**AUTHORIZING THE STATE OF FLORIDA**

**COUNTY OF ALACHUA**

**RELEASE AND/OR RECEIPT**

**OF CUSTOMER RECORDS,**

**CELL SITE AND OTHER INFORMATION**

**INCLUDING GEOLOCATION OF A**

**CERTAIN COMMUNICATION DEVICE(S)**

**Target Device(s)/Account(s) /**

**Telephone Number(s)/Identifier(s):** (phone number)

**Florida Statute(s)/Offense(s) under Investigation:** (crimes here)

**Agency(ies) for which Requested:** (your agency)

**Requesting Agent/Applicant:** DETECTIVE (your name)

**Case Number:** CR# here

**Target (if known) of Investigation:** (suspect’s name)

**WARRANT / ORDER**

This matter having come before the Court pursuant to the application of Detective (your name) of the (your agency), whose application requested: authorization to release, acquire and/or receive communication detail records (not including content of communications) and enhanced caller identification information; signaling information (including “cell site location”) for the Target Telephone, in real time; authorization for the release, acquisition and/or the receipt of E911 Locations, GPS/Geolocations, Range To Tower, Per Call Measurement Data, and other location based measurements of the Target Telephone; and directing certain communication and/or information service providers to furnish forthwith, all information in printed form, electronic format, or orally, as required, facilities, records, and technical assistance necessary to accomplish the requests in said application:

1. This Court finds that there is probable cause to believe that (suspect’s name) has committed the felony crimes of (crimes here). An arrest warrant having been issued based upon a finding of [OR if no arrest warrant, Affiant having stated] probable cause that (suspect’s name) has committed the offenses of (crimes here), there is probable cause to believe that (suspect’s name) is and will continue to utilize the certain mobile communications device, the Target Telephone, to-wit: telephone number (phone number), serviced by (phone company) to aid in avoiding apprehension and arrest, contains evidence relevant to a felony offense, and/or to facilitate or further the commission of a felony offense.

AND, this Court having found that Applicant, Detective (your name), has certified to this Court that the information likely to be obtained by the requests and such installations and uses sought are relevant to an ongoing criminal investigation related to the offenses of (crimes here), and that there is probable cause, based on specific and articulable facts, that the target telephone is being used in the commission of felony crimes and/or the location of the target telephone is relevant and material to an on-going criminal investigation, to proving felony crimes, or may lead to relevant evidence to prove a felony crime, AND, this Court having found the sworn Application in this matter to have sufficiently articulated **probable cause** for the issuance of this Order / Warrant, and complies with Florida Statutes §§934.23, including 934.23(4)(a)1, 934.31 – 934.34, and 934.42 [Florida’s Mobile Tracking Device, in light of United States v. Jones, 132 S.Ct. 945 (2012)], Carpenter v. U.S., 138 S.Ct. 2206 (2018), and Tracey v. State, 152 So.3d 504 (Fla. 2014), and other relevant legal provisions, and is consistent with Title 18, United States Code, §§3121 -3127 and 2703(c)(1)(A), it is therefore,

A. ORDERED AND ADJUDGED that the (your agency, and any agencies helping or involved) (hereinafter collectively the “Investigating Agency”), with all lawful assistance, is authorized to install and use, or cause to install and use, such equipment as to obtain the communication detail records (including call, SMS, and MMS detail, not including content of communications) (without geographic limitations), as well as caller identification/caller identification deluxe including caller identification on call waiting[[1]](#footnote-1), to obtain those telephone numbers dialed or pulsed from the target telephone, to record the date and time of such pulsings and/or recordings, and to capture the incoming electronic pulsings to the target telephone that identify the originating number of an instrument or device from which wire or electronic communication is transmitted, to record and decode the dialing, routing, addressing, or signaling information for the target telephone, in real time, and the Investigating Agency, with all lawful assistance, is authorized to install and use, or cause to install and use, such equipment as to obtain GPS/Geolocations, E911 Locations, Range To Tower, Per Call Measurement Data and other location based measurements of the Target Telephone, in real-time.

B. BY THE TERM, “target telephone,” this Court means telephone number (phone number) and/or any changed telephone number(s) subsequently assigned to the same International Mobile Subscriber Identity (IMSI) and/or instrument bearing the same Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), and/or Mobile Equipment Identifier (MEID), or any new IMSI, ESN, IMEI and/or MEID, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the target telephone within the period authorized by order; and/or any new IMSI, ESN, IMEI and/or MEID is assigned to the target telephone or new/changed telephone number(s), whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the target telephone within the period authorized by this order.

C. BY THE TERM “such equipment,” this Court means that the Investigating Agency is authorized to use, cause the use of, and/or receive the data from the installation and use of: a pen register with enhanced caller identification, trap and trace device(s) (without geographic limitations), cell-site simulator technology or equipment, and/or wi-fi geo-location technology or equipment, to aid locating the target telephone, in aid of this criminal investigation. This includes, but is not limited to, the collection and examination of signals emitted by the target device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications; and signals emitted by the target device in response to signals sent to the target device by the Investigating Agency, during all times of day and night. This warrant does not authorize the interception of any communications content and this warrant prohibits the seizure of any tangible property.

2. FURTHER ORDERED AND ADJUDGED that (phone company), and all other Service Providers[[2]](#footnote-2), landlords, custodians, and other persons and entities are hereby authorized and ordered to furnish, in a format specified by the Investigating Agency, **for the period of (start date), to and including (end date)**, such requested records of the target telephone, whether maintained by (phone company) or any other service provider supplying service to the target telephone, including but not limited to such information stored in computer databases dedicated to fraud detection by (phone company) or any other service provider supplying service to the listed telephone, or in any form or location maintained by (phone company) or any other service provider supplying service to the target telephone, as soon as practicable from the date of this Warrant, all information to include:

1. The current Subscriber, activation date, Application and Billing Information, including payment method and credit card information, including any and all customer service records, all circuits terminating records, can be reached (CBR) numbers, enhanced custom call features, subscribed to services and primary long distance carrier,
2. The target telephone’s International Mobile Subscriber Identification (IMSI), the Mobile Subscriber Identification Number (MSID/ MIN), Temporary Mobile Subscriber Identifier (TMSI) numbers provided in real-time, the Electronic Information Numbers (EIN), the Electronic Serial Number (ESN), Individual Mobile Subscriber Identification (IMSI) number, and any replacement combinations of those numbers, and these same numbers for any additional cellular telephones owned by or leased to the same account or subscriber,
3. The brand name and model of handset, and special features information; and all of the previous information for any additional cellular telephones owned by or leased to the same account or subscriber,
4. Communication Detail Records (CDR’s) with Cellular Sites and associated street addresses, to include numbers dialed, incoming numbers, call durations, signaling and communications processing information, geographic location of towers and sectors activated, as available, without communications content and excluding post-cut-through dialed digits, sent and received by the target telephone for any form of communication it is capable of, including voice, VoIP, text, SMS, MMS, internet, mobile-to-mobile, “direct connect” or any push-to-talk like feature, non-billed calls, uncharged call detail, CDR and iDEN network search engine reports, Viador Reports, airtime usage data, Automated Message Accounting (AMA) records and data bases and Calls-to Destination data,
5. The MAC addresses of the target telephone, Wi-Fi MAC address of the target telephone and/or the MAC address of the access point(s) to which the target telephone connects to the internet via wireless networking technology that allows computers and other devices to communicate over a wireless signal (commonly referred to as “Wi-Fi”), and packet data, control channels used and their corresponding cell sites,
6. Radio Signal Strength Indicators (RSSI) for the period of the warrant, timing advance and other pertinent information delivered in real time with regard to neighboring towers as feasible,
7. All Internet Protocol (IP) addresses, email addresses, email logs (with header information, but without any content, such as subject lines or the body of emails), website addresses, servers, and user names, including user identifying information of communications both to and from the target telephone,
8. GEO/Precision (GPS- Locator Tools) Locations and/or E911 locations, Range to Tower Measurements (RTT), Per Call Measurement Data (PCMD), Historical Mobile Locator,
9. And facilities and technical assistance necessary to accomplish the requests stated herein.

3. FURTHER ORDERED AND ADJUDGED that:

A. Pursuant to Florida Statute §92.605, this order recognizes the potential “adverse result” which may befall the investigation for failure to obtain the information requested in the time periods directed in this Order, including the following consequences: (1) danger to the life or physical safety of an individual or (2) flight from prosecution,

B. (phone company), and other service providers shall provide to the Investigating Agency upon request, subscriber information from any service provider, not including cell tower or other location data beyond area codes, including thirty (30) days of voice communication/call logs, text/SMS logs, IP Address and/or data/MMS logs, for the telephone numbers dialed to or pulsed from the target telephone, whether published or non-published, including the names, addresses, credit and billing information, if requested of the service providers by the Investigating Agency within forty-five (45) days of the signing of this order, including toll records (call, text and/or media), also referred to as “detailed bill” for a period of thirty (30) days from the date of request. Such service providers shall provide the requested information WITHIN 48 HOURS OF THE REQUEST,

C. (phone company), and other service providers, shall provide to the Investigating Agency information relating to any other central office-based features, such as call forwarding, speed calling or dialing, touchstar, and ring master, if such features exist or are subscribed to during the pendency of this warrant. The information provided shall include subscriber information, including billing and credit information, relating to each individual digit(s) associated to speed dialing, whether published or non-published, and the destination to which the target telephone is call forwarded (including call forwarding to the final destination), including billing and credit information whether published or non-published,

D. During the pendency of this warrant, (phone company), and other service providers shall notify Detective (your name) [(your email address)] WITHIN 24 HOURS OF THE FOLLOWING CHANGES OR ATTEMPTED CHANGES to the target telephone including any changed telephone number(s) subsequently assigned to the same International Mobile Subscriber Identity (IMSI) and/or instrument bearing the same Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), and/or Mobile Equipment Identifier (MEID), or any new IMSI, ESN, IMEI and/or MEID, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the target telephone within the period authorized by order, and/or any new IMSI, ESN, IMEI and/or MEID assigned to the target telephone or new/changed telephone number(s), whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the target telephone within the period authorized by this order,

E. The (your agency) shall reasonably compensate (phone company), and other service providers affected by this order, landlords, custodians, and other persons and entities who furnish facilities and/or technical assistance pursuant to this warrant for all reasonable charges and/or expenses incurred in providing such facilities and assistance, provided that said charges and/or expenses shall be identified and billed to the (your agency) as is provided in Section 934.26, Florida Statutes,

F. This warrant and its supporting application shall be sealed until further order of this Court or another Court of competent jurisdiction, provided that a copy of this warrant may be made available to employees of (phone company), and other service providers, landlords, custodians, other persons and entities, if necessary, to facilitate their assistance in implementing the provisions of this warrant,

G. Pursuant to Florida Statutes §934.33(4)(b) and 934.43, (phone company), and other service providers, and their agents and employees, landlords, custodians, and other persons and entities ordered hereby to provide assistance to the Investigating Agency, shall not disclose to the listed subscriber, lessee or sub-lessee of the target telephone, or to any other person or entity, the existence of this warrant and its supporting application, or of this investigation, unless otherwise ordered by this Court or another Court of competent jurisdiction,

H. Pursuant to Florida Statutes §934.23(4)(c) (An investigative or law enforcement officer who receives records or information under this subsection is not required to provide notice to a subscriber or customer.) and §934.32-33, §934.42(5), no notice to the subscriber or customer of the issuance of this order is required,

I. This warrant / order and shall be effectuated by the Investigating Agency and/or served upon (phone company) by the Investigating Agency within ten (10) days of issuance by this Court.

DONE AND ORDERED this \_\_\_ day of (month), 20(year) in (ALACHUA) County, Florida.

CIRCUIT COURT JUDGE

**AUTHORIZING THE STATE OF FLORIDA**

**COUNTY OF ALACHUA**

**RELEASE AND/OR RECEIPT**

**OF CUSTOMER RECORDS,**

**CELL SITE AND OTHER INFORMATION**

**INCLUDING GEOLOCATION OF A**

**CERTAIN COMMUNICATION DEVICE(S)**

**APPLICATION FOR WARRANT**

Comes now affiant (your name), who is a sworn DETECTIVE with the (YOUR AGENCY), to apply to this Court for a warrant authorizing the release, acquisition and/or receipt of communication detail records (not including content of communications) and enhanced caller identification information, authorizing the release, acquisition and/or the receipt of E911 Locations, GPS/Geolocations, Range To Tower, Per Call Measurement Data, and other location based measurements of the target telephone, and directing certain communication and/or information service providers to furnish forthwith all information, in printed form, electronic format or orally, as required, facilities, records, and technical assistance necessary to accomplish the requests in said application. This application is being submitted pursuant to Florida Statute §934.23, including §934.23(4)(a)1, §934.31-.34 and §934.42, Tracey v. State, 152 So.3d 504 (Fla. 2014), United States v. Jones, 132 S.Ct. 945 (2012), Shaktman v. State, 553 So. 2d 148 (Fla. 1989) and other relevant legal provisions, and is consistent with Title 18, United States Code, §3121 -3127 and 2703(c)(1)(A). The use of the term “warrant” herein also contemplates and is inclusive of the term “order,” as applicable, for those statute sections.

In support of this application, your Affiant asserts as follows:

1. Your Affiant, Detective (your name), has been a law enforcement officer for (#) years and has received (your training and experience here). YA is currently assigned to (assignment) and has been assigned to investigate various criminal offenses to include, but not limited to, (crimes here) since (when did you start assignment). Your Affiant is employed as a sworn law enforcement officer with the (your agency) in Alachua County, Florida. The (your agency) is participating in an on-going criminal investigation of violations of Florida Statutes (crimes here). These unlawful activities have occurred in the Eighth Judicial Circuit of Florida.

2. Your Affiant has participated in this on-going criminal investigation and has personal knowledge of the facts set forth in this affidavit and/or has received this information from other law enforcement officers. Relevant to this application, your Affiant has learned the following during this investigation: [brief PC]

1. (facts showing Suspects / Defendant is involved with crime).
2. The target telephone, cellular telephone number (phone number), is an active (phone company) cellular telephone believed to be utilized by (suspect’s name). [sample] During an interview with (suspect’s name), he was in possession of his cell phone. He identified the cell phone as his and provided his cell phone number (phone number) and service provider, which was confirmed.

1. The jurisdictional provisions for the sections of the Florida Statutes under which this Application is made have the following statements of jurisdiction: Florida Statutes §934.32 and 934.33 (Application and Issuance of Pen Registers/Trap and Trace Devices, respectively), and Florida Statutes §934.42 (Mobile Tracking Device), each refer to a “court of competent jurisdiction,” which is defined in §934.02(8) as “… circuit judge, or judge of any court of record having felony jurisdiction of the State of Florida, irrespective of the geographic location or jurisdiction where the judge presides.” Florida Statute §934.23 (Required Disclosure of Customer Records), specifically states, “as used in this section, the term ‘a court of competent jurisdiction’ means a court that has jurisdiction over the investigation or that is otherwise authorized by law.” As a circuit judge having jurisdiction over the investigation over the crimes alleged above, which are believed to have occurred in the Eighth Judicial Circuit, this Court has jurisdiction to authorize the devices requested herein.

3. Your Affiant has probable cause to believe that the information likely to be obtained through the use of the requested devices and/or such equipment, including communications traffic data, cell site location data information and/or GPS tracking, and by signing below certifies that the information likely to be obtained through the use of the requested devices and/or such equipment is relevant and material to this on-going criminal investigation and/or may lead to the discovery of evidence relevant to proving a felony crime.

As the U.S. Supreme Court stated in Carpenter v. U.S., 138 S.Ct. 2206 (2018), 2018 WL 303916,

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying “roaming” charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

The U.S. Supreme Court further found in Carpenter that, “a cell phone—almost a ‘feature of human anatomy,’ [Riley, 573 U.S., at ––––, 134 S.Ct., at 2484](https://1.next.westlaw.com/Link/Document/FullText?findType=Y&serNum=2033666953&pubNum=0000708&originatingDoc=Iebe9c7e2761f11e89d59c04243316042&refType=RP&fi=co_pp_sp_708_2484&originationContext=document&transitionType=DocumentItem&contextData=(sc.Search)#co_pp_sp_708_2484)—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time.” Carpenter v. U.S., 138 S.Ct. 2206 (2018), 2018 WL 303916.

4. Accordingly, based upon the above information, and pursuant to §934.32, 934.33, 934.23, 934.42, Florida Statutes, because your Applicant asserts probable cause to believe that the target telephone is being utilized as described above, your Affiant respectfully requests that this Court issue an order authorizing the (your agency) (Investigating Agency) with all lawful assistance, be authorized: to install and use, or cause to install and use, such equipment as to obtain the communication detail records (including call, SMS, and MMS detail, not including content of communications) (without geographic limitations), as well as caller identification/caller identification deluxe including caller identification on call waiting, to obtain those telephone numbers dialed or pulsed from the target telephone, to record the date and time of such pulsings and/or recordings, to capture the incoming electronic pulsings to the target telephone that identify the originating number of an instrument or device from which wire or electronic communication is transmitted, to record and decode the dialing, routing, addressing, or signaling information for the target telephone, in real time, and the Investigating Agency, with all lawful assistance, be authorized to install and use, or cause to install and use, such equipment as to obtain GPS/Geolocations, E911 Locations, Range To Tower, Per Call Measurement Data and other location based measurements of the Target Telephone, in real-time.

5. Your Affiant requests that this Honorable Court issue an order directing that the term, “target telephone,” means telephone number (phone number) and/or any changed telephone number(s) subsequently assigned to the same International Mobile Subscriber Identity (IMSI) and/or instrument bearing the same Electronic Serial Number (ESN), International Mobile Equipment Identity (IMEI), and/or Mobile Equipment Identifier (MEID), or any new IMSI, ESN, IMEI and/or MEID, whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the target telephone within the period authorized requested, and/or any new IMSI, ESN, IMEI and/or MEID is assigned to the target telephone or new/changed telephone number(s), whether the changes occur consecutively or simultaneously, listed to the same subscriber and wireless telephone account number as the target telephone within the period requested by this Application.

6. Your Affiant requests that this Honorable Court issue an order directing that the term, “such equipment,” means that the Investigating Agency is authorized to use, cause the use of, and/or receive the data from the installation and use of a pen register with enhanced caller identification, trap and trace device(s) (without geographic limitations), cell-site simulator technology or equipment, and/or wi-fi geo-location technology or equipment, to aid locating the target telephone, in aid of this criminal investigation(s). This Application does not request the interception of any communications content nor the seizure of any tangible property.

1. Your Affiant requests that during the pendency of the requested warrant this Court authorize the Investigating Agency to determine the location of the target device by collecting and examining signals emitted by the target device for the purpose of communicating with cellular infrastructure, including towers that route and connect individual communications, and signals emitted by the target device in response to signals sent to the target device by the Investigating Agency, during all times of day and night. Cell-site simulators function by transmitting as a cell tower, while Wi-Fi simulators function by transmitting as an access point (without requesting to connect to a target device). In response to the signals emitted by the cell-site simulator technology or equipment and/or wi-fi geo-location technology or equipment (herein “simulator”), devices in the proximity of the simulator identify the simulator as the most attractive cell tower in the area, or as an available access point as to Wi-Fi simulator, and thus the target device then transmits signals to the simulator which identify the device in the same way they would with a networked tower or access point. The simulator receives and uses an industry standard unique identifying number assigned to the target device by a device manufacturer or cellular network provider. When used to locate a known target device, a simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the simulator identifies the specific device for which it is looking, it will obtain the signaling information relating only to that particular device. When used to identify an unknown device, the simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device.
2. Your Affiant discloses that, through the use of simulators, the Investigating Agency may send signals to the target device that will cause it, and non-target devices on the same provider network in close physical proximity, to emit unique identifiers, which will be obtained by the technology, and that investigators will use the information collected to determine information pertaining to the physical location of the target device or to determine the currently unknown identifiers of the target device.
3. When used to locate a known device, a simulator initially receives the unique identifying number from multiple devices in the vicinity of the simulator. Once the simulator identifies the specific device for which it is looking, it will obtain the signaling information relating only to that particular device. When used to identify an unknown device, the simulator obtains signaling information from non-target devices in the target's vicinity for the limited purpose of distinguishing the target device. Simulators provide only the relative signal strength and general direction of a target device. They do not function as a GPS locator, as they do not obtain or download any location information from the device or its applications.
4. The target device and other cellular devices in the area might experience a temporary disruption of service from the service provider. Any potential service disruption to non-target devices would be temporary and all operations will be conducted to ensure the minimal amount of interference to non-target devices.
5. When the equipment is used to locate a known device, all data will be deleted as soon as that device is located, and no less than once daily. Prior to deploying equipment for another investigation, the Investigating Agency will verify that the equipment has been cleared of any previous operational data. Law enforcement will make no affirmative investigative use of any non-target data absent further order of the Court, except to identify and distinguish the target device from other devices.

7. It is further requested that this Court direct that order (phone company), and all other service providers, landlords, custodians, and other persons and entities are hereby authorized and ordered to furnish, in a format specified by the Investigating Agency, **for the period of (start date), to and including (end date)**, such requested records of the target telephone, whether maintained by (phone company) or any other service provider supplying service to the target telephone, including but not limited to such information stored in computer databases dedicated to fraud detection by (phone company) or any other service provider supplying service to the listed telephone, or in any form or location maintained by (phone company) or any other service provider supplying service to the target telephone, as soon as practicable from the date of this warrant, all information including:

1. The current subscriber, activation date, application and billing information, including payment method and credit card information, including any and all customer service records, all circuits terminating records, can be reached (CBR) numbers, enhanced custom call features, subscribed to services and primary long distance carrier.
2. The target telephone’s International Mobile Subscriber Identification (IMSI), the Mobile Subscriber Identification Number (MSID/ MIN), Temporary Mobile Subscriber Identifier (TMSI) numbers provided in real-time, the Electronic Information Numbers (EIN), the Electronic Serial Number (ESN), Individual Mobile Subscriber Identification (IMSI) number, any replacement combinations of those numbers, and these same numbers for any additional cellular telephones owned by or leased to the same account or subscriber.
3. The brand name and model of handset, and special features information, and all of the previous information for any additional cellular telephones owned by or leased to the same account or subscriber.
4. Communication Detail Records (CDR’s) with cellular sites and associated street addresses, including numbers dialed, incoming numbers, call durations, signaling and communications processing information, geographic location of towers and sectors activated, as available, without communications content and excluding post-cut-through dialed digits, sent and received by the target telephone for any form of communication of which it is capable, including voice, VoIP[[3]](#footnote-3), text, SMS, MMS, internet, mobile-to-mobile, “direct connect” or any push-to-talk like feature, non-billed calls, uncharged call detail, CDR and iDEN network search engine reports, Viador Reports, airtime usage data, Automated Message Accounting (AMA) records and Data Bases and Calls-to Destination data.
5. The MAC addresses[[4]](#footnote-4) of the Target Telephone, Wi-Fi MAC addresses of the target telephone, and/or the MAC address of the access point(s) to which the target telephone connects to the internet via wireless networking technology that allows computers and other devices to communicate over a wireless signal (commonly referred to as “Wi-Fi”), and packet data; control channels used and their corresponding cell sites.
6. Radio Signal Strength Indicators (RSSI) for the period of the warrant, timing advance and other pertinent information delivered in real time with regard to neighboring towers as feasible.
7. All Internet Protocol (IP) addresses, email addresses, email logs (with header information, but without any content, such as subject lines or the body of emails), website addresses, servers, and user names, including user identifying information of communications both to and from the target telephone.
8. GEO/Precision (GPS- Locator Tools) locations and/or E911 locations, Range to Tower Measurements (RTT), Per Call Measurement Data (PCMD), Historical Mobile Locator.
9. And facilities and technical assistance necessary to accomplish the requests stated herein.

8. Your Affiant respectfully requests that this Court direct (phone company), and other service providers to provide to forthwith the Investigating Agency upon request, subscriber information from any service providers, excluding cell tower or other location data beyond area code, including voice communication/call logs, text/SMS logs, IP Address and/or data/MMS logs, for the telephone numbers dialed to or pulsed from the target telephone, whether published or non-published, including the names, addresses, credit and billing information, if requested of the service providers by the Investigating Agency within forty-five (45) days of the signing of an order by this Court, including toll records (call, text and/or media) also referred to as “detailed bill” for a period of thirty (30) days from the date of request, and direct that the service provider shall provide the requested information WITHIN 48 HOURS OF THE REQUEST; to direct (phone company), and other service providers, to provide forthwith to the Investigating Agency, information relating to any other central office-based features, such as call forwarding, speed calling or dialing, touchstar, and ring master, if such features exist or are subscribed to during the pendency of the warrant, the information provided including subscriber information, including billing and credit information, relating to each individual digit(s) associated to speed dialing, whether published or non-published, and the destination to which the target telephone is call forwarded (including call forwarding to the final destination), including billing and credit information whether published or non-published, to direct (phone company) or other service providers not to discontinue or disconnect (Hotline) service to the target telephone, and to authorize the Investigating Agency to use any and all information obtained by this request in aid of criminal investigation(s).

9. Your Affiant further requests that this application and any resulting warrant be sealed until further order of this Court, or another Court of competent jurisdiction, provided that a copy of the warrant may be made available to employees of (phone company), and other service providers, landlords, custodians, other persons and entities, if necessary, to facilitate their assistance in implementing the provisions of any resulting warrant.

10. Your Affiant asserts that pursuant to §934.23(4)(c), Florida Statutes (an investigative or law enforcement officer who receives records or information under this subsection is not required to provide notice to a subscriber or customer), §934.32-33; §934.42 (5) (the standards established by the United States Supreme Court for the installation and monitoring of mobile tracking devices shall apply to the installation and use of any device as authorized by this section) and {“‘[i]t may be that achieving the same result [tracking on public streets] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question,’ Tracey v. State, 152 So.3d 504, 525 (Fla. 2014), citing United States v. Jones, 132 S.Ct. at 954 (bracketed material added),”}, no notice to the subscriber or customer of the issuance of this order is required.

11. Your Affiant requests the providers be ordered pursuant to § 934.33(4)(b) and 934.43, Florida Statutes, not to disclose to the listed subscriber, lessee or sub-lessee of the target telephone, or to any other person or entity, the existence of this application any resulting warrant.

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

Detective (your name), Affiant

(your agency)

Subscribed to and sworn before me by the aforementioned Applicant,

[] who is personally known to me

[] who has produced law enforcement credentials as identification,

this \_\_\_ day of (month), 20(year).

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

Notary or Assistant State Attorney

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

(attorney’s name), Reviewing Attorney

**BUSINESS RECORD CERTIFICATION**

Pursuant to Sections 90.803(6) and 90.902(11), Florida Statutes

1. I \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ am currently employed with:

(Print name of affiant)

Business Name:

Business Address:

1. I am a custodian of records maintained by our business.
2. The attached record(s) are either originals or duplicate copies described as: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. The attached record(s) were made at or near the time of the occurrence of the matters set forth by, or from information transmitted by, a person having knowledge of those matters.
4. The attached record(s) were kept in the course of the regularly conducted activity of our business.
5. The attached records(s) were made as a regular practice in the course of the regularly conducted activity of our business.
6. I am aware that falsely making this Certification or Declaration would subject me to criminal penalty under the laws of the foreign or domestic location in which this certification or declaration was signed.
7. I have signed this Certificate under oath.

I do hereby swear or affirm that this certification and the attached records are true and accurate.

(Affiant Signature)

BEFORE ME, the undersigned authority, personally appeared \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, who was duly sworn under oath and who did sign the above Certification on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

The affiant is

\_\_\_\_\_ personally known to me or

\_\_\_\_\_ has presented \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ as identification.

NOTARY PUBLIC (print name) NOTARY PUBLIC (sign name)

My Commission Expires: \_\_\_\_\_\_\_\_\_

1. (phone company) and other providers of communication and/or information services shall examine the target telephone account and determine if it is equipped with a call identification feature as is supplied by (phone company) to retail customers.  If target telephone is not equipped with a caller identification feature, (phone company) is to add to the existing service the enhanced caller identification feature with no record of said service to the telephone's subscriber and/or account holder. (phone company) shall be compensated by the Investigating Agency for any additional expenses incurred by the installation of a caller identification feature.  (phone company) shall take all necessary steps to ensure that the addition of said feature, or any activity relating to said feature shall not be reflected on the subscriber's bill, or in any other way, be disclosed to the person(s) utilizing the target telephone and/or the subscriber and/or account holder of the target telephone. [↑](#footnote-ref-1)
2. By “service providers” or “service provider” this Court means, and hereby directs this warrant to, any communications and/or information service provider, including but not limited to: Aio Wireless, Alltel Wireless, AT&T Wireless, VERIZON, AT&T Southeast, BellSouth Telecommunications, BrightHouse Network, Cellco Partnership, Cricket Wireless, CREDO Mobile, Comcast Cable Communications, Comcast, Florida Digital Network, Level 3, Level 3 Communications, Liberty Wireless, MetroPCS, Neustar, Sprint / Nextel Corporation, Nextel Communications, Spectrum L.P., Simple Mobile, T-Mobile (USA), Ting, TracFone, Verizon Wireless, Virgin Mobile, U.S. Cellular, Windstream Communications, XIT Communications, XO Cellular. [↑](#footnote-ref-2)
3. Voice over Internet Protocol (VoIP), is a technology that allows a user to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. VoIP services convert a person’s voice into a digital signal that travels over the Internet. www.fcc.gov/encyclopedia/voice-over-internet-protocol-voip. [↑](#footnote-ref-3)
4. A “MAC address” is a “Media Access Control” address, a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi. [↑](#footnote-ref-4)