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

-This search warrant mask is specifically for the search of a vehicle infotainment system for all data associated with the identified account name, pen registry and location data

-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.

- 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**

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 thing to be searched, described as:

The vehicle is a COLOR, YEAR, MAKE MODEL bearing STATE license plate LICENSE PLATE NUMBER. The Vin number of the vehicle: VIN. More specifically, located within the vehicle, the infotainment system, related vehicle electronic control units and all related digital storage media associated with said vehicle will be searched.

ADD PHOTO OF VEHICLE IF AVAILIABLE

ADDRESS WHERE VEHICLE IS LOCATED

The following data stored in the infotainment system, related vehicle electronic control units and all related digital storage media associated with said vehicle, relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, methods of payment, account names, user names, screen names, remote data storage accounts, documents, files, metadata, log files, user voice profiles and other biometric identifiers or any other information and evidence that may demonstrate attribution to a particular user or users;
2. Live and deleted historical navigation data tracks, routes, and waypoints, GPS fixes, favorites, past journeys, trip logs, and user entered data, Latitude, Longitude, and Altitude coordinates, and related dates and times pertaining to Subject Offense(s);
3. Live and deleted logs, records, documents, and other items that may constitute evidence, contraband, fruits, and/or instrumentalities of violations of crimes, pertaining to Subject Offense(s);
4. Live and deleted contact lists, call logs, text messages and multimedia messages (SMS and MMS messages), e-mails, chats, video conference communication data, contact information, installed application information including their content and any other information which can be used to identify potentially associated persons pertaining to Subject Offense(s);
5. Live and deleted passwords, password files, PIN codes, encryption codes, or other information necessary to access the digital device or data stored on the digital device such as hidden file applications;
6. Live and deleted documents, programs, pictures, videos, audio files, text files, databases, application data, calendar entries, user dictionaries, malware, viruses, tracking or other remote monitoring software, and any associated metadata pertaining to Subject Offense(s);
7. Live and deleted web browser history, web browser bookmarks, temporary Internet files, cookies, searched items, downloaded and uploaded files, social networking websites or applications pertaining to Subject Offense(s);
8. Live and deleted data stored on removable media such as Subscriber Identity Modules (SIM cards), flash memory storage devices such as Secure Digital (SD) and Micro SD media cards and any associated wireless devices (Bluetooth, Wi-Fi, or other technology) pertaining to Subject Offense(s);
9. Live and deleted historical event data to include, but not limited to, when the headlights were on or off, when doors were opened or closed, when gears were changed, when brakes were applied, and when connections and disconnections were made to other devices, such as Bluetooth, media cards and Wi-Fi pertaining to Subject Offense(s).

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

For which a search warrant may be issued upon one or more of the grounds set forth in Crim. P. 41 and CRS § 16-3-301, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state, or the seizure of which is expressly required, authorized or permitted by any statute of this state, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant is outstanding.

The facts tending to establish the grounds for issuance of a Search Warrant are as follows:

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 VEHICLE LISTED COULD LEAD TO MATERIAL EVIDENCE OR A FUGITIVE MIXED WITH THE BELOW PARAGRAPHS

Motor Vehicle Infotainment System Capabilities

Your affiant knows that a motor vehicle is not limited to transportation. Many modern motor vehicles are factory installed with entertainment and communications consoles. These consoles are commonly called Infotainment Systems. Infotainment Systems allow drivers and/or passengers to connect their devices to the digital world. Such systems can store and/or stream digital content to and from a variety of devices; it may even broadcast a wireless signal which would allow passengers to connect to the World Wide Web (Internet).

Your affiant also knows that many motor vehicle Infotainment Systems allow a user to sync (connect and integrate communications wirelessly and/or with a cable) mobile devices to a particular motor vehicle Infotainment System. This connectivity generally allows motor vehicle occupants to perform hands-free operations such as voice calling and texting, access data streaming services such as music, news, weather, maps, navigation, traffic data, and other web based information and related content.

Furthermore, your affiant knows that Motor Vehicle Infotainment Systems commonly support the importing of content and other data information from a particular user’s mobile device. Such data may include content that may provide user attribution to particular user(s) that may include, but is not limited to, mobile device identifiers, telephone numbers, user accounts details, methods of payment, passwords, PIN codes, user voice profiles and other biometric identifiers, contact lists, call logs, text messages, e-mails, pictures, videos, web history, telephone numbers, addresses and/or GPS (Global Positioning System) coordinates, and other historical navigation information.

Your affiant knows that Global Positioning System or GPS portable navigation systems associated with Infotainment Systems use a space-based radio-navigation system which provides users with accurate information on position, velocity, and time anywhere in the world and in all weather conditions using a connected network of orbiting satellites. GPS portable navigation devices can store information in their digital memory about the locations where the device was for a period of time.

Consequently, there is probable cause to believe that the historical GPS data associated with the Infotainment System will contain recorded evidence of the physical location of the associated vehicle and/or person(s) whenever the vehicle and/or person was moving or stationary. Information and evidence of the associated vehicle and/or person(s) travels should contribute to identifying the locations from which the vehicle and/or person departed, the locations where the associated vehicle and/or person(s) traveled to and the time the associated vehicle and/or person(s) remained at different coordinates.

Your affiant knows that even after a previously connected mobile device is removed, much historical live and deleted data may remain within the digital storage capabilities of the Infotainment System.

Your affiant knows that these Infotainment Systems and associated connected or previously connected mobile devices can be used to delete, create, share, and store files and other data including, but not limited to, navigation history, documents, photographs, videos, electronic mail, search history and other relevant live and deleted user information. Your affiant also knows that such devices can be used to communicate and share information with others and that data can be transferred between various devices – wirelessly and by connected cables.

Your affiant also knows that live and deleted data recovered from Infotainment Systems may show evidence of current, on-going, future, and past criminal activity. Such information can be used to identify locations, victims, witnesses, associates and co-conspirators. Your affiant also knows that data from these devices can often include user attribution data that can identify the person(s) who sent, received, created, viewed, modified, or otherwise had control over particular content.

Your affiant is seeking evidence of ownership, use, and identiﬁcation, and knows that ownership and control of a vehicle, computer and/or a digital device can be placed at issue through a simple denial, “that is not mine.” Your affiant also knows that it is necessary to search live and deleted data recovered from a mobile device from when a mobile device was first activated to when a device was seized. This is specifically necessary to establish a particular device and associated application to a particular owner, user or users. Additionally, this full range of time may be necessary to identify communications, contacts, calendar entries, pictures, videos, location information (including GPS, navigation, and maps) that may convey communication between parties and identify suspects, co-conspirators, associates, witnesses and other individuals who may have involvement or knowledge of crimes and to establish pre-planning, execution, and post event information of criminal activity. Without this information, it may not be possible to understand events of a particular day and time in proper context and to attribute a particular owner, user or users of a device and their associated applications. Therefore, your Affiant is seeking all of the above information to establish ownership and control of the vehicle data.

Your affiant also knows that if these items are not seized and isolated from network connectivity in a timely manner, evidence may be destroyed, transferred, encrypted, modified, or otherwise lost forever. Your affiant knows that data recovered from an Infotainment System could be used to refute or corroborate data recovered from other mobile devices or obtained from service providers.

Your affiant knows that motor vehicles equipped with an Infotainment System and related storage media may retain live and deleted data relating to previously connected mobile device(s) such as mobile device identifiers, telephone numbers, user accounts details, methods of payment, passwords, PIN codes, user voice profiles and other biometric identifiers, contact lists, call logs, text messages, emails, pictures, videos, web history, telephone numbers, addresses and/or GPS (Global Positioning System) coordinates, and other historical navigation information.

Your affiant knows that live and deleted data stored in an Infotainment System and related storage media to include, call logs, MMS messages, SMS messages, device users, passwords, GPS, locations, tracklogs, system metadata, audio files, event logs, along with user attributes may be forensically located on the related storage. Your affiant believes it is probable and reasonable to believe that live and deleted data may be found on the Infotainment System and related storage media inside.Your affiant believes the data stored inside the Infotainment System and related storage media is evidence relevant to the above described investigation.

Your affiant also understands that in order to successfully complete a forensic extraction from an Infotainment System it may be necessary to repair the device, replace the screen, replace the chassis, reconnect wires, replace batteries, and remove trim and other components. Your affiant also understands that it may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes may include, but are not limited to, potentially destructive processes such as gaining root and/or super user level access, JTAG, ISP-JTAG and chip-off. Your affiant request authorization to utilize the least destructive means to analyze the device before using more potentially destructive methods described in this paragraph, if necessary.

Computer Processing

Due to the nature and vulnerability of magnetic or digital data, it is necessary to seize media capable of storing magnetic data, and the computer, or what is commonly referred to as the CPU, meaning the computer case which contains the hard drive, motherboard and related hardware. It is necessary to remove these items from the scene and transport them to a controlled environment so a complete search of the items may be accomplished in such a way that the data it is protected, and unaltered.

Your affiant is aware that the current technology available for the downloading of data from digital devices such as cell phones, computers, or other mobile devices, does not allow the download of information only for a specific date range. Your affiant is also aware that the current technology available may not allow the downloading of only specific types of data, (e.g. pictures, messages, contacts, application data, etc.) as this data, including dates, may be in raw form, making it humanly unreadable without the use of specific software.  In light of that, the data from the digital device must be downloaded as completely as technologically possible. Once that download is completed, and the downloaded data is processed with specific software, a search of the data for a specific date range or specific type of data content is possible.

Your affiant is also aware that many times, there is only one opportunity to download the information from a digital device. Without obtaining all of the downloadable data from the cell phone, computer, or other mobile device, if additional information is learned later in the investigation, either by law enforcement, the District Attorney’s Office, or defense counsel, the same data that existed at the time of the initial download may no longer be available.  The only way to ensure preservation of all the downloadable data that existed at the time of the original download is to initially obtain all the downloadable data from the cell phone, computer, or other mobile device, and then preserve that data for any future searches.

Your affiant is requesting to obtain all of the downloadable data from the digital device(s). That data will be saved to preserve it in case additional review of the data is warranted and authorized by the courts at a later time. If a future search of the downloaded data from the device is necessary at a later time, additional applications will be made to the courts. At this time, the review of the data extracted from the device(s) will be for the date range and data authorized in the warrant.

***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 filing of charges based on this 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.

The executing law enforcement officer(s) may enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imaging, and analysis of any and all of the information described.

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 County of Larimer and State of Colorado.

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

AFFIANT

This affidavit was sworn to and subscribed by telephone this DATE day of MONTH 20\*\* at \_\_\_\_\_\_\_\_.

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

JUDGE / MAGISTRATE

Case No.

COUNTY OF LARIMER ) IN THE COMBINED COURT

) SS

STATE OF COLORADO )

**SEARCH WARRANT**

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

JUDGE / MAGISTRATE

TO: ANY PEACE OFFICER AUTHORIZED BY LAW TO EXECUTE SEARCH WARRANTS IN THE STATE OF COLORADO.

The Court, upon review of a sworn affidavit filed by YOUR NAME HERE, a commissioned law enforcement officer, in support of the issuance of this search warrant, hereby commands you to search the following described property, namely:

The vehicle is a COLOR, YEAR, MAKE MODEL bearing STATE license plate LICENSE PLATE NUMBER. The Vin number of the vehicle: VIN. More specifically, located within the vehicle, the infotainment system, related vehicle electronic control units and all related digital storage media associated with said vehicle will be searched.

ADD PHOTO OF VEHICLE IF AVAILIABLE

ADDRESS WHERE VEHICLE IS LOCATED

The following data stored in the infotainment system, related vehicle electronic control units and all related digital storage media associated with said vehicle, relevant to the criminal activity described in the affidavit, which is incorporated by reference, and possible prosecution of CRIMINAL OFFENSE(S) perpetrated against NAME OF VICTIM OR LOCATION [IF APPLICABLE] (hereinafter “Subject Offense(s)”):

REVIEW THE LISTED CATEGORIES OF DATA, PLEASE REMOVE ANY CATAGORIES NOT SUPPORTED BY THE FACTS CONTAINED IN YOUR AFFIDAVIT

1. Live and deleted user attribution data including user accounts, e-mail accounts, passwords, PIN codes, patterns, methods of payment, account names, user names, screen names, remote data storage accounts, documents, files, metadata, log files, user voice profiles and other biometric identifiers or any other information and evidence that may demonstrate attribution to a particular user or users;
2. Live and deleted historical navigation data tracks, routes, and waypoints, GPS fixes, favorites, past journeys, trip logs, and user entered data, Latitude, Longitude, and Altitude coordinates, and related dates and times pertaining to Subject Offense(s);
3. Live and deleted logs, records, documents, and other items that may constitute evidence, contraband, fruits, and/or instrumentalities of violations of crimes, pertaining to Subject Offense(s);
4. Live and deleted contact lists, call logs, text messages and multimedia messages (SMS and MMS messages), e-mails, chats, video conference communication data, contact information, installed application information including their content and any other information which can be used to identify potentially associated persons pertaining to Subject Offense(s);
5. Live and deleted passwords, password files, PIN codes, encryption codes, or other information necessary to access the digital device or data stored on the digital device such as hidden file applications;
6. Live and deleted documents, programs, pictures, videos, audio files, text files, databases, application data, calendar entries, user dictionaries, malware, viruses, tracking or other remote monitoring software, and any associated metadata pertaining to Subject Offense(s);
7. Live and deleted web browser history, web browser bookmarks, temporary Internet files, cookies, searched items, downloaded and uploaded files, social networking websites or applications pertaining to Subject Offense(s);
8. Live and deleted data stored on removable media such as Subscriber Identity Modules (SIM cards), flash memory storage devices such as Secure Digital (SD) and Micro SD media cards and any associated wireless devices (Bluetooth, Wi-Fi, or other technology) pertaining to Subject Offense(s);
9. Live and deleted historical event data to include, but not limited to, when the headlights were on or off, when doors were opened or closed, when gears were changed, when brakes were applied, and when connections and disconnections were made to other devices, such as Bluetooth, media cards and Wi-Fi pertaining to Subject Offense(s).

Items ITEMS LIMITED BY DATE are limited to data with created, accessed or modified dates between DATE OF INTEREST through DATE OF INTEREST.

For which a search warrant may be issued upon one or more of the grounds set forth in the Colorado Rules of Criminal Procedure and CRS § 16-3-301 and 19-2-504, namely that this property is stolen or embezzled, or is designed or intended for use as a means of committing a criminal offense, or is or has been used as a means of committing a criminal offense, or the possession of which is illegal, or would be material evidence in a subsequent criminal prosecution in this state or another state, or the seizure of which is expressly required, authorized or permitted by any statute of this state, or which is kept, stored, maintained, transported, sold, dispensed, or possessed in violation of a statute of this state, under circumstances involving a serious threat to public safety or order or to public health, or which would aid in the detection of the whereabouts of or in the apprehension of a person for whom a lawful arrest warrant 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 that the property described is located at the place or thing to be searched as described above, and probable cause to search that property upon one or more of the grounds set forth in the Colorado Revised Statutes and the Colorado Rules of Criminal Procedure.

Therefore, any member of law enforcement agency or a designee, and/or a computer forensic lab, are commanded to:

* If not already in possession of the device, seize the aforementioned device within 14 days of the date this warrant is signed;
* Access the aforementioned device and view, copy and maintain the above described data contained therein;
* Use and employ such force as may reasonably be necessary in the performance of the duties described herein;
* The ability to use whatever means necessary to override any encryption or secure files encountered during the forensic examination of the phone, which may be destructive to the equipment. This could include having the item transferred to specialized forensic laboratories outside of the jurisdiction and/or the State of Colorado, if necessary.
* The ability to repair the device, replace the screen, replace the chassis, reconnect wires, or replace a battery. I also understand that it may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes including potentially destructive and destructive processes such as gaining root and/or Super user level access, JTAG, ISP-JTAG and chip-off.
* The ability to enlist the aid of a law enforcement computer forensic laboratory and/or certified digital evidence examiner(s) in the searching, viewing, photographing, recording, copying, forensic imagining, and analysis of any and all of the information described.
* Deliver to the person from whom the property is taken a copy of this warrant together with a receipt for the property taken, or to leave a copy of the warrant and receipt at the place from which the property was taken;
* Make prompt return of this search warrant, accompanied by a written inventory describing the physical storage media that was seized or copied, to the undersigned judge.

IT IS FURTHER ORDERED:

1. That this Search Warrant and Order and application be **SEALED** until the filing of charges based on this 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. After charges are filed, disclosure of this Search Warrant and Order and application is governed by Crim. P. 55.1.

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. 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