\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*INSTRUCTIONS\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-This search warrant mask is specifically for the search of Amino for all data associated with identified account

-There is RED text below that needs to be changed based on the needs of your search warrant.

-There is BLUE text below which is provided for information to the reader about what is being requested and why. Make sure you read this information and understand it since you are putting it your search warrant. You may need to adjust some of the wording or content in these areas to the specifics of your case.

-There is GREEN text below that articulate facts specific to ICAC or sexual exploitation investigations. Include this language only if it applies. Make sure you read this information and understand it since you are putting it your search warrant. You may need to adjust some of the wording or content in these areas to the specifics of your case.

- After the warrant is finalized, highlight all of the text by selecting CTRL+A and then change all text to black

- It would be a good idea to delete this section before printing/sending your warrant to get signed.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*PLEASE DELETE\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Case No:

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

BEFORE THE HONORABLE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

JUDGE / MAGISTRATE

Affiant, YOUR NAME HERE, a commissioned law enforcement officer, being duly sworn, deposes and states that I have probable cause to believe that at the place or business entity known or described as:

Amino c/o MediaLab

1237 7th Street

Santa Monica, CA 90401

The following records, data, or information for Amino user identified as PROFILE URL OR EMAIL ADDRESS, hereinafter referred to as SUBJECT ACCOUNT, between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. All Personally Identifiable Information including, by way of example but not limitation, username, account identification number, first name, last name, aliases or monikers, electronic mail (email) addresses, phone number(s), physical or postal address, gender, date of birth or age, hometown, zip code, country, and/or general geographic area, other demographic information, user supplied profile or biographic information such as work and/or education histories, and profile picture(s), symbols, or graphics.
2. All device identification information including the operating system type, the operating system version, device manufacturer serial numbers, unique serial numbers of mobile devices including the Mobile Equipment Identifier (MEID) , the International Mobile Equipment Identity (IMEI), the International Mobile Subscriber Identity (IMSI), and the Media Access Control (MAC) address. Other unique identifiers may include information developed by the software operating system such as the Identifier for vendor (IFV), the advertising identifier (AI), the Unique Device Identifier (UDID), the cellular service provider and the cellular telephone number(s) associated with the device, and/or the internet service provider associated with the device.
3. All stored electronic address book or contact information including all first names, last names, nicknames, or monikers, phone numbers associated with the contact such as home phone numbers, mobile phone numbers, and/or work phone numbers, the email address(es) of the contact, social media account information of the contact such as account names or account identification numbers, and/or profile pictures used to identify the contact.
4. All stored messages, files, images, and videos including publicly or privately viewable messages to common message boards, forums, blogs, or walls, public or private chatrooms, electronic mail (email), short message service (SMS) text messages, multimedia message service (MMS) messages, and instant messages. In addition, all corresponding messages logs consisting of sender, recipient(s), date sent, time sent, date received, time received, message status such as read, unread, or undelivered, corresponding metadata such as the Internet Protocol (IP) addresses of the sender and receiver(s), message content including text and associated pictures, videos, and audio files and file attachments such as pictures, images, and audio and video files.
5. All stored digital images or pictures and videos including publicly or privately viewable messages to common message boards, forums, or walls, public or private chatrooms, electronic mail (email), short message service (SMS) text messages, multimedia message service (MMS) messages, and instant messages. In addition, all corresponding messages logs consisting of sender, recipient(s), date sent, time sent, date received, time received, message status such as read, unread, or undelivered, corresponding metadata such as the Internet Protocol (IP) addresses of the sender and receiver(s), message content including text and associated pictures, and file attachments such as pictures.
6. All metadata, including EXIF data, for all digital images, pictures, videos, documents, and files.
7. All log file information the date and time a computer or mobile device accessed the application or service, the type of computer or mobile device used to access the application or service, the type of operating system, the version of operating system, the internet browser type, the internet browser language, referring/exit webpages, landing pages, the pages viewed and the order of those pages, the amount of time spent viewing each page, the date and time the application or service was used.
8. Internet Protocol (IP) addresses used to create SUBJECT ACCOUNT. The IP address information shall include the IPv4 or IPv6 address, the date and time of access, and the time zone the access occurred in for the account creation. Amino App, LLC is further ordered/commanded to provide Affiant with Internet Protocol (IP) addresses used to access their services. The IP address information shall include the IPv4 and/or IPv6 address, the date and time of access, and the time zone the access occurred in.
9. All stored location information derived from any means including Global Positioning System (GPS), Wireless Fidelity (Wi-Fi), and cell site location information. Such records shall include the date and time the location information was collected, the type of technology used to measure the location, and the range variation of the technology used to measure the location.
10. All linked or associated groups or communities (referred to as Aminos) on the same operating platform for the target account.
11. A copy of images and videos, files and logs associated with Cybertip # CYBERTIP NUMBER

For which a search warrant and court order for production of records may be issued upon one or more of the grounds set forth in 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, namely that this property has been stolen or embezzled, or which is designed or intended for use as a means of committing a criminal offense, or which is or had been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

The facts establishing grounds for issuance of a search warrant and showing probable cause to believe that they exist are as follows:

**Electronic Definitions**

“Internet” means a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are physically located in the same state.

“Computers”, “digital media storage”, or “digital storage devices” may be used interchangeably, and are intended to include any physical object upon which computer data can be recorded as well as all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices capable of performing logical, arithmetic, or storage functions, including desktop and laptop computers, mobile phones, tablets, server computers, game consoles, network hardware, hard disk drives, RAM, floppy disks, flash memory, CDs, DVDs, and other magnetic or optical storage media.

Internet Service Providers “ISP’s” or Electronic Service Providers “ESP’s” are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line (DSL) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, that the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an “email address,” an email mailbox, and a personal password selected by the subscriber. By using a computer equipped with a telephone or cable modem, the subscriber can establish communication with an ISP over a telephone line or through a cable system, and can access the Internet by using his or her account name and personal password.

“Internet Protocol Address” or “IP address”: Every computer or device on the Internet is referenced by a unique Internet Protocol address the same way every telephone has a unique telephone number. An IP address is a series of numbers separated by periods; an example of an IP address is 192.168.10.102. Each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address. A central authority provides each ISP a limited block of IP addresses for use by that ISP’s customers or subscribers. Most ISPs employ dynamic IP addressing, that is they allocate any unused IP address at the time of initiation of an Internet session each time a customer or subscriber accesses the Internet. A dynamic IP address is reserved by an ISP to be shared among a group of computers over a period of time. The ISP logs the date, time and duration of the Internet session for each IP address and can identify the user of that IP address for such a session from these records. Typically, users who sporadically access the Internet via a dial-up modem will be assigned an IP address from a pool of IP addresses for the duration of each dial-up session. Once the session ends, the IP address is available for the next customer. On the other hand, some ISPs, including most cable providers, employ static IP addressing, that is a customer or subscriber’s computer is assigned one IP address that is used to identify each and every Internet session initiated through that computer. In other words, a static IP address is an IP address that does not change over a period of time and is typically assigned to a specific computer. A modem is an electronic device that allows one computer to communicate with another.

Social Media: In general, social media may be defined as websites and applications that enable users to create and share content or to participate in social networking.

IMEI: IMEI (International Mobile Equipment Identity) is a unique identification number that identifies mobile devices.

IMSI: An international mobile subscriber identity (IMSI) is a unique number, usually fifteen digits, associated with Global System for Mobile Communications (GSM) and Universal Mobile Telecommunications System (UMTS) network mobile phone users. The IMSI is a unique number identifying a GSM subscriber.

Cookie: A cookie is a small amount of data generated by a website and saved by your web browser. Its purpose is to remember information about you, similar to a preference file created by a software application. One purpose of a cookie is to save log in and password information for an account. It also serves the purpose of saving user preferences for a site, such as a search engine saving a search or a news website saving a certain font you prefer.

**Child Pornography/Child Exploitation Definitions**

NCMEC- The National Center for Missing and Exploited Children (“NCMEC”) is an organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a cybertip, also known as a CyberTipline Report. To make such a report, a company providing services on the internet (“ISP) can go to an online portal that NCMEC has set up for the submission of these tips. The ISP then can provide to NCMEC information about the child exploitation activity it believes has occurred, including the incident type, the incident time, any screen or user names associated with the activity, any IP address or port numbers it captured, as well as other information it may have collected in connection with the suspected criminal activity. Other than the incident type and incident time, the remainder of the information the ISP provides is voluntary and undertaken at the initiative of the reporting ISP. The ISP may also upload to NCMEC any files it collected in connection with the activity. The ISP may or may not independently view the content of the files it uploads. Using publicly available search tools, NCMEC then attempts to locate where the activity occurred based on the information the ISP provides such as IP addresses. NCMEC then packages the information from the ISP along with any additional information it has, such as previous related cybertips, and sends it to law enforcement in the jurisdiction where the activity is thought to have occurred.

“Sexually Exploitative Material” means any photograph, motion picture, video, recording, or broadcast of moving visual images, print, negative slide, or other mechanically, electronically, chemically, or digitally reproduced visual material that depicts a child engage in, participating in, observing, or being used for explicit sexual conduct.

**Statements Regarding Current Investigation**

BACKGROUND OF AFFIANT

STATEMENT OF PROBABLE CAUSE REGARDING CRIME BEING INVESTIGATED – OR IF FOR FUGITIVE PURPOSES, EXISTENCE OF OUTSTANDING WARRANT – AND PC TO BELIEVE THE ACCOUNT LISTED IS AN ACCOUNT THAT COULD LEAD TO MATERIAL EVIDENCE OR A FUGITIVE MIXED WITH THE BELOW PARAGRAPHS

**Relevant Background on Amino**

Applications distributed or developed by Amino App, LLC include the word Amino somewhere in the title as a component of their product branding and marketing. The Amino application is somewhat unique in the industry in that an individual can use the core Amino Communities for Chat and Forums application to create a community around any topic or subject they choose. Users of the application create and customize a user profile which may contain user generated, and unverified, biographical information. From within the application the users can communicate about the subject through messages which can be either public and available for anyone to see, to a select group determined by the message poster, or via one-to-one chats. Users may also use the application to watch videos related to their interest(s), read and respond to the web log, or 'blog', postings of others, post or respond to polls, and stay updated on news and information related to their interests.

Your Affiant is aware through research, documentation, prior training, experience, and/or the experience of other investigators that Amino App, LLC collects and stores personally identifying information (PII.) PII consists of user supplied information that tends to identify the user or creator of an account with Amino App, LLC This information may include, but not be limited to: username, account identification number, first name, last name, aliases or monikers, electronic mail (email) addresses, phone number(s), physical or postal address, gender, date of birth or age, hometown, zip code, country, and/or general geographic area, other demographic information, user supplied profile or biographic information such as work and/or education histories, and profile picture(s), symbols, or graphics. Your Affiant is aware this information is freely supplied by the user and required in order to create an account or use the service. Your Affiant is also aware that in most cases this information is exclusively user supplied and not verified. Therefore, the information may be fictitious. However, your Affiant is also aware user supplied email addresses and/or phone numbers may go through a verification process wherein the user must confirm receipt of a message sent via email or to their phone in order to access the service.

Amino App, LLC collects and stores information about the hardware and software of a mobile device or computer used to access their application or service. This information is generically referred to as device information. Device information may consist of information such as the operating system type, the operating system version, device manufacturer serial numbers, and unique serial numbers of mobile devices including the Mobile Equipment Identifier (MEID), the International Mobile Equipment Identity (IMEI), the International Mobile Subscriber Identity (IMSI), and the Media Access Control (MAC) address. Other unique identifiers may include information developed by the software operating system such as the Identifierforvendor (IFV), the advertisingidentifier (AI), the Unique Device Identifier (UDID), the Android Device ID, and/or the Google Service Framework (GSF) number. Furthermore, device information may include information specific to mobile devices such as the cellular service provider and the cellular telephone number(s) associated with the device.

Amino App, LLC accesses the electronic address book or contacts stored in the user’s device or in one or more of the user’s electronic mail (email) or social media accounts. The electronic address book may consist of the user entered name such as first name, last name, nickname, or moniker, one or more phone numbers associated with the contact such as home phone number, mobile phone number, and/or work phone number, the email address of the contact, social media account information of the contact such as account name or account identification number, and/or profile pictures used to identify the contact. It should be noted the user freely accepts the collection and storage of their contacts as outlined in Amino App, LLC ’s terms of service and/or privacy policy. It should also be noted that the fact Amino App, LLC accesses the user’s electronic contact information is does not always mean the information is stored or stored in a human readable format.

Amino App, LLC allows users to send messages from within the application or service. These messages may be sent using one or more of the following techniques or platforms: public or private postings to a common message board, forum, web log (commonly referred to as a blog) or wall, public or private postings in chat rooms dedicated to a specific topic, one-to-one messages sent via electronic mail (email), short message service (SMS) text messages, multimedia message service (MMS) messages which can include pictures, video, and/or audio files, and instant messages. Amino App, LLC also allows users to send and receive digital images from within the application or service. These pictures may be sent using one or more of the following techniques or platforms: public or private postings to a common message board, forum, or wall, public or private postings in chat rooms, electronic mail (email), short message service (SMS) text messages, multimedia message service (MMS) messages which can include pictures and videos and instant messages.

Amino App, LLC users to store, send, and/or receive digital images/pictures/videos/documents/and other file types through their service. Your Affiant is further aware that digital files, whether pictures, images, videos, documents, spreadsheets, or other files, contain metadata. Metadata can be described as information about the file type and can consist of different components. This may include the file creation date and time, the date and time the file was last modified, and the author is the document. Metadata for digital images is known as EXIF data or Exchangeable Information Format. EXIF data includes information about the camera such as the type of device that took the picture, whether the flash was used, the orientation of the device, the focal point, and the distance from the camera to the object depicted in the picture. EXIF data may also include additional information about the image including the date and time it was taken and, in some cases, the global positioning system (GPS) coordinates where the camera was when the image was taken.

Your Affiant is aware some social media companies, application providers, and online services strip the EXIF or metadata from publicly viewable files. This is done to protect the privacy interests of the user who may be unaware of the existence of the EXIF data. However, some companies that removed the EXIF data from public view still retain the data in non-publicly viewable databases associated with the user’s account. Therefore, it may still be possible to recover the EXIF data associated with the image(s) by compelling the company to provide the image file with accompanying EXIF/metadata.

Your Affiant believes the EXIF/metadata associated with the digital images, pictures, videos, documents, and files would tend to show the author or originator of the data, the date and time it was created and/or modified, and potentially the GPS coordinates where the file was created.

Amino App, LLC collects and stores information generically referred to as log file information. Log file information consists of background data collected by Amino App, LLC and shows information such as the date and time a computer or mobile device accessed their application or service, the type of computer or mobile device used to access their application or service, the type of operating system, the version of operating system, the internet browser type, the internet browser language, referring/exit webpages, landing pages, the pages viewed and the order of those pages, the amount of time spent viewing each page, the date and time the application or service was used.

Amino App, LLC applications include a passive location capability. The purpose of this location feature is to record, collect, and store the user’s location history. The location information is usually not shared publicly and is used to bring location based content and advertising to the user. The collection of this information is detailed in the company’s terms of service and privacy policy. The customer consents to the collection and storage of this information by installing, accessing, logging in, and/or using the service.

The location information is derived from the Assisted-Global Positioning System (A-GPS) incorporated into most modern portable or mobile devices. A-GPS information is calculated using a combination of the device’s Global Positioning System (GPS), readings and calculations from nearby Wireless Fidelity (Wi-Fi) access points, and readings and calculations from nearby cell sites (commonly referred to as cell towers.) Each location method has its respective pros and cons. GPS location information is the most precise but requires the user’s device to have a clear line of sight with at least four orbiting satellites. Wi-Fi is less accurate but works indoors and does not require the user’s device to actively use the network. Cell site location information is the least precise but works when GPS and Wi-Fi are not available.

**Relevant Background Information of Child Pornography**

Collectors and distributors of child pornography often use online resources to retrieve, share, and store child pornography. Non-pornographic, seemingly innocuous images of minors are often found in accounts that also contain child pornography, or that are used to communicate with others about sexual activity or interest in children. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images. Further, the online services allow a user to set up an account with a remote computing service that provides email services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. These online storage accounts are often free but can involve a charge. A subscriber assigned a free online storage account frequently can set up such accounts by providing limited identifying information. Any information provided is frequently fictitious in an attempt to preserve the anonymity of the user. Consequently, even if it is known that a collector or distributor of child pornography is a subscriber of a free online storage service, the service provider frequently will have no records in that subscriber’s name. Instead, the online service will only be able to identify files, including child pornography, that are associated with a “login,” or unique, user-created identity the subscriber uses to “log on” to the online service. Such an online storage account is particularly useful to a collector or distributor of child pornography. Such a subscriber can collect, store, view and distribute electronic images, including child pornography, directly from the online service. Consequently, the illegal files have minimal contact with the subscriber’s home computer. The subscriber can also manipulate the files on an online storage service from any computer connected to the Internet. Nonetheless, evidence of an online storage account is often found on a home computer of a user subscribing to such a service. Evidence of an online storage account may take the form of passwords located in encrypted, archived, or other files on the user’s home computer. Other evidence can also be found through unique software that may exist on a user’s home computer that has been developed by the online storage service. This unique software will frequently contain evidence not only of the existence of such accounts, but the login and password.

I know from training and experience that persons trading in, receiving, transporting, distributing, or possessing images involving the sexual exploitation of children or those interested in the firsthand sexual exploitation of children often communicate with others through correspondence or other documents (whether digital or written) which could tend to identify the origin of the images as well as provide evidence of a person's interest in child pornography or child sexual exploitation.

**Relevant Background Information of Technology**

I know from training and experience that digital evidence is not limited to computers. I have been involved in cases where persons engaged in the type of crime under investigation can access the Internet, display images reflecting their interests or participation in the crime, and communicate with other individuals with the same interests using digital storage devices to include cellular telephones, email devices, and personal digital assistants. These devices are frequently found to contain chat communications in the form of short message service (SMS) messages as well as enabling Internet and digital cellular network access.

I know from training and experience that the complete contents of online accounts may be important to establishing the actual user who has dominion and control of an online account at a given time. Online accounts may be registered in false names or screen names from anywhere in the world with little to no verification by the service provider. They may also be used by multiple people. So, information stored in connection with an online account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation. This helps establish and prove each element of the crime or alternatively, may exclude the innocent from further suspicion. In my training and experience, an online user’s account activity, IP log, location information, search history, stored electronic communications, and other data retained by providers, can indicate who has used or controlled an online account or can provide context for the crime under investigation. This can include evidence of motive and intent to commit a crime (e.g., communications about planning crimes) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). For example, profile contact information, direct messaging logs, shared photos and videos, and captions (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. Further, account activity, especially when paired with other evidence of the crime, can show how and when the account was accessed or used and may reflect a user’s motive or state of mind when doing so. For example, as described herein, Providers log the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Especially when considered in context with other evidence, such information allows investigators to understand the geographic and chronological context of an account’s access, use, and events relating to the crime under investigation. Location data also helps with this. Providers allow users to “tag” their location in posts to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the account user or other suspects.

I know from training and experience that criminals discussing their criminal activity may use slang, short forms (abbreviated words or phrases such as “lol” to express “laugh out loud”) or code words (which require entire strings or series of email conversations to determine their true meaning) when discussing their crimes. They can also discuss aspects of the crime without specifically mentioning the crime involved. In the electronic world, it is even possible to use pictures, images and emoticons (images used to express a concept or idea such as a happy face inserted into the content of an email or the manipulation and combination of keys on the computer keyboard to convey an idea, such as the use of a colon and paren “:)” to convey a smile or agreement) to discuss matters. Keyword searches would not account for any of these possibilities, so actual review of the contents of an online account by law enforcement familiar with the identified criminal activity is necessary to find all relevant evidence within the account.

I recognize the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit in order to prevent unnecessary invasion of privacy and overbroad searches. I advise it would be impractical and infeasible for the government to review records produced by a Service Provider and keep only such records as the government finds to be related to the offenses described herein during a single analysis. I have learned through practical experience that various emails often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review, and incorporation of evidence into a consolidated whole. Analysis is content relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually and not in sum. Due to the interrelation and correlation between communication threads and contents of accounts, and any respective attachments, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. Therefore, to obtain the full picture and meaning of the data from the information sought in this application, and to maintain its admissibility at trial, the government needs to maintain access to all of the resultant data. The completeness and potential of probative value of the online accounts and data must be assessed within the full scope of the investigation. As with all evidence, the government will maintain the contents of the account(s) in its custody and control, without alteration.

Based on these facts, Your Affiant believes there exists probable cause to believe that there is material evidence now located in the above described Amino account that is crucial to the investigation of this case and the offenses described above, and a search warrant is requested pursuant to 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41.

C.R.S. 16-3-301.1(5)(a) permits a court order for the productions of records to be granted to a Colorado criminal investigator or peace officer whose affidavit supports the issuance of the order. The Colorado criminal investigator or peace officer granted the order need not have authorization to execute a search warrant in the jurisdiction in which the business entity is located. C.R.S. 16-3-301.1(5)(c) permits service of a court order to be made through any electronic or other means established and utilized by the business to receive service of process.

Amino is a provider of electronic communication services subject to the Stored Communication Act (SCA), 18 U.S.C. §2703, et seq. The SCA permits a state court with jurisdiction over an offense to issue an extraterritorial warrant for production of electronic communication content and electronic communication records. 18 U.S.C. §2703(g) authorizes service of the warrant via methods other than in-person service by a law enforcement officer. It is the intent of this affiant, consistent with the SCA and the procedures established by Amino for compliance with the SCA, to serve this warrant via fax and/or email or law enforcement portal.

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

***Further requests:***

1. Pursuant to Crim. P. 41 and §16-3-304(2), Your Affiant requests that this Court seal the affidavit and search warrant and court order for production of records until the completion of the law enforcement criminal investigation. The affidavit establishes grounds to believe that disclosure at this time of the affidavit and search warrant and court order for production of records would be contrary to the public interest. Such order for sealing does not apply to representatives of law enforcement agencies, and District Attorney’s Offices.
2. So as not to disrupt this ongoing investigation, Your Affiant also requests that this Court order Amino NOT to take adverse action against the subject account, such as disabling or terminating the account, because of this warrant.
3. Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), Your Affiant requests that Amino be ordered NOT to disclose the existence of this search warrant and court order to the subscriber for a period of one year from receipt of the requested documents, unless otherwise ordered by a court of competent jurisdiction. Based on the information set forth in this affidavit, notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

I believe the above facts to be true from official LAW ENFORCEMENT AGENGY records, conversations with fellow officers, personal observations and interviews. I am a YOUR TITLE with the LAW ENFORCEMENT AGENGY. I have been trained at the State, and local levels with regard to my duties. I am authorized by law to execute search warrants in the State of Colorado.

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

AFFIANT

This affidavit was sworn to and subscribed in my presence this DATE day of MONTH 20\*\* at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**SEARCH WARRANT AND COURT ORDER FOR PRODUCTION OF RECORDS**

Before the Honorable \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Judge / Magistrate

The Court, upon review of an affidavit filed by YOUR NAME HERE which is incorporated by reference, in support of the issuance of this order, hereby orders the production of the following records, for which there is probable cause to believe are in the actual or constructive possession or control of the business entity known or described as:

Amino c/o MediaLab

1237 7th Street

Santa Monica, CA 90401

This Court also finds that there is probable cause to issue this Search Warrant and Court Order for Production of Records pursuant to the provisions of 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, namely that this property has been stolen or embezzled, or which is designed or intended for use as a means of committing a criminal offense, or which is or had been used as a means of committing a criminal offense, or the possession of which is illegal, or which would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court, or the seizure of which is expressly required, authorized, or permitted by a statute of this state or the United States, or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

IT IS ORDERED that the internet service/social media provider provide the following records, data, information and technical assistance:

The following records, data, or information for Amino user identified as PROFILE URL OR EMAIL ADDRESS, hereinafter referred to as SUBJECT ACCOUNT, between the dates of DATE OF INTEREST through DATE OF INTEREST for evidence of the crimes CRIMINAL OFFENSE:

1. All Personally Identifiable Information including, by way of example but not limitation, username, account identification number, first name, last name, aliases or monikers, electronic mail (email) addresses, phone number(s), physical or postal address, gender, date of birth or age, hometown, zip code, country, and/or general geographic area, other demographic information, user supplied profile or biographic information such as work and/or education histories, and profile picture(s), symbols, or graphics.
2. All device identification information including the operating system type, the operating system version, device manufacturer serial numbers, unique serial numbers of mobile devices including the Mobile Equipment Identifier (MEID) , the International Mobile Equipment Identity (IMEI), the International Mobile Subscriber Identity (IMSI), and the Media Access Control (MAC) address. Other unique identifiers may include information developed by the software operating system such as the Identifier for vendor (IFV), the advertising identifier (AI), the Unique Device Identifier (UDID), the cellular service provider and the cellular telephone number(s) associated with the device, and/or the internet service provider associated with the device.
3. All stored electronic address book or contact information including all first names, last names, nicknames, or monikers, phone numbers associated with the contact such as home phone numbers, mobile phone numbers, and/or work phone numbers, the email address(es) of the contact, social media account information of the contact such as account names or account identification numbers, and/or profile pictures used to identify the contact.
4. All stored messages, files, images, and videos including publicly or privately viewable messages to common message boards, forums, blogs, or walls, public or private chatrooms, electronic mail (email), short message service (SMS) text messages, multimedia message service (MMS) messages, and instant messages. In addition, all corresponding messages logs consisting of sender, recipient(s), date sent, time sent, date received, time received, message status such as read, unread, or undelivered, corresponding metadata such as the Internet Protocol (IP) addresses of the sender and receiver(s), message content including text and associated pictures, videos, and audio files and file attachments such as pictures, images, and audio and video files.
5. All stored digital images or pictures and videos including publicly or privately viewable messages to common message boards, forums, or walls, public or private chatrooms, electronic mail (email), short message service (SMS) text messages, multimedia message service (MMS) messages, and instant messages. In addition, all corresponding messages logs consisting of sender, recipient(s), date sent, time sent, date received, time received, message status such as read, unread, or undelivered, corresponding metadata such as the Internet Protocol (IP) addresses of the sender and receiver(s), message content including text and associated pictures, and file attachments such as pictures.
6. All metadata, including EXIF data, for all digital images, pictures, videos, documents, and files.
7. All log file information the date and time a computer or mobile device accessed the application or service, the type of computer or mobile device used to access the application or service, the type of operating system, the version of operating system, the internet browser type, the internet browser language, referring/exit webpages, landing pages, the pages viewed and the order of those pages, the amount of time spent viewing each page, the date and time the application or service was used.
8. Internet Protocol (IP) addresses used to create SUBJECT ACCOUNT. The IP address information shall include the IPv4 or IPv6 address, the date and time of access, and the time zone the access occurred in for the account creation. Amino App, LLC is further ordered/commanded to provide Affiant with Internet Protocol (IP) addresses used to access their services. The IP address information shall include the IPv4 and/or IPv6 address, the date and time of access, and the time zone the access occurred in.
9. All stored location information derived from any means including Global Positioning System (GPS), Wireless Fidelity (Wi-Fi), and cell site location information. Such records shall include the date and time the location information was collected, the type of technology used to measure the location, and the range variation of the technology used to measure the location.
10. All linked or associated groups or communities (referred to as Aminos) on the same operating platform for the target account.
11. A copy of images and videos, files and logs associated with Cybertip # CYBERTIP NUMBER

Pursuant to §16-3-301.1, C.R.S., a criminal investigator or peace officer is hereby authorized to serve this order during normal business hours of the above-named business entity, and to receive the records during normal business hours of the business entity. Service shall issue in the same manner as a summons in a civil action or by personal service on a manager or supervisor of the business entity or through any electronic or other means established and utilized by the business to receive service of process. This order must be served within 14 days after the date it is issued.

The business entity is ORDERED to produce the above described records to the affiant or his/her designee within thirty-five (35) days of service.

The records should be provided to:

YOUR NAME, BADGE NUMBER

LAW ENFORCEMENT AGENGY

YOUR ADDRESS

YOUR PHONE NUMBER

EMAIL

The business entity shall also provide a notarized attestation of accuracy that the records produced represent complete and accurate copies of all records identified in this order that are in the actual or constructive control of the business entity. If the business entity does not produce all records identified in this order, it shall identify the records not produced. Failure to comply with this order shall support a finding of contempt of court.

Upon receiving the records from the business entity, the peace officer named herein shall file a return and inventory with the court indicating the records that have been received and the date and time upon which the records were received. The peace officer named herein may also file the original of the attestation of accuracy with the court.

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the completion of the law enforcement criminal investigation, that the identity of any target(s) of the underlying criminal investigation may be redacted from any copy of this Order to be served on any service provider or other person.
2. That Amino NOT take adverse action against the subject accounts, such as disabling or terminating the accounts, because of this warrant.
3. Pursuant to 18 U.S.C. §2705(b) and 18 U.S.C. §2705(b)(1)-(5), and Crim. P. 41 and §16-3-304(2), that Amino, **NOT disclose the existence of this search warrant and court order to the subscriber for a period of one year**, unless otherwise ordered by a court of competent jurisdiction, as notification of the warrant may have an adverse result, as defined in 18 USC §2705(b)(1)-(5), i.e., disclosure may endanger the life or physical safety of an individual; allow flight from prosecution; allow destruction of or tampering with evidence; allow intimidation of potential witnesses; and/or would otherwise seriously jeopardize an investigation or unduly delay a trial.

THE INFORMATION SO ORDERED is related to the active and ongoing criminal investigation by YOUR AGENCY and in accordance with 18 U.S.C. §2703, C.R.S. §16-3-301, §16-3-301.1 and Crim. P. 41, the records and information requested are or have been used as a means of committing a criminal offense or would be material evidence in a subsequent criminal prosecution in this state, another state, or federal court; the seizure of which is expressly required, authorized, or permitted by statute; or that would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest order is outstanding.

Based upon the affidavit of the above-named Affiant, which is incorporated by reference, I am satisfied that there is probable cause to believe there is a legal basis and also legal authority for the issuance of this Search Warrant and Court Order for Production of Records. You are therefore authorized to execute this Search Warrant according to these terms and as otherwise permitted by law.

Dated this **\_\_\_\_\_day of \_\_\_\_\_\_\_\_\_ 20\_\_**, at \_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE