UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES AND FOR SUBSCRIBER INFORMATION FOR WHATSAPP ACCOUNT NUMBER 52-6383800020	MISC. NO. 19-sw-6046-GPG
	Filed Under Restriction

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. §§ 3122, 3123 AND ORDER PURSUANT TO 18 U.S.C §§ 2703(c)(2) AND 2703(d)

The United States of America, moving by and through Pete Hautzinger, its undersigned counsel, respectfully submits under restriction from public access this ex parte application for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices ("pen-trap devices") on WhatsApp Inc. account number 52-6383800020, associated with telephone number 52-6383800020, believed to be in the possession of Jesus Manuel URIAS-CASTANEDA (hereinafter referred to as URIAS-CASTANEDA and to obtain information for the accounts revealed by the use of the pen-trap devices pursuant to 18 U.S.C. §§ 2703(c)(2) and 2703(d). In support of this application, the United States asserts:

THE INSTALLATION AND USE OF PEN-TRAP DEVICES

1. This is an application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.

2. Such an application must include three elements: (1) "the identity of the attorney for the Government or the State law enforcement or investigative officer making the

application"; (2) "the identity of the law enforcement agency conducting the investigation"; and (3) "a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b).

3. The undersigned applicant is an "attorney for the government" as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the Drug Enforcement Administration. The Drug Enforcement Administration is investigating criminal activity involving drug trafficking. The investigation concerns possible violations by URIAS-CASTANEDA of, inter alia, 21 U.S.C. § 841(a)(1) and 846, Conspiracy to Distribute and Possess with the Intent to Distribute a Controlled Substance.

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by the Drug Enforcement Administration.

6. This Court is a "court of competent jurisdiction" under 18 U.S.C. § 3122(a)(2) because it "has jurisdiction over the offense being investigated," 18 U.S.C. § 3127(2)(A)(i).

ADDITIONAL INFORMATION

7. Other than the three elements described above, federal law does not require that an application for an order authorizing the installation and use of a pen register and a trap and trace device specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

8. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire

or electronic communication is transmitted." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

9. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

10. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by a unique number called an Internet Protocol, or "IP" address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. An IP address is analogous to a telephone number and can be recorded by pen-trap devices, and it indicates the online identity of the communicating device without revealing the communication's content.

11. A network is two or more computers or other devices connected to each other that can exchange information with each other via some transmission method, such as by wires, cables, or radio waves. The equipment that connects a computer or other device to the network is commonly referred to as a network adapter. Most network adapters have a Media Access Control ("MAC") address assigned by the manufacturer of the adapter that is designed to be a unique identifying number. An adapter's unique MAC address allows for proper routing of communications on a local area network and may be used for other purposes, such as authentication of customers by some network service providers. Unlike a device's IP address

that often changes each time a device connects to the Internet, a MAC address is fixed at the time of manufacture of the adapter. Because the address does not change and is intended to be unique, a MAC address can allow law enforcement to identify whether communications sent or received at different times are associated with the same adapter.

12. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet's source and destination IP addresses and the packet's size.

13. In addition, different Internet applications are associated with different "port numbers," or numeric identifiers. The port number is transmitted along with any communication using that application. For example, port 80 typically is associated with communications involving the World Wide Web.

14. Providers use cookies and other software to track the online movements of its customers and to show that one person is using multiple online accounts. Information gathered using such tools is helpful in identifying a user of an account as well as identifying other accounts the customer is using.

15. A cellular telephone, or cell phone, is a mobile device that transmits and receives wire and electronic communications. Individuals using cell phones contract with cellular service providers, who maintain antenna towers covering specific geographic areas. In order to transmit

or receive calls and data, a cell phone must send a radio signal to an antenna tower that, in turn, is connected to a cellular service provider's network.

16. In addition to a unique telephone number, each cell phone has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cell phone could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), a Mobile Subscriber Integrated Services Digital Network Number ("MSISDN"), or an International Mobile Station Equipment Identity ("IMEI"). When a cell phone connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower, and the cellular antenna or tower records those identifiers as a matter of course. The unique identifiers—as transmitted from a cell phone to a cellular antenna or tower—are like the telephone number of an incoming call. They can be recorded by pen-trap devices and indicate the identity of the cell phone device making the communication without revealing the communication's content.

17. In addition, a list of incoming and outgoing telephone numbers is generated when a cell phone is used to make or receive calls, or to send or receive text messages (which may include photographs, videos, and other data). These telephone numbers can be recorded by pen-trap devices and then used to identify the parties to a communication without revealing the communication's contents.

18. A cell phone can also be used to exchange text messages with email accounts. The email addresses associated with those text messages can be recorded by pen-trap devices and

then used to identify parties to a communication without revealing the communication's contents.

19. Cellular phones can connect to the Internet via the cellular network. When connecting through the cellular network, Internet communications sent and received by the cellular phone each contain the same unique identifier that identifies cellular voice communications, such as an ESN, MEIN, MIN, SIM, IMSI, MSISDN, or IMEI. Internet communications from a cellular phone also contain the IP address associated with that cellular phone at the time of the communication. Each of these unique identifiers can be used to identify parties to a communication without revealing the communication's contents.

20. These telephone numbers can include "post-cut-through dialed digits," which are numbers dialed from the cell phone after the initial call set up is completed. For example, some post-cut-through dialed digits may be the actual telephone number called, such as when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. That final number sequence is necessary to route the call to the intended party and, therefore, identifies the place or party to which the call is being made. In the event that the pen-trap devices capture some post-cut-through dialed digits that could be considered call content, such as account numbers or passwords, despite the government's use of reasonably available technology to avoid the recording or decoding of such content, the United States will make no affirmative investigative use of such information.

21. Most cellular phone providers offer their customers the ability to send text messages to one another via their phones. However, most charge for this service. As a consequence, there are applications (or "apps), which can be downloaded to a cell phone that

allow the user to send text messages through the cell phone's internet connection for free. WhatsApp is one of those apps.

22. The WhatsApp Messenger application allows users to send text messages, audio messages, video messages, and location information between mobile devices. WhatsApp Messenger application users may also set up and participate in group chats. Each WhatsApp Messenger application account's unique identifier is the telephone number of the mobile device on which the WhatsApp Messenger application is installed. Instead of sending a message to an email address, the WhatsApp message is routed across the Internet, via WhatsApp, Inc. servers located in the United States, from one mobile device to another. The telephone numbers associated with the application indicate the origin and destination of the WhatsApp messages. These account numbers can be recorded by pen-trap devices and can be used to identify parties to a communication without revealing the communication's content.

23. WhatsApp, Inc., maintains that it does not store the contents of the communication. Instead, WhatsApp Inc. maintains that it merely routes the message to the receiving mobile device as soon the receiving device's receiver is on-line. It does maintain that it can capture a text message's IP address as well as the online user's IP address when the user is logged into his/her WhatsApp account.

OBTAINING SUBSCRIBER INFORMATION

24. Cingular Wireless, Sprint Nextel Corporation, Leap Wireless Communications, Inc., Cricket Communications, T-Mobile USA, Cellco Partnership d/b/a Verizon Wireless, AT&T Wireless, Google, and WhatsApp, Inc. are providers of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or remote computing services, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under 18 U.S.C.

§ 2703(d) to require those entities to disclose subscriber information as defined in 18 U.S.C. § 2703(c)(2).

25. This Court has jurisdiction to issue the proposed order for subscriber information because it is "a court of competent jurisdiction," as defined in 18 U.S.C. § 2711. See 18 U.S.C. § 2703(d). Specifically, the Court is a district court of the United States that has jurisdiction over the offense being investigated. See 18 U.S.C. § 2711(3)(A)(i).

26. A court order under 18 U.S.C. § 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Accordingly, this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the requested subscriber information is relevant and material to an ongoing criminal investigation as follows:

27. Between June and July, 2019, an Albuquerque, New Mexico DEA Agent acting in an undercover capacity had been in contact with an individual known to the Agent as "Jesus" utilizing telephone number 52-638380020. A query of telephone number 52-638380020 indicated that on June 03, 2019, a Jose M. Trujillo had sent a $1,000.00 wire transfer to Jesus Manuel URIAS-CASTANEDA who is utilizing telephone number 52-6383800020 in Hermosillo, Sonora, Mexico.

28. On October 08, 2019, Ismael Ramos was arrested by the Eagle County Sheriff's Office when Ramos was found to be in possession of approximately 201 grams of methamphetamine. A post Miranda interview was conducted of Ramos who stated that Ramos' source of supply was in Mexico and that all communications with the methamphetamine source

of supply of was via WhatsApp application. Ramos stated that he would send payment for the methamphetamine via Western Union to Mexico and that the methamphetamine was subsequently mailed to Ramos via UPS. After Ramos signed a consent to search form, a search of Ramos' cellular telephone revealed a text message conversation with telephone number 52-6383800020. A search of DEA databases revealed that telephone number 52-6383800020 is associated with an individual in Mexico known as "Jesus" and that "Jesus" is a known source of supply for methamphetamine. A further search of Ramos' cellular telephone revealed a screen shot of a Western Union wire transfer in the amount of $1,000.00 from Jesus Del Toro in Avon, Colorado to Jesus Manuel URIAS CASTANEDA in Hermosillo, Sonora, Mexico on October 01, 2019.

29. Based on the interviews and consensual search of Ramos' cellular telephone, TRIDENT Commander Dave Moreno acting in an undercover capacity contacted URIAS-CASTANEDA on telephone number 52-6383800020 and told URIAS-CASTANEDA that he was a friend of Ramos and that Ramos was in jail. URIAS-CASTANEDA and Commander Moreno exchanged several text messages and then had a telephone conversation via WhatsApp. During the telephone call, URIAS-CASTANEDA stated that he ships pound amounts of methamphetamine and charges $2500 or $3000 per pound. URIAS-CASTANEDA requires a $1000 deposit sent via Western Union prior to sending the methamphetamine. URIAS-CASTANEDA told Commander Moreno that he has 30 pounds of methamphetamine in the United States and that 20 have been sold and has 10 remaining for sale.

30. Between October 11, 2019 and October 20, 2019, Commander Moreno and URIAS-CASTANEDA have been in contact via WhatsApp. During these conversations, URIAS-CASTANEDA agreed to send one or two pounds of methamphetamine via UPS to

Commander Moreno pending a down payment via Western Union. URIAS-CASTANEDA sent a message utilizing telephone number 52-638380020 to Commander Moreno that instructed Commander Moreno to send the down payment via Western Union to URIAS-CASTANEDA's wife and provided the name Daniela Jimena Llanes Inzunza in Sonora, Mexico. On that date, Commander Moreno sent $1,500.00 via Western Union to the name URIAS-CASTANEDA provided.

31. On October 19, 2019, URIAS-CASTANEDA called Commander Moreno and stated that he will be sending one pound of methamphetamine to Commander Moreno via UPS.

32. The pen-trap devices sought by this application will be installed at location(s) to be determined, and will collect dialing, routing, addressing, and signaling information associated with each communication to or from the WhatsApp Inc. account, including the date, time, and duration of the communication, and the following, without geographic limit:

- IP addresses, including IP addresses associated with access to the account
- Headers of WhatsApp messages, including the source and destination network addresses, as well as the routes of transmission and size of the messages, but not content located in headers, such as subject lines
- the number and size of any attachments
- MAC addresses
- Port numbers
- Packet headers
- Any unique identifiers associated with the cell phone device or devices used to send and receive WhatsApp messages, or to send or receive other electronic communications, including the ESN, MEIN, IMSI, IMEI, SIM, MSISDN, or MIN

- IP addresses of any websites or other servers to which the cell phone using the WhatsApp device connected
- Source and destination WhatsApp account/telephone numbers
- "Post-cut-through dialed digits," which are digits dialed after the initial call set up is completed, subject to the limitations of 18 U.S.C. § 3121(c) [1]

GOVERNMENT REQUESTS

33. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication to or from the WhatsApp Inc. account 52-6383800020, along with the date, time, and duration of the communication, without geographic limit. The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

34. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty days, pursuant to 18 U.S.C. § 3123(c)(1).

35. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order WhatsApp Inc. and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to install the pen-trap devices, including installation and operation of the

[1] In the event that the pen-trap devices capture some post-cut-through dialed digits that could be considered call content, such as account numbers or passwords, despite the government's use of reasonably available technology to avoid the recording or decoding of such content, the United States will make no affirmative investigative use of such information.

pen-trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by the DEA, pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in providing facilities and assistance in furtherance of this Order.

36. The United States further requests that the Court order WhatsApp Inc. and any other person or entity whose assistance may facilitate execution of this Order to notify the applicant and the DEA of any changes relating to the WhatsApp account (336) 639-5427, including changes to subscriber information, and to provide prior notice to the applicant and the DEA before terminating or changing service to the account.

37. The United States further requests that the Court order that the DEA have access to the information collected by the pen-trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

38. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order WhatsApp Inc. and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this application and Order, the resulting pen-trap devices, or this investigation, except as necessary to effectuate the Order, unless and until authorized by this Court.

39. The United States further requests, pursuant to 18 U.S.C. § 2703(c) and (d), that WhatsApp Inc., Cingular Wireless, Sprint Nextel Corporation, Leap Wireless Communications, Inc., Cricket Communications, T-Mobile USA, Cellco Partnership d/b/a Verizon Wireless, AT&T Wireless, Google, and/or any other provider of wire communications service, provide subscriber information as defined in 18 U.S.C. § 2703(c)(2) pursuant to this Order for the

accounts revealed by the pen-trap devices to the DEA. The United States further requests that the Order require WhatsApp Inc., Cingular Wireless, Sprint Nextel Corporation, Leap Wireless Communications, Inc., Cricket Communications, T-Mobile USA, Cellco Partnership d/b/a Verizon Wireless, AT&T Wireless, Google, and/or any other provider of wire communications service, not to notify any person, including the subscribers or customers of the account(s) for which subscriber information is provided, of the existence of the Order for the period of one year from the date of the order. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order may seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this investigation may be stored electronically. If alerted to the investigation, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

40. The United States further requests that this case, namely the application and any resulting order, be restricted from all public access until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1). In addition, as explained above, these documents discuss an ongoing

criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to restrict these documents from public access because their premature disclosure may seriously jeopardize that investigation.

52. The foregoing is based on information provided to me in my official capacity by agents of the United States Drug Enforcement Administration.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

Executed on October 22, 2019.

JASON R. DUNN
United States Attorney
District of Colorado

s/ *Pete Hautzinger*
Pete Hautzinger
Assistant United States Attorney
205 N. 4th Street, Suite 400
Grand Junction, CO 81501