AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

# UNITED STATES DISTRICT COURT

unsealed on 6/7/21 per order -dlg

~~SEALED~~

for the

Southern District of California

In the Matter of the Search of
*(Briefly describe the property to be searched or identify the person by name and address)*

Google LLC
1600 Amphitheater Parkway, Mountain View, CA 94043
Host of expliamdavis@gmail.com

Case No. '21 MJ01948

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| 21 USC §§ 841, 846 | Conspiracy to Distribute Controlled Substances |

The application is based on these facts:

See Attached Affidavit of FBI Special Agent Nicholas Cheviron, incorporated herein by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

*Applicant's signature*

Nicholas Cheviron, FBI Special Agent
*Printed name and title*

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means).*

Date: May 17, 2021

*Judge's signature*

City and state: San Diego, California

Honorable Michael S. Berg, U.S. Magistrate Judge
*Printed name and title*

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Nicholas I. Cheviron, being duly sworn, depose and state as follows:

1. This affidavit is in support of an application by the United States of America for a search warrant for Google LLC at 1600 Amphitheatre Parkway, Mountain View, CA 94043, as described in Attachment A, to search the following email account:

**expliamdavis@gmail.com**

(hereinafter "Subject Account") from January 1, 2021, to May 17, 2021, for items that constitute evidence, fruits, and instrumentalities of violations of federal criminal law, namely, Title 21, United States Code, Sections 841(a)(1), 846 (Conspiracy to Distribute Controlled Substances), as described in Attachment B. This affidavit and application are sought pursuant to Rule 41 of the Federal Rules of Criminal Procedure and 18 U.S.C. § 2703(a) and (b), which applies to providers of electronic communication and remote computing services.

2. The facts set forth in this affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; interviews of victims; my review of documents and computer records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation. All dates, times, and amounts discussed herein are approximate.

EXPERIENCE & TRAINING

3. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since January 2007. I am currently assigned to the San Diego Division, working as a member of the Organized Crime squad. Prior to my employment with the FBI, I was a police officer with the Bloomington, Illinois, Police Department for

approximately three years. I received basic narcotic enforcement training while attending the Illinois Police Training Institute, for 12 weeks, in Champaign, Illinois. During my time as a police officer, I received several hours of specialized narcotic enforcement training. I also had the opportunity to investigate and take part in several narcotic investigations. In addition to the training I received as a police officer, I also received extensive investigative training while attending the FBI Academy at Quantico, Virginia, for 21 weeks.

4. Since becoming an FBI Special Agent, I have investigated all aspects of criminal organizations to include narcotics trafficking, money laundering, and the operation of illegal gambling businesses. I have interviewed and operated informants, executed search warrants, arrested and interviewed subjects, conducted physical surveillances, utilized electronic and video surveillance, and testified in federal and state courts. I have led and participated in investigations involving the use of electronic surveillance techniques to include, but not limited to, court-authorized wire intercepts; video surveillance; global positioning satellite ("GPS") trackers; and body-worn monitoring devices. These investigations have included violations of statutes listed under Titles 18, 21, 31, and 49 of the United States Code as well as violations under California state law. As a result of these investigations, I have reviewed conversations of hundreds of individuals involved in both drug trafficking and the laundering of illicit proceeds. From my training and experience, I have become familiar with the techniques and methods utilized by criminal organizations.

5. I have conducted and participated in investigations concerning the identification of co-conspirators through telephone records and bills, financial documents, drug ledgers, photographs, and other documents. I have also participated in and conducted debriefs of individuals who were arrested and later cooperated with law enforcement. I have led and participated in investigations in which the court-authorized interception of communications or other electronic surveillance tools were utilized to further the investigation. In that regard, my involvement has included writing Title III affidavits and

search warrants for email accounts and the GPS pings of cellular phones based off information gleaned from Title III intercepts, assisting with surveillance, reviewing intercepted communications, and preparing written reports resulting from my observations.

6. Based on my training and experience, I am familiar with the methods of operation of drug smuggling organizations, including their methods of distribution, storage, and transportation of illicit drugs, their methods of collecting proceeds of drug trafficking, and their methods of laundering money to conceal the nature of the proceeds. During the course of my employment, I have also become familiar with the ordinary meaning of controlled substance slang and jargon, packaging methods, consuming and transferring of controlled substances, and I am familiar with the manners and techniques of traffickers in cocaine, methamphetamine, heroin, fentanyl, and marijuana.

7. In addition to above-stated training and experience, I have also worked with and consulted numerous agents and law enforcement officers who have investigated criminal organizations throughout the United States, including Southern California, as well as transnational organized crime groups. Additionally, I have received training focusing on criminal enterprises and tactics utilized by the enterprise to generate and facilitate illicit funds. Those tactics include narcotics trafficking, illegal gambling and bribery. I have also attended training that focused on the laundering of illicit funds. Additionally, I have participated in numerous working group meetings which focused on transnational organized crime and the various methods used to facilitate transnational organized crime. In additional to formal training, I have consulted with various experienced law enforcement officers who are trained in the abovementioned topics. Furthermore, I have had numerous discussions with senior law enforcement officers and agents specializing in maritime and aviation-based drug smuggling organizations. Through these investigations and training, I am familiar with the operations of drug trafficking and money laundering organizations in the United States and abroad.

8. My experience as a law enforcement officer, both as a police officer and as a

SA with the FBI; my participation in numerous criminal organization investigations; my conversations with other SAs of the FBI, SAs of the Drug Enforcement Administration (DEA), and other law enforcement officers familiar with narcotics trafficking, money laundering, and transnational organized crime; and my training form the basis of the opinions and conclusions set forth below which I drew from the facts set forth herein.

STATEMENT OF PROBABLE CAUSE

**A. Background on Criminal Use of Hardened Encrypted Devices**

9. In 2017, FBI San Diego began investigating a company named Phantom Secure which provided hardened encrypted devices.[1] The investigation revealed Phantom Secure sold its encrypted devices exclusively to members of criminal organizations. The company targeted its customer base to transnational criminal organizations ("TCOs") (primarily drug traffickers) and provided an array of services intended to impede law enforcement's ability to legally surveil their communications and collect evidence of criminal activities. The investigation uncovered the use of Phantom Secure devices all around the world by criminal syndicates.

10. In March 2018, a grand jury in the Southern District of California returned an indictment against the CEO of Phantom Secure, Vincent Ramos, and four other principals of the company, charging them with violating RICO and aiding and abetting the

[1] A "hardened encrypted device" is a communication device that (1) sends and receives encrypted electronic communications, and/or (2) encrypts the data stored on the device. Like other competitor brands of hardened encrypted devices, Phantom Secure's devices had limited functionality: a user could not make a normal phone call or browse the internet. Phantom Secure provided encryption service plans lasting from two to six months, and devices cost $1,500 to $2,000 each for a six month service plan. Devices could not be purchased in a regular store or online; would-be users needed to have a connection to a known distributor to even begin the initial conversation to obtain a device. Users of Phantom Secure devices operated in a closed loop system; that is, device-to-device communication was limited to a self-selected closed group of individuals using only other Phantom Secure devices.

distribution of cocaine. Ramos was arrested in March 2018.[2] On October 2, 2018, Ramos pled guilty to the Indictment. During his change of plea hearing, Ramos admitted Phantom Secure (1) aided and abetted the importation, exportation, and distribution of illegal drugs throughout the world; (2) obstructed justice through the destruction and concealment of evidence from law enforcement; and (3) laundered drug trafficking proceeds. Ramos was sentenced to nine years in prison and ordered to forfeit $80,000,000.00 in assets which constituted the proceeds of this criminal activity.

11. Because hardened encrypted devices provide an impenetrable shield against law enforcement surveillance and detection, it is a service in high demand by TCOs. Encrypted communications service providers other than Phantom Secure exist in the market and continue to thrive. Based on my training and experience, I am aware that the continued demand for these encrypted device platforms by criminals is significant. It is primarily driven by the requirements for organized crime, and especially TCOs, to have a trusted method of communications they regard as secure and immune from law enforcement surveillance and interception techniques. TCOs are the target market for this technology because the entire success of their illicit activity is premised on avoiding law enforcement detection. Drug trafficking in particular relies on international, real time coordination by multiple actors. The huge illicit profits in the international drug trade mean they are both willing and able to pay $2000 for a device which has a singular function—sending secure, encrypted messages—in a closed-loop environment. The Phantom Secure investigation showed that hardened encrypted devices are not known to be used by privacy-minded individuals because of the devices' limited functionality and the high cost of a single device.

[2] Ramos' arrest resultantly shut down Phantom Secure. In the time since Ramos' arrest, the FBI has not identified a single legitimate, non-criminal user of Phantom Secure. The FBI provided opportunities for any user of a Phantom Secure device to come forward and retrieve their data. No request was made by any Phantom Secure user to the FBI.

**B. A CHS Gave FBI An In-Development Encrypted Device Company**

12. After Ramos was arrested, San Diego FBI agents recruited a Confidential Human Source ("CHS")[3] who had been developing the "next generation" encrypted communications product, poised to compete for market share against established hardened encrypted device competitors. At the time, the void created by Phantom Secure's dismantlement provided a new opportunity for criminal users to switch to a new, secure brand of device. The CHS previously distributed both Phantom Secure and Sky Global[4] devices to TCOs and had invested a substantial amount of money into the development of a new hardened encrypted device. The CHS offered this next generation device, named "Anom," to the FBI to use in ongoing and new investigations. The CHS also agreed to offer to distribute Anom devices to some of the CHS's existing network of distributors of encrypted communications devices, all of whom have direct links to TCOs. Because encrypted communications devices exist to eschew law enforcement, the distribution of these devices is predicated on trust. This shadowy distribution system is designed, in part, to impede law enforcement's ability to obtain the content from these devices. To prevent law enforcement from obtaining devices, the Phantom Secure investigation revealed that oftentimes, a distributor must vet would-be purchasers of these devices. This vetting

[3] The CHS has been working for FBI agents since 2018 in exchange for the possibility of having a reduced sentence in relation to charges the CHS is facing. The CHS has been paid $120,000 by the FBI for services and $59,508 for expenses related to living and travel expenses. The information and services provided by the CHS in this case are considered reliable because in part, they have been corroborated by recorded communications, interviews, and business records. The CHS has a previous conviction for importing narcotics, for which the CHS was sentenced to six years in prison.

[4] On March 12, 2021, a Grand Jury in the Southern District of California returned an indictment against Sky Global CEO Jean Francois EAP and one of Sky's distributors, Thomas Herdman, which charged a RICO conspiracy predicated on aiding and abetting drug trafficking and obstruction of justice. The announcement of the charges and the service of seizure warrants on Sky Global's infrastructure resultantly shut down Sky Global.

process comes from either a personal relationship or reputational access with a purchaser premised on prior/current criminal dealings. By introducing Anom to the CHS's trusted distributors, who were likewise trusted by criminal organizations, the FBI aimed to grow the use of Anom organically through these networks.

13. The FBI opened a new covert investigation, Operation Trojan Shield, which centered on exploiting Anom by inserting it into criminal networks and working with international partners, including the Australian Federal Police ("AFP"), to monitor the communications. Before the device could be put to use, however, the FBI, AFP, and the CHS built a master key into the existing encryption system which surreptitiously attaches to each message and enables law enforcement to decrypt and store the message as it is transmitted. A user of Anom is unaware of this capability. By design, as part of the Trojan Shield investigation, for devices located outside of the United States,[5] an encrypted "BCC" of the message is routed to an "iBot" server located outside of the United States, where it is decrypted from the CHS's encryption code and then immediately re-encrypted with FBI encryption code. The newly encrypted message then passes to a second FBI-owned iBot server, where it is decrypted and its content available for viewing in the first instance.

14. Each Anom user is assigned to a particular Jabber Identification ("JID") by the CHS or an Anom Administrator. A JID is akin to a "PIN" in Blackberry Messenger. The JID is either a fixed, unique alphanumeric identification, or for more recent devices, a combination of two English words. Anom users can select their own usernames and can change their list of usernames over time. As part of the Trojan Shield investigation, the FBI maintains a list of a JIDs and corresponding screen names of Anom users.

**C. The CHS's Criminal Distributors Get Anom Devices to Only TCOs**

15. The CHS has controlled the distribution of Anom devices in consultation with the FBI. Beginning in October 2018, the CHS began offering these devices to three former

[5] As explained further herein, devices located in the United States are not obtained by the second FBI-owned server because the U.S. is geo-fenced.

Phantom distributors with connections to criminal organizations, primarily in Australia. These three individuals, relying on their expertise from distributing Phantom, and seeing a huge payday, agreed. For this initial "beta test," AFP obtained a court order to legally monitor the Anom devices of the individuals in Australia or with a clear nexus to Australia. Approximately fifty devices were distributed as part of the beta test, and it was a success. Through the interception of these communications, the AFP penetrated two of the most sophisticated criminal networks in Australia. The AFP has shared generally with San Diego FBI the nature of conversations occurring over Anom,[6] which included drug trafficking activity (including discussing the transportation of hundreds of kilograms of narcotics), firearms purchases, and other illegal activity. Moreover, as the FBI saw with Phantom Secure, according to Australian law enforcement, 100% of Anom users in the test phase used Anom to engage in criminal activity. Intercepted conversations have also detailed a willingness among TCO members to provide these devices to senior members of organized crime groups who reside outside of Australia.

16. The growth of devices in Australia was initially slow. It grew organically based on word of mouth from the CHS's criminal distributors and other end-users. Growth ramped up by the summer of 2019. During the successful test in Australia, the CHS saw an increase in demand for devices both inside and outside of Australia. The CHS—in coordination with the FBI—began increasing the distribution of devices to other criminal associates in the CHS's distribution network. Australia continued to monitor these communications.

17. But the FBI itself was not yet reviewing any of the decrypted content of Anom's criminal users. Also by summer of 2019, the investigative team engaged representatives from a third country to receive an iBot server of its own and obtain the contents of communications occurring between Anom users. Negotiations about the

[6] Australia's judicial order to intercept Anom communications did not allow for the sharing of the content with foreign partners.

logistics and legal framework in the third country progressed throughout fall 2019. The third country agreed to obtain a court order in accordance with its own legal framework to copy an iBot server located there and provide a copy to the FBI pursuant to a Mutual Legal Assistance Treaty ("MLAT"). Unlike the Australian beta test, the third country would not review the content in the first instance. FBI geo-fenced the U.S., meaning that any outgoing messages from a device with a U.S. MCC would not have any communications on the FBI iBot server. But if any devices landed in the United States, the AFP agreed to monitor these devices for any threats to life based on their normal policies and procedures.

18. In October 2019, the third country obtained a court order which enabled the copying of the iBot server and the receipt of its contents every two to three days. The initial MLAT between the U.S. and the third country authorized FBI to receive data from October 7, 2019, through January 7, 2020. Due to technological issues with decryption and putting the content into a usable format, the FBI did not begin receiving the actual server content from the third country until October 21, 2019. By this time, there were several hundred users of Anom, with the majority still located in Australia. Since October 2019, the third country has obtained additional court order pursuant to its own laws to copy the iBot server and the United States has obtained the server data pursuant to additional MLATs. The third country provides Anom server data to the FBI every Monday, Wednesday, and Friday, and will continue to do so until the expiration of the third country's court order on June 7, 2021. This data comprises the encrypted messages of all of the users of Anoms with a few exceptions (e.g., the messages of approximately 15 Anom users in the U.S. sent to any other Anom device are not reviewed by FBI).

19. Since October 2019, the FBI has reviewed the content from the iBot server in the third country pursuant to the MLAT. They have translated the messages (where necessary and where translations are available) and have catalogued more than 20 million messages from a total of 11,800 devices (with approximately 9000 active devices currently)

located in over 90 countries. The following graphic shows the locations of Anom users around the world:


The top five countries where Anom devices are currently used are Germany, the Netherlands, Spain, Australia, and Serbia.

20. The Trojan Shield investigation has uncovered that Anom devices are used by TCOs to traffic drugs and launder the proceeds of those drug sales. The distributors of these devices also obstruct justice by remotely wiping the content of devices when law enforcement seizes them. Additionally, the review of Anom messages has initiated numerous high-level public corruption cases in several countries. The most prominent distributors are currently being investigated by the FBI for participating in an enterprise which promotes international drug trafficking, money laundering, and obstruction of justice. The FBI has identified, with the recent assistance of a Task Force at Europol, over 300 distinct TCOs using Anom, including Italian organized crime, Outlaw Motorcycle Gangs, and various international narcotics source, transportation, and distribution cells. I have reviewed a portion of messages on the Anom platform since October 2019, and I have

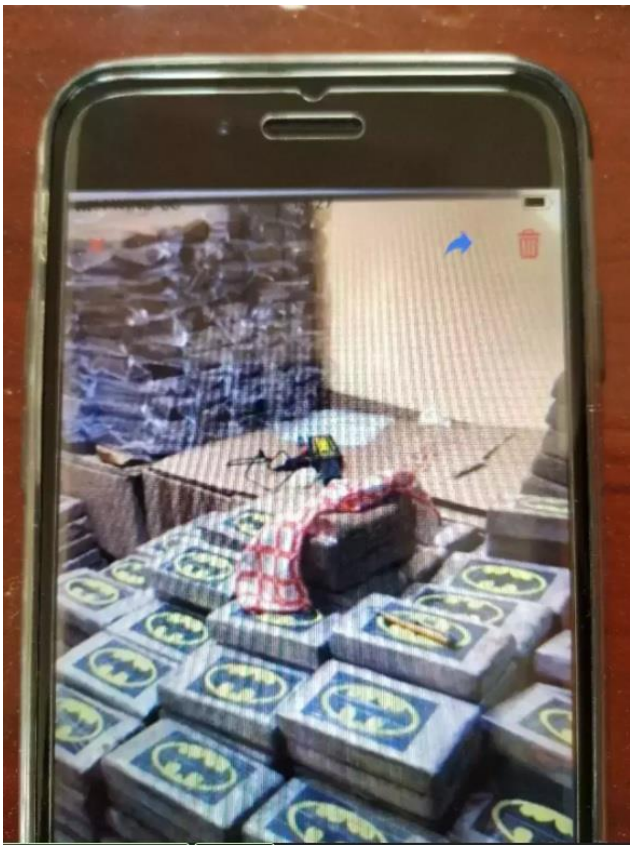
talked to other FBI agents who have reviewed the content. Based on my familiarity with FBI's the review of content from all international Anom users and my experience investigating transnational criminal organizations, I believe that Anom devices are used exclusively to openly discuss criminal schemes or to maintain relationships in furtherance of those schemes.

21. The Trojan Shield investigation has unveiled how criminal organizations compartmentalize their activities with multiple brands of hardened encrypted devices. For example, some users assign different types of devices to different parts of a drug trafficking transaction. For example, I have seen conversations where Anom is used for the logistics of the drug shipments, but Ciphr or Sky were used to coordinate the concealment of the illicit proceeds. This compartmentalization shows the inter-connectivity of the encrypted communications device industry. The interconnectedness was also apparent in the increase in demand when two major platforms were dismantled during the Trojan Shield investigation. First, in July 2020, European investigators announced an investigation into EncroChat which led to its dismantlement. Demand for Anom devices from criminal groups increased after this announcement. Additionally, in March 2021, the announcement of charges against Jean Francois Eap and the dismantlement of Sky Global resulted in a massive increase in demand for Anom devices by criminal organizations. Before Sky's dismantlement, there were approximately 3,000 active Anom users. Since March 12, 2021, as a direct result of the Sky Global charges, there are now close to 9000 active Anom users. The criminals who use hardened encrypted devices are constantly searching for the next secure device, and the distributors of these devices have enabled criminals' impenetrable communications on these devices for years. A goal of the Trojan Shield investigation is to shake the confidence in this entire industry because the FBI is willing and able to enter this space and monitor messages.

**D. Examples of Criminal Conversations on Anom**

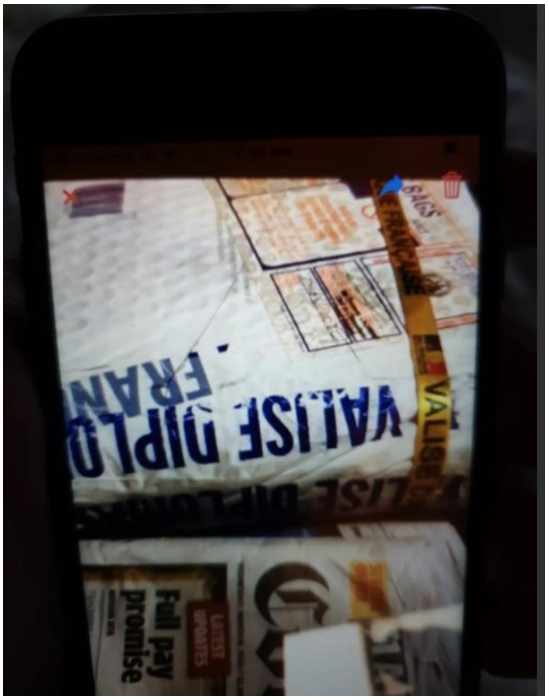
22. The following conversations area a small but representative sample of the criminal content of that the FBI has reviewed of overseas Anom devices since October 2019.

23. On January 4, 2020, the user of JID b14f2c, who has been identified through review of Anom messages as Domenico Catanzariti, and JID 31bcf1, who has been identified as Salvatore Lupoi, discussed the cocaine supply of "atlas." Catanzariti said that the batman photo "was all atlas stock" and "Thi[n]k he got it in." Lupoi responded, "Your dreaming. You reckon. What he offer it to you for." Catanzariti then asked what Lupoi meant and whether Atlas sent the same photo in which atlas said it was all his. Lupoi said he never got the photo. Catanzariti responded that Lupoi was the one who sent it to him one month ago. Catanzariti then sent the following photo to Lupoi of Atlas's supply, which showed hundreds of kilograms of cocaine with a batman label.



Lupoi then asked Catanzariti what price he is telling them for pieces. Catanzariti suggested 150 or 160 (150,000-160,000 AUD/kilogram). Lupoi agreed that 160 maximum was the right price.

24. On March 23, 2020, the user of JID 58f4a9, who has been identified through Anom messages as Baris Tukel, asked the user of JID cfdf8a, who has been identified as Shane Geoffrey May, what the price of cocaine is at the moment. Tukel also asked if May had "that building block address." May replied that cocaine was around the 200k mark and asked if Tukel had some news. Tukel wrote, "Ok sweet, i got a small job that popped up for [t]he building block" and "There is 2kg put inside french diplomatic sealed envelopes out of Bogotta [sic]" and "They have already got a few packages in." Tukel added, "Only issue is that COL takes 50/4 Partners including yourself will need to split other 50" (meaning the Colombian distributors take 50% of the profits while four other people split the other 50%). Tukel wrote, "They can do it weekely [sic]" (meaning packages containing two kilograms can be sent every week). May responded that this sounded good and he would send the address shortly. Tukel then sent three photos: two of the French diplomatic pouches and one of the available cocaine to send.




After sending the photo of cocaine packages, Tukel wrote, "There waiting to be sent from this crew." Tukel added later in the conversation, "They landed these jobs in brisbane (Australia) already."

25. On May 29, 2020, the user of JID c2c367, with username "Real G" wrote to the user of JID 08511a, with username IRONMAN, "South side asked what the prices [are] in HK [Hong Kong] per piece [kilogram of narcotics]? What's the entry fee? And if they have someone in port to clear it? They secure exit 90% just if Bogota police got info about it then they are above it. Ask HK if they can receive banana cause turbo [Port of Turbo, Colombia] sends banana to HK to will be good if possible cause this will be finished product." IRONMAN responded that he couldn't tell the price per piece in Hong Kong because Hong Kong is very different and said right now the price for a kilogram is Australia

is about 100,000. IRONMAN also said there was "no one in port to clear it" meaning they had no corrupt official available to see the drugs successfully enter. IRONMAN asked how the drugs were hidden in bananas. Real G responded, "They packed the work [narcotics packages] inside the boxes." Real G sent the following photo of narcotics packages (suspected cocaine based on the shape and size) packed into a banana shipment:


Real G added, "They cover this with a layer of banana." They then discussed needing to do a few legitimate shipments "since no one in HK door."

26. In October 2020, a TCO orchestrated a shipment of cocaine from Ecuador to Belgium to be imported via a shipping container concealed within cans of tuna. The FBI reviewed the content of messages from the TCO. Those messages revealed that the TCO discussed the logistics of the importation, and shared container information. This information was passed to U.S. authorities in Brussels, who worked with law enforcement agencies in Belgium to search the suspected container. Upon completion of the search, law enforcement located approximately 613 kilograms of cocaine. Furthermore, information identifying the Ecuadorian tuna company was passed to law enforcement in

Ecuador, which resulted in an additional seizure of approximately 1,523 kilograms of cocaine located in a container destined for Antwerp, Belgium.

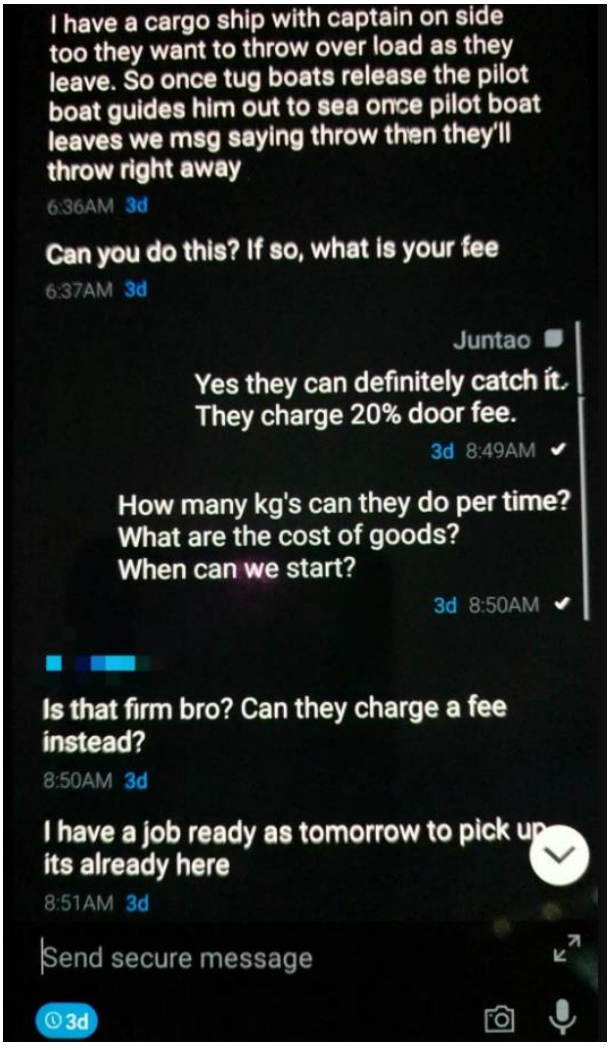

27. In April of 2021, a TCO orchestrated a shipment of cocaine (using Anom devices) from Ecuador to Spain to be imported via shipping container concealed within refrigerated fish. The FBI and law enforcement officials in Spain reviewed the messages which contained specific details regarding the shipment and distribution once it arrived in Spain. The suspected container arrived into the Port of Algeciras, Spain on April 29, 2021. Law Enforcement officials in Spain conducted a search of the container and upon completion located approximately 1401 kilograms of cocaine.

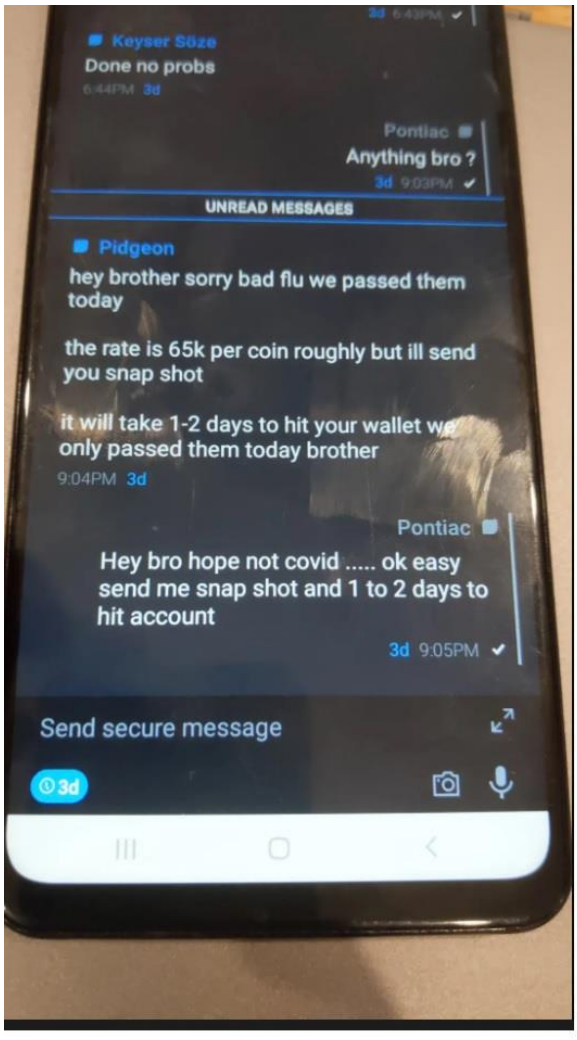
28. In May of 2021, a TCO orchestrated a shipment of cocaine (using Anom devices) from Costa Rica to Spain to be imported via shipping container concealed within hollowed out pineapples. The FBI and law enforcement officials in Spain reviewed the messages which contained specific details regarding the shipment and distribution once it arrived in Spain. The suspected container arrived into the Port of Algeciras, Spain on May 12, 2021. Law Enforcement officials in Spain conducted a search of the container and upon completion located approximately 1595 kilograms of cocaine.


29. The conversations detailed above are a small sample set pulled from more than 20 million messages that FBI reviewed of Anom's criminal users. From those messages, more than 450,000 photos have been sent detailing conversations on other encrypted platforms discussing criminal activity, cryptocurrency transactions, bulk cash smuggling, law enforcement corruption[7], and self-identification information. A representative sample of photos has been included below, which includes bulk cash proceeds of illegal transactions, GPS location of narcotics shipments, and discussions of criminal activity on other encrypted devices:

[7] Information reviewed on the platform has revealed law enforcement sensitive information passed to TCOs, such as reports and warrants. TCOs have also been notified of anticipated enforcement actions against the TCO or other criminal associates.


緯度: -18.345037
經度: 81.192827
Degree


I have a cargo ship with captain on side too they want to throw over load as they leave. So once tug boats release the pilot boat guides him out to sea once pilot boat leaves we msg saying throw then they'll throw right away
6:36AM 3d
Can you do this? If so, what is your fee
6:37AM 3d
Juntao
Yes they can definitely catch it. They charge 20% door fee.
3d 8:49AM
How many kg's can they do per time? What are the cost of goods? When can we start?
3d 8:50AM
Is that firm bro? Can they charge a fee instead?
8:50AM 3d
I have a job ready as tomorrow to pick up its already here
8:51AM 3d
Send secure message
3d

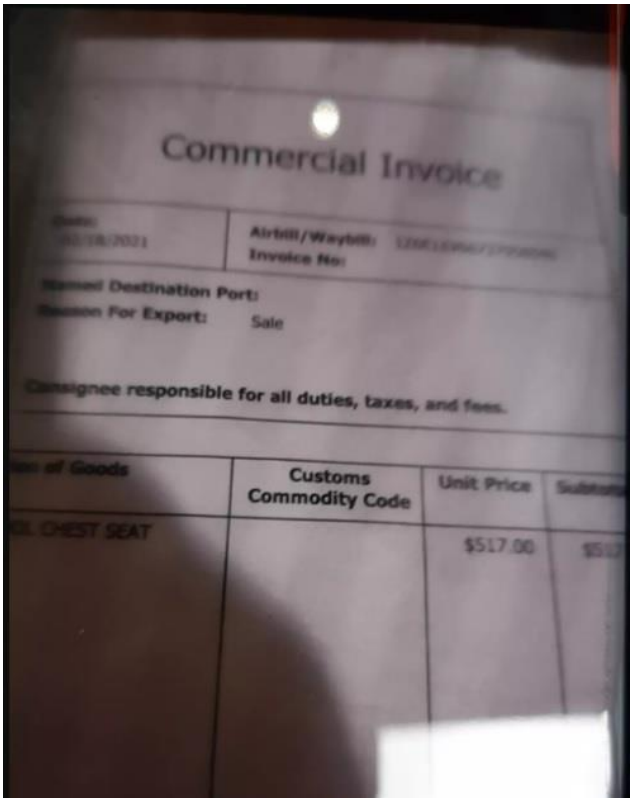

Keyser Söze
Done no probs
6:44PM 3d
Pontiac
Anything bro ?
3d 9:03PM
UNREAD MESSAGES
Pidgeon
hey brother sorry bad flu we passed them today
the rate is 65k per coin roughly but ill send you snap shot
it will take 1-2 days to hit your wallet we only passed them today brother
9:04PM 3d
Pontiac
Hey bro hope not covid ..... ok easy send me snap shot and 1 to 2 days to hit account
3d 9:05PM
Send secure message
3d


**E. Identification of the Subject Account and Probable Cause to Search**

30. On February 25, 2021, JID 11096a (with username TOM FORD) forwarded a message from JID 700204 (with username Sion) that stated, "We are on standbys to receive the package today bro. Tell him the two available addresses for now is the hotel and the mechanic shop. The next mechanic shop and hotel I waiting on final approval to have them on board." Sion responded, "I understand brother, but now I can't send on this two addresses, because it will be more packages to send in same address," "I can send to same address one time every week, in this way it will be safe," "6kgs," and "If I have more addresses I can send more KGS." TOM FORD replied, "Ok my brother we will have don't worry." Sion replied, "Thanks brother, let start work with more KGS brother."

31. Later in the same conversation, TOM FORD sent two photographs of a commercial invoice to Sion. The invoice appeared to be for a "Chest Seat" sent from "Liam Davis" with address: Lowe's Home Improvement at 2515 Palomar Airport Road, Carlsbad, CA 92008 USA, phone number 760-331-0195, and email address

expliamdavis@gmail.com (Subject Account). I am aware that this is the correct address and phone number for a Lowe's store Carlsbad (which is in the Southern District of California). According to Anom metadata records, at the time of this conversation, TOM FORD was likely located in Australia and Sion was likely located in Armenia.





32. The consignee for the shipment was "Pro Worx Performance" at 288 Princes Hwy, Banksia NSW 2216, Australia with phone number +61-403-305-460. Based on public records, I am aware that there is a mechanic called Pro Worx Performance at 28**6** Princes Hwy with the same telephone number as provided in the consignee information.

33. After TOM FORD sent these photos, Sion expressed relief "because package is ready I want to send today, I ordered next KGS to prepare for sending." In the same string of messages, TOM FORD and Sion sent photos of cocaine bricks to each other and claimed it was from America and on the way to Europe.

34. I believe, based on the content of these conversations and my knowledge of how Anom devices are used, that TOM FORD and Sion coordinated the shipment of likely six kilograms of cocaine from Carlsbad to Australia in February 2021. I believe they also discussed further transactions as soon as additional delivery addresses in Australia could be procured.

35. Based on the discussions above and other conversations I have reviewed, I believe that this TCO involving TOM FORD and Sion is using shipping information from real businesses to concealing narcotics shipments. I believe the group will continue utilizing email accounts, including the Subject Account, to transmit invoices, Bill of Lading information, and shipping information and to further coordinate narcotics transactions. The TCO has specifically used the Subject Account in at least one shipment of a suspected cocaine transaction from Carlsbad, California, to Australia. This email account will likely contain evidence of the TCO's drug trafficking activities in the past and may assist in identifying future shipments and identifying the users of the Subject Account, who are involved in distribution of controlled substances.

36. I respectfully request permission to obtain the content from the Subject Account from January 1, 2021, to May 17, 2021, because the specific narcotics trafficking

job was first discussed in February 2021 and I have probable cause to believe that evidence, as outlined in Attachment B, may be present from this time period. Based on my training and experience, I am aware that the narcotics concealment methods take many months to accomplish. I am also aware that oftentimes several "dry runs" are tested before any narcotics are actually sent, which still require the use of email correspondence to set up and use as proof of the shipping transaction. These "dry runs" monitor the speed at which a shipment occurs, if there are any issues in customs in the exporting or importing country, and whether the transportation channels are in place. Thus, evidence of planning and preparation may be present on the Subject Account for several months before an actual narcotics shipment is sent. I also respectfully request permission to search the subject account from January 1, 2021, until May 17, 2021, because TOM FORD and Sion alluded to additional kilogram quantity shipments in the future. Based on their conversations over Anom, I believe they or co-conspirators may have continued using the Subject Account for future narcotics transactions.

BASIS FOR EVIDENCE SOUGHT IN SEARCH WARRANT

37. Based on my training and experience, consultation with other law enforcement officers experienced in international maritime narcotics smuggling investigations, and all the facts and opinions set forth in this affidavit, I believe that probable cause exists that the Subject Account is being used to conceal the distribution of controlled substances aboard maritime vessels and that the following evidence may be found stored on the premises of Google LLC in relation to the Subject Account:

a. Communications, records, and attachments tending to discuss or establish the creation of businesses, records, invoices, transactions, Bill of Lading information, and shipping information to conceal the distribution of controlled substances or to set up test runs of such shipments;

b. Communications, records, and attachments tending to discuss the legitimate cargo or details of the modes of transportation being used conceal the distribution of narcotics or to set up test runs of such shipments;

c. Communications, records, and attachments tending to identify the individuals and locations sourcing the concealed narcotics as well as the recipient individuals and locations and Ports of the concealed narcotics;

d. Communications, records, and attachments tending to identify the users of screen names TOM FORD, Sion, and any co-conspirators (such as Liam Davis) involved in the activities in III(a)-(c) above; and

e. Communications, records, and attachments that provide context to any communications described above, such as electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail tending to identify user(s) of the subject account.

GENUINE RISKS OF DESTRUCTION OF EVIDENCE

38. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, electronically stored data can be permanently deleted or modified by users possessing basic computer skills. In this case, only if the subject receives advance warning of the execution of this warrant, will there be a genuine risk of destruction of evidence.

PRIOR ATTEMPTS TO OBTAIN THIS EVIDENCE

39. The United States has not attempted to obtain this data by other means.

THE SERVICE PROVIDER

40. Google LLC is an Internet company that, among other things, provides electronic communication services to its subscribers. Google LLC's electronic mail service (Gmail) allows its subscribers to exchange electronic communications with others through the Internet. ISP subscribers access ISP's services through the Internet.

41. Subscribers to Google LLC use screen names during communications with others. The screen names may or may not identify the real name of the person using a particular screen name. Although Google LLC requires users to subscribe for a free Google account, Google LLC does not verify the information provided by the subscriber for its free services.

42. At the creation of a Google account and for each subsequent access to the account, Google LLC logs the Internet Protocol ("IP") address of the computer accessing the account. An IP address is a unique address through which a computer connects to the Internet. IP addresses are leased to businesses and individuals by Internet Service Providers. Obtaining the IP addresses that have accessed a particular Google account often identifies the Internet Service Provider that owns and has leased that address to its customer. Subscriber information for that customer then can be obtained using appropriate legal process.

PROCEDURES FOR ELECTRONICALLY STORED INFORMATION

43. Federal agents and investigative support personnel are trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. It would be inappropriate and impractical for federal agents to search the vast computer network of Google for the relevant accounts and then to analyze the contents of those accounts on the premises of Google LLC. The impact on Google LLC's business would be disruptive and severe.

44. Therefore, I request authority to seize all content, including electronic mail and attachments, stored instant messages, stored voice messages, photographs, and any other content from the Google account, as described in Attachment B. In order to accomplish the objective of the search warrant with a minimum of interference with the business activities of Google LLC, to protect the privacy of ISP subscribers whose accounts are not authorized to be searched, and to effectively pursue this investigation, FBI seeks authorization to allow Google LLC to make a digital copy of the entire contents of the

account subject to seizure. That copy will be provided to me or to any authorized federal agent. The copy will be imaged and the image will then be analyzed to identify communications and other electronic records subject to seizure pursuant to Attachment B. Relevant electronic records will be copied to separate media. The original media will be sealed and maintained to establish authenticity, if necessary.

45. Analyzing the data to be provided by Google LLC may require special technical skills, equipment, and software. It may also be very time-consuming. Searching by keywords, for example, often yields many thousands of "hits," each of which must be reviewed in its context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keyword searches do not capture misspelled words, reveal the use of coded language, or account for slang. Keyword searches are further limited when electronic records are in or use foreign languages. Certain file formats also do not lend themselves to keyword searches. Keywords search text. Many common electronic mail, database and spreadsheet applications, which files may have been attached to electronic mail, do not store data as searchable text. Instead, such data is saved in a proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases dramatically. The ISPs do not always organize the electronic files they provide chronologically, which makes review even more time consuming and may also require the examiner to review each page or record for responsive material.

46. Based on the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. Keywords need to be modified continuously based upon the results obtained and, depending on the organization, format, and language of the records provided by the ISP, examiners may need to review each record to determine if it is responsive to Attachment B. The personnel conducting the examination will complete

the analysis within ninety (90) days of receipt of the data from the service provider, absent further application to this court.

47. Based upon my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize all electronic mails that identify any users of the Subject Account and any electronic mails sent or received in temporal proximity to incriminating electronic mails that provide context to the incriminating mails.

48. All forensic analysis of the imaged data will employ search protocols directed exclusively to the identification and extraction of data within the scope of this warrant.

REQUEST FOR SEALING & PRECLUSION OF NOTICE

49. This is an ongoing investigation of which the targets are unaware. Specifically, this sophisticated, covert FBI investigation is currently operating in over 90 countries. The FBI is targeting almost two dozen of the Anom platform's Administrators and Distributors its investigation. Other countries have opened investigations into the criminal end users of these devices. The Subject Account is directly connected to a target of the FBI's investigation. The Trojan Shield investigation is anticipated to be concluded at the expiration of the third country's warrant period on June 7, 2021, and the investigation will be publicly announced on June 8, 2021. Until then, the continued success of the investigation depends on maintaining the secrecy of the FBI's role in Anom. If notice of this warrant were served on the user and/or subscriber of the Subject Account immediately, it could result in flight from prosecution of the user of the subject account and his co-conspirators, destruction of evidence (including many encrypted devices), or otherwise seriously jeopardize the ongoing investigation by compromising the trust that the targets of the investigation have put into the device. Additionally, it is believed that premature disclosure could endanger the life and safety of the CHS. It is very likely, based upon the above, that evidence of the crimes under investigation exists on computers and devices subject to the control of the targets. There is reason to believe, based on the above, that

premature disclosure of the existence of the warrant will result in destruction or tampering with that evidence and seriously jeopardize the success of the investigation. Accordingly, it is requested that this warrant and its related materials be sealed until June 7, 2021, absent further order of the Court.

50. In addition for the same reasons, pursuant to Title 18, United States Code, Section 2705(b), it is requested that this Court order the electronic computing service provider to whom this warrant is directed not to notify anyone of the existence of this warrant, other than its personnel essential to compliance with the execution of this warrant, until June 7, 2021, absent further order of the Court.

## CONCLUSION

51. Based on the foregoing, there is probable cause to believe that the items identified in Attachment B have been used in the commission of a crime and constitute evidence, fruits, and instrumentalities of violations of Title 21, United States Code, Sections 841, 846 and will be found at the premises to be searched as provided in Attachment A.

NICHOLAS I. CHEVIRON
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 17th day of May, 2021

HON. MICHAEL S. BERG
U.S. MAGISTRATE JUDGE

# ATTACHMENT A

Google LLC is an Internet Service Provider with its primary computer information systems and other electronic communications and storage systems, records and data located at 1600 Amphitheater Parkway, Mountain View, California 94043.

# ATTACHMENT B

**I.** Service of Warrant

The officer executing the warrant shall permit Google LLC, as custodian of the computer files described in Section II below, to locate the files and deliver digital copies to the officer.

**II**. Items to be provided by Google LLC

Subscriber and/or user information, electronic mail, images, text messages, histories, phone and VoIP logs, contacts or friend lists, profiles, method of payment, detailed billing records, access logs, backup data, transactional data, and any other files or records associated with the following account and screen name:

**expliamdavis@gmail.com**

**III**. The search of the data supplied by Google LLC pursuant to this warrant will be conducted by the FBI as provided in the "Procedures For Electronically Stored Information" of the affidavit submitted in support of this search warrant and will be limited to the period of January 1, 2021, to May 17, 2021, and to the seizure of:

a Communications, records, and attachments tending to discuss or establish the creation of businesses, records, invoices, transactions, Bill of Lading information, and shipping information to conceal the distribution of controlled substances or to set up test runs of such shipments;

b. Communications, records, and attachments tending to discuss the legitimate cargo or details of the modes of transportation being used conceal the distribution of narcotics or to set up test runs of such shipments;

c. Communications, records, and attachments tending to identify the individuals and locations sourcing the concealed narcotics as well as the recipient individuals and locations and Ports of the concealed narcotics;

d. Communications, records, and attachments tending to identify the users of screen names TOM FORD, Sion, and any co-conspirators (such as Liam Davis) involved in the activities in III(a)-(c) above; and

e. Communications, records, and attachments that provide context to any communications described above, such as electronic mail sent or received in temporal proximity to any relevant electronic mail and any electronic mail tending to identify user(s) of the subject account.

**which are evidence of violations of Title 21, United States Code, Sections 841(a)(1), 846.**