider, consider citing this Penal Code in your legal process and bringing it to the provider’s attention.

Registered Agent of Service:

Please consider that nearly all national companies have a **Registered Agent for Service of Process** in each state. That agent can usually be found by either searching your Secretary of State’s online database or contacting the legal department of the target company. *You may be able to serve your Search Warrant on the agent in your state.* If you use a local agent, we also recommend sending a courtesy copy directly to the target company at their preferred FAX, email or web portal with a cover letter that explains the dual-service. (Source: Santa Clara DA’s Office)

Domestication:

The final option if those don’t work is to have a peace officer in the state where you are trying to serve the warrant **domesticate** your warrant. You’ll get in contact with a District Attorney Investigator or Detective in the jurisdiction where the provider is, supply them with your affidavit, and they will attempt to obtain a California search warrant for you. This is usually unnecessary, but some providers will insist on it.

COURT ORDERS: CALIFORNIA TIME OF COMPLIANCE

A common issue that law enforcement gripes about when discussing social media investigations is *unnecessary delays* in waiting for provider records once they are served with legal process. Take **CashApp** for example: they may keep us waiting up to 60 days. Meta Platforms may take a month. Sometimes, these waits are *unacceptable* because of the facts of our case, urgency for public safety, or can seriously jeopardize our ongoing criminal investigations due to the delay.

California Penal Code § 1524.2(b)(1):

Penal Code Text: “When properly served with a search warrant issued by the California court, a foreign corporation subject to this section shall provide to the applicant, all records sought pursuant to that warrant **within five business days of receipt**, including those records maintained or located outside this state.”

Clarification: Penal Code §1524 defines a “foreign corporation” as “any corporation that is qualified to do business in this state.” Note that while many social media providers are based (and served with legal process in California), they tend to be incorporated in Delaware or states with more ideal tax laws.

What It Means: Any social media or technology provider “doing business” in California is required, by state law, to produce records within five business days. *The Penal Code even allows us to shorten that, if the facts of the case support it.*

Cite This In Your Legal Process: We should be putting this language in our legal process, and when uploading it to law enforcement portals specifying a due date.

It’s Been 5 Days and I Don’t Have Records (But I NEED Them ASAP):

Follow Up with the Provider: The first step is to contact the provider *on Day 6*. Explain why it’s important, point out the Penal Code requirement they produce the records in 5 days (cite it in your email), and ask them to expedite their production. This *may or may not* work – sometimes they just reply “we process legal process in the order received.”

Work with the Prosecutor: Sometimes, an email from the prosecutor carries a lot of weight. Ask your prosecutor to send the provider an email and explain if they *don’t* produce records, they’ll follow up with an “Order to Show Cause” hearing.

Order to Show Cause: Your prosecutor can calendar a hearing to call the social media provider into court, and have their attorneys explain to the issuing judge *why* it’s taking so long to produce records. Oftentimes, before that hearing, you’ll get your records.

I Don’t Work in California:

Consult with your prosecutors to see if your state has a similar law, *or* if it’s possible to have a judge order a “due date” within the orders of your legal process given the facts of your specific investigation and why the records are time sensitive.

TOOLS & RESOURCES

Reviewing and sorting through the returns for nearly *every* social media provider can be done without *any tools or software*, but *oftentimes* these tools can make our work analyzing productions and searching for evidence far more efficient and easier.

We'll avoid recommending *any specific tool* – it seems that through training we've learned that some people prefer certain tools more than other people. Instead, we'll just share some of the available tools to consider. Some are free, and others are paid.

Because links to software and tools can change, **check the GBG Consulting, LLC. student portal for links to any of these tools**. Some are *download links* and others will take you to the provider's website where you can download it or purchase it (for the paid options)

FREE TOOLS & SOFTWARE



BadgeApps offers a free tool called **Aaron's Maps for Police** which can map out social media location data (and other location data such as cell records).



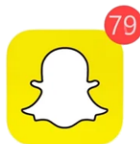
North Loop Consulting offers a few useful free tools for law enforcement, my favorite is **Cash Crawler** which is a tool for analyzing CashApp data productions.

.social

Free software available from the NDCAC which allows you to easily parse social media data productions from a number of different providers and applications.

RIPT

Another free tool offered by NDCAC which allows you to ingest large batches of IP addresses obtained from social media providers and identify ISPs from them.



SNAPCHAT CONVERSATION PARSING TOOL

Free tool from Detective Mike Smithey (Iowa City Police Dept) that can ingest Snapchat returns and display it in a little webpage that's easy to review.



Free tool that can download videos from YouTube, Facebook, TikTok, Tumblr, Vimeo or Twitch (and more).



ChatGPT

Open source AI tool (free or paid subscriptions) that can help with *tons* of tasks for our investigations.

PAID RESOURCES, TOOLS & SOFTWARE



Warrant Builder is a paid service used by numerous law enforcement agencies which can easily generate search warrants for most providers.



Famety.com offers great resources when creating undercover accounts. You can purchase friends, followers, likes, comments, etc. on multiple platforms.

PAID TOOLS / SOFTWARE FOR PARSING SOCIAL MEDIA DATA PRODUCTIONS

The following paid tools can be utilized to parse, analyze and review social media data productions (among other evidence such as cell phone data, Apple, Google, cell records, etc.). They are each different in their capabilities and features. If you're interested in purchasing one for your agency, I'd recommend trying out a few to see which works best.



MAGNET AXIOM®



LEADS ONLINE
NIGHTHAWK

PAID TOOLS / SOFTWARE FOR MAPPING / ANALYZING SOCIAL MEDIA LOCATION DATA

The following paid tools can be utilized to upload, parse, **map** and analyze social media geolocation data (among other evidence such as cell records, etc.). They are each different in their capabilities and features, **but I believe every agency should have access to one of these tools**. If you're interested in purchasing one for your agency, I'd recommend trying out a few to see which works best. **Note: PenLink (above) does this too.**



Accurint® TraX™
(Formerly ZetX)

OTHER TOOLS FOR SOCIAL MEDIA INVESTIGATIONS

If you are aware of other useful tools for social media investigations, or created one, please **contact us** so we can add it to our handbook and student portal!

CONCLUSION

The digital landscape is constantly evolving, and with it, so are the methods criminals use to communicate, coordinate, and conceal their activity. As investigators, we can no longer afford to treat digital platforms as secondary evidence sources — they are often the primary stage where crimes are committed, facilitated, and documented.

This guide has aimed to provide a practical foundation for accessing data from the most commonly used social media, messaging, and payment platforms in modern investigations. But beyond the technical language and legal templates, the real key to success lies in understanding the platforms you're investigating — how they work, what data they retain, and how that data can tie directly into the elements of your case.

Features will change. Policies will shift. New platforms will emerge. But investigators who remain curious, adaptable, and committed to learning will always be a step ahead. Keep pushing yourself to go beyond the surface, ask smarter questions, and be able to explain the “how” and “why” of what you found — not just what you asked for.

To those of you out there doing this work: thank you. Social media investigations are not just modern — they're necessary. You are helping to uncover hard truths, locate victims, build stronger cases, and hold offenders accountable in an increasingly digital world. We recognize that social media investigations can be “outside the comfort zone” of many investigators — particularly those who don't use social media regularly.

Oftentimes these offenders who use social media are targeting juveniles and youth — one of our most vulnerable populations, thus making these cases all the more important. Offenders using social media for criminal activity are often extremely conceited (they may believe they are “smarter” than law enforcement because they use a VPN or use Signal). **Together, we can prove them wrong.**

Stay sharp, stay safe, and keep doing the work that matters. **Good luck.**



<https://www.gbgconsulting.org>