

IN THE UNITED STATES DISTRICT COURT
FOR WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

IN THE MATTER OF THE SEARCH OF
INFORMATION AND RECORDS
ASSOCIATED WITH GOOGLE EMAIL,
YOUTUBE, GOOGLE PLUS, and BLOGGER
ACCOUNTS THAT ARE STORED AT
PREMISES CONTROLLED BY GOOGLE
LLC OR GOOGLE PAYMENT CORP.

Case No. 1:18-m-218

FILED
2018 MAR 27 AM 10:26
CLERK OF DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY g

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, **Scott Kibbey**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with Google accounts related to Google e-mail, YouTube, Google Plus, and Blogger accounts that are stored at premises owned, maintained, controlled, or operated by Google, LLC. or Google Payment Corporation ("Google"), a networking and remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) and Rule 41 of the Federal Rules of Criminal Procedure to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I have been employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) since November since 2011. I am currently designated as a Cyber agent

assigned to the Austin Resident Agency of the San Antonio Field Office. I have received formal and on the job training in cyber crime investigation techniques, computer evidence identification, and computer evidence seizure and processing. As a Federal Agent, I am authorized to investigate violations of laws of the United States and to execute warrants issued under the authority of the United States. I have participated in the execution of numerous search warrants for documents and other evidence, including computers and electronic media, in cases involving crimes the FBI is authorized to investigate. I am a "federal law enforcement officer" within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. I am engaged in enforcing federal criminal laws and am authorized by the Attorney General to request a search warrant, among other things.

3. I have participated in the investigation of the offense(s) listed herein. This affidavit is based on my personal knowledge as well as reports made by other law enforcement officers from agencies to include the FBI, Austin Police Department (APD), Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF), the U.S. Postal Inspection Service (USPIS), and others. Because this affidavit is being submitted for the limited purpose of establishing probable cause for the issuance of a search warrant, it does not contain every fact known to me or other agents of the Federal Bureau of Investigation. Additionally, the incidents described herein occurred a short time ago and the investigation is ongoing.

4. The APD, ATF, FBI, USPIS, and other agencies are investigating a series of bombings that occurred in Austin, Texas, which is within the Western District of Texas, in March 2018. Preliminary analysis of the bombings revealed that several of the explosive devices were pipe bombs. Those devices are each legally classified as a Destructive Device as defined by Title 26 United States Code § 5845. Title 26 United States Code § 5861 makes it unlawful for

any person to possess a firearm (“firearm” is defined as including a Destructive Device) that is required to be registered with the National Firearms Registration and Transfer Record and is not so registered. Title 26 United States Code § 5861 also makes it unlawful to transfer a firearm (including a Destructive Device) to a person to whom the firearm is not registered.

5. There is probable cause that the accounts listed Attachment A belong to Mark Conditt, the perpetrator of the bombings, and probable cause that information associated with the Google accounts and other linked Google accounts contain additional evidence related to the bombings. Among other things, the information may help law enforcement identify other persons who may have knowledge about the bombings..

6. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 26, United States Code, Section 5861 have been committed by Mark Conditt, who may have been assisted by one or more unknown subjects. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711 and 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

DEFINITIONS

The following definitions apply to this Affidavit and Attachment B:

9. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.” See 18 U.S.C. § 1030(e)(1).

10. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) could assign a different unique IP address to a computer every time it accesses the Internet. IP addresses might also be static, if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet.

11. A User Agent String (UAS) is the text that programs use to identify themselves to servers, such as web servers, for usage tracking and other purposes. A UAS identifies a user’s web browser and provides certain system details to the services hosting the website a user visits that the server uses to provide content back to the user that is tailored to their respective environment. Web browsers collect UAS of all visitors to a webpage in order to provide the visitor a version of the website that is properly formatted for their web browser. A UAS provides details about the hardware and software the user might be using to visit the webpage such as operations system, web browser version, and occasionally hardware manufacturer of the device used to visit the webpage.

BACKGROUND INFORMATION ABOUT GOOGLE

12. In my training and experience, I have learned that Google provides a variety of

online services, including, but not limited to, Google Search, a web search engine, and YouTube, a video sharing website, to the public. Google also maintains records of the IP addresses associated with searches conducted on Google Search and YouTube. YouTube allows users to communicate with each other in the “comments” section below the video. YouTube also allows users to post videos privately, restricting access to the content. Additionally, I know that Google keeps records of the YouTube videos viewed by particular users. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain information concerning users and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

13. In my training and experience, Google generally asks its subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). Such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

14. In my training and experience, Google retains certain transactional information about the creation and use of each account on its systems. Google also maintains transactional

information about users who access a Google account. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers, mobile devices, or other electronic devices were used to access the email account

15. As explained herein, information stored in connection with a Google account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element of an offense, or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with a Google account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

16. Further, I know that information maintained by Google can show how and when the account was accessed or used. Google also collects and maintains location information pertaining to an account and the use of various Google services. For example, as described below, Google typically logs the Internet Protocol (IP) addresses from which users access a Gmail account, along with the time and date of that access, and location data for the device(s) logged into the account. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account

access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner, but can also help locate the device that has logged into a Google account.

17. In my training and experience, e-mail providers typically retain sign-in, session state, and site cookies. E-mail providers also retain information linking accounts by sign-in, session state, and site cookies. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

18. Web browsers collect User Agent Strings (UAS) of all visitors to a web page in order to provide the visitor a version of the website that is properly formatted for their web browser. A UAS provides details about the hardware and software the user might be using to visit the webpage; such as operating system, web browser version, and occasionally hardware manufacturer of the device used to visit the web page. These details will aid in identifying persons searching for information in connection with the aforementioned bomb threats.

19. Previous investigations and legal process have confirmed that this information does exist and can be provided with an appropriate court order with a narrow time frame for the requested terms.

20. Therefore, the computers of Google are likely to contain all the material described above, including stored electronic search terms. It is requested that Google provide any IP addresses, User Agent Strings, and associated Google account information as further described in Attachment B, that entered the search terms in Attachment A into Google Search and/or YouTube during the prescribed timeframes.

21. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.¹

FACTS

22. Your Affiant is familiar with the information contained in this affidavit, either through personal investigation or through reports and discussion with other law enforcement officers, who have participated in and have contributed their investigative efforts in this matter.

23. Between March 2 and March 20, 2018, five explosive devices detonated in and around Austin, and an additional explosive device was recovered, all at locations within the Western District of Texas. Two people were killed in these explosions, and five people were injured. Two of the explosive devices were sent on March 18, 2018, from a FedEx location on Brodie Lane in Austin, Texas.

¹ It is possible that Google stores some portion of the information sought outside of the United States. In Microsoft Corp. v. United States, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information – including data stored outside the United States – pertaining to the identified account(s) that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where information responsive to this warrant is/are stored.

24. Investigation by law enforcement, including interviews with witnesses, review of surveillance video, analysis of physical and electronic records, and examination of the explosive devices by ATF Special Agents, led investigators to believe that Mark Conditt was responsible for all six explosive devices. ATF analysis to date indicates that all of these explosive devices constituted Destructive Devices under federal law.

25. Based on the information collected during this investigation, on March 20, 2018, this Court issued a Complaint and Arrest Warrant for Mark Conditt in cause number A-18-m-207(1). Law enforcement attempted to execute this arrest warrant in the early morning hours of March 21, 2018.

26. The details of the events that occurred on March 21, 2018 are still under investigation, but my understanding, based on discussions with other law enforcement, is as follows. On March 21, 2018, at approximately 1:00 am, Mark Conditt was located in a hotel parking lot. At approximately 1:57 am, while officers on the scene were waiting for backup, Conditt exited the parking lot and headed southbound on I-35 Frontage road. Law enforcement units rammed Conditt's vehicle from behind and boxed in his vehicle on the shoulder of the Frontage Road. As officers approached the vehicle and attempted to take Conditt into custody, Conditt apparently detonated an explosive device within the vehicle. Although confirmation has not yet been provided from the Medical Examiner, it appears that Mark Conditt is deceased.

27. Evidence recovered from the vehicle confirmed that Mark Conditt had been the sole occupant and driver. A recording was recovered from a device within the vehicle, in which Conditt confessed his responsibility for setting the explosive devices described above.

28. A search warrant was executed on Conditt's home on March 21, 2018. Due to the likelihood of Destructive Devices and other dangerous materials being present, law enforcement

proceeded with caution and continued the search through March 22, 2018. Inside Conditt's bedroom, law enforcement located Destructive Device-making equipment, fraudulent paper license plate tags, a wig similar in appearance to that seen in the FedEx footage, over 100 pounds of ammonium nitrate, and other materials that could be used to manufacture additional Destructive Devices.

29. Although Conditt is believed dead, law enforcement continues to investigate where and how Conditt acquired the materials and knowledge required to construct Destructive Devices, as well as his motivation in placing the Destructive Devices at the locations he chose. Additionally, investigators wish to determine if Conditt had any aiders, abettors, accessories after the fact, or coconspirators.

30. Information from social media revealed that Mark Conditt was utilizing a cellular telephone with number [REDACTED]. Records revealed that [REDACTED] is registered to Mark Conditt's father.

31. Open source queries for "Mark Conditt" yielded a Google Plus account for a Mark Conditt, <https://plus.google.com/116427204794402574361>. Google records show that the Google Plus account and phone number [REDACTED] were associated with mark.conditt1425@gmail.com. The phone number, [REDACTED] was also associated with markconditt@gmail.com. The mark.conditt@gmail.com was associated with a mobile device with the same ID as lucasdanny580@gmail.com. Therefore, I believe that Conditt utilized all three Google accounts and emails.

32. Preliminary analysis of online searches associated with the account, lucasdanny580@gmail revealed searches for the location of the FedEx where two of the devices were mailed from on March 18, 2018, prior to Conditt mailing the packages at the FedEx. Other

searches included directions to Conditt's parents in Pflugerville, Texas, Home Depot, Fry's Electronics, various shipping companies, and other various commercial and residential addresses.

33. Records show that Blogger profile ID 08558225658664573125 of the blog definingmystance.blogspot.com was associated with the mark.conditt@gmail.com e-mail address. Additionally, the YouTube channel vANX3KyVcYRq3ImMvzujtQ and associated URL <http://www.youtube.com/channel/UCvANX3KyVcYRq3ImMvzujtQ>, were also associated with the mark.conditt@gmail.com e-mail address.

34. In my training and experience and that of other law enforcement with expertise in Destructive Device making and explosives, I know and have learned that Destructive Device manufacturers often research their targets using the internet and electronic means. Destructive Device-makers often research methods of constructing Destructive Devices, as well as information related to motive for using explosives, using the internet and other electronic devices. Searches for YouTube videos are a popular means to research methods of "how to build" various items and devices.

35. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 26, United States Code, Section 5861 have been committed by Mark Conditt. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

36. Based on my investigative experience and knowledge provided by other law enforcement officers, information associated with the Google accounts and other linked Google

accounts may contain additional evidence related to the bombings, and may help law enforcement identify persons who may have knowledge about the bombings.

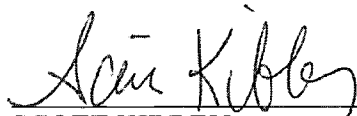
CONCLUSION

37. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, there exists reasonable cause to permit the execution of the requested warrant during any time, day or night.

REQUEST FOR SEALING

38. I further request that the Court orders that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, some of the facts of which are not public, and there may be additional targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize this investigation.

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



SCOTT KIBBEY
Special Agent
Federal Bureau of Investigation
Austin, Texas

Subscribed and sworn to before me at Austin, Texas, on this 27 day of March, 2018.



HON. MARK LANE
UNITED STATES MAGISTRATE JUDGE