AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Information associated with dclarke.cowboy@gmail.com that is stored at premises controlled by Google, Inc.

Case No. 17-M-014

APPLICATION FOR A SEARCH WARRANT

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:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ■ 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 violations of: Title 18, U.S.C., Section 242
Title 18, U.S.C., Section 241

The application is based on these facts: See attached affidavit.

☐ 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

Special Agent Jennifer Walkowski, FBI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: March 7, 2017

Judge's signature

City and State: Milwaukee, Wisconsin

Honorable David E. Jones, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jennifer Walkowski, 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 a certain account that is stored at premises controlled by Google, Inc., an email provider headquartered in Mountain View, CA. 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) to require Google, Inc. 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 am a Special Agent with the Federal Bureau of Investigation, and have been since November 2, 2003. Since December 2009, I have been assigned to the Milwaukee Field Office, and prior to that I was assigned to the Baltimore Field Office. Since entering on duty, I have been assigned to work criminal investigations involving violations of federal law, including but not limited to Bank Robbery, Kidnapping, Theft of Government Property, Wire Fraud, Mail Fraud, Money Laundering, Bank Fraud, Mortgage Fraud, Healthcare Fraud, Public Corruption, and Civil Rights violations.

3. By virtue of my FBI employment as a field office case agent, I perform and have performed a variety of investigative tasks, including the execution of search warrants for both physical and electronic evidence. During the 13 years of my employment, I have received regular training on each of the criminal programs I am assigned to investigate.

4. This affidavit is based upon my investigation as well as the investigation and reports of other investigating agencies that I find trustworthy and reliable. Some of the information used to demonstrate the probable cause for this warrant has come from other investigators also assigned to work this matter, as described below. 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.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 242 (Deprivation of Rights Under Color of Law) and 18 U.S.C. § 241 (Conspiracy of Rights) have been committed by Milwaukee County Sheriff David Clarke. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

JURISDICTION

6. 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. 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).

PROBABLE CAUSE

Case Background

7. On February 9, 2017, the Federal Bureau of Investigation (FBI) - Milwaukee Office received a packet of reports from the Forensic Audit Manager for the Milwaukee County Office of the Comptroller - Audit Services Division (ASD), which included a report of ASD's investigation of a complaint by citizen, Dan Black, against Milwaukee County Sheriff David Clarke. The reports were forwarded to the FBI for review and determination as to whether the

actions of Sheriff David Clarke were a violation of federal criminal civil rights statutes. The ASD report outlined ASD's investigation regarding an incident which occurred on January 15, 2017 at General Mitchell International Airport in Milwaukee, WI.

8. ASD is responsible for auditing the fiscal concerns of Milwaukee County, which includes examining financial statements, reviewing internal accounting and administrative controls, assuring compliance with applicable laws and regulations, and assuring the effectiveness in achieving program results. In addition, ASD maintains a hotline service to receive information regarding waste, fraud, and abuse of Milwaukee County resources.

9. On January 18, 2017, the ASD investigators interviewed Dan Black and reviewed Black's formal written complaint that he filed with the Milwaukee County Executive's Office. Black stated that on January 15, 2016 in Milwaukee, WI he was unlawfully detained by six Milwaukee County Sheriff deputies and two bomb/drug dogs at General Mitchell International Airport after his plane arrived in Milwaukee from Dallas.

10. Dan Black's written complaint to the Milwaukee County Executive's Office, states, in part: "On Sunday, January 15, 2017, I flew from DFW to Milwaukee on American Airlines flight 1534 at 12:20 p.m. As I was boarding, I saw an older man in first class who looked like Sheriff Clarke, but I could not be sure as he was dressed in Dallas Cowboys gear and wasn't wearing his signature cowboy hat. As I passed him, I asked if he was Sheriff Clarke, and he responded in the affirmative. I shook my head as I was moving on to my seat near the back of the plane. From behind, he asked if I had a problem. I shook my head 'no' again and continued to my seat. I was surprised that he was wearing Dallas Cowboys gear, as I hadn't seen the media stories about his Dallas fandom (I have since seen them). I intentionally did not say anything more to him because I did not want to make a scene or get in trouble as a Milwaukee man did in September

when confronting Clarke on an airplane. I just moved on and took my seat. When I exited the flight at Mitchell International, there were six uniformed deputies and two bomb/drug dogs standing there with Sheriff Clarke waiting for me to exit. As soon as Sheriff Clarke gestured towards me, he and some of the officers left us. I was very publicly escorted in front of everyone down the hall to a waiting area, and then questioned by two of the Sheriff's Department deputies. They told me that Sheriff Clarke said I had made some remarks to him upon entering the plane. When I asked for clarification, the deputies said they couldn't tell me, and when I asked if they even knew the context of my 'remarks,' they responded 'no.' After questioning me for about fifteen minutes, asking me who I was, why I was in Dallas, what my views of Sheriff Clarke were and essentially treating me as a threat, they escorted me all the way out of the airport in front of everyone there. I was walked through the terminal, down through baggage claim, and all the way to my friend's car by the officers. I was not given the opportunity to use the bathroom, to stop for coffee, or to browse the bookstore. It was clear to the deputies after their interrogation that I hadn't done anything (let alone done anything wrong), so I was confused as to why I needed to leave the airport directly...."

11. The ASD investigators concluded, in part: "Clarke used his official position as Sheriff of Milwaukee County in excess of his lawful authority to direct his deputies to stop and question Black without legal justification. Under state statute, a stop is lawful if there is reasonable suspicion that the person has committed, is committing or is about to commit a crime. ASD finds Black's version of events to be credible. Per Black, he verified Clarke's identity and then shook his head at him. He shook his head again in response to Clarke asking if there was a problem. Black's actions cannot reasonably be considered criminal conduct regardless if made to a private citizen, a person of national profile such as Clarke, or a law enforcement officer, on or off-duty...."

FBI Investigation

Dan Black Interview

12. On February 24, 2017, I interviewed Dan Black. Black's explanation of the January 15, 2017 incident was largely consistent with his previous written complaint to the Milwaukee County Executive's Office.

Review of Milwaukee County Sheriff's Office Documents

13. I received records from the Milwaukee County Sheriff's Office (MCSO) relating to the January 15, 2017 Dan Black incident. One MCSO document showed a screenshot of a text message exchange between Sheriff Clarke and his employee Captain Mark Witek on January 15, 2016. The text messages incoming to Captain Witek's cellphone are from "D Clarke, 414-759-8002". I was able to verify that the cellphone number 414-759-8002 is used by Sheriff Clarke. MCSO confirmed that the content of the text messages shows a conversation between Sheriff Clarke and Captain Witek on January 15, 2016 where Sheriff Clarke directs his deputies how to interact with Dan Black when he exits the plane in Milwaukee. Inspector Edward Bailey is one of Sheriff Clarke's supervisors.

14. The text message conversation from Captain Witek's cellphone follows:

> Sheriff Clarke: Are you working?
>
> Captain Witek: Yes, I just spoke to Inspector Bailey and he informed me of what was going on.
>
> Captain Witek: We will meet you
>
> Sheriff Clarke: 10-4 Just a field interview, no arrest unless he becomes an asshole with your guys. Question for him is why he said anything to me. Why didn't he just keep his mouth shut? Follow him to baggage claim and out the door You can escort me to carousel after I point him out

Milwaukee County Sheriff Office Facebook Postings

15. The FBI also discovered that on the MCSO's publicly available Facebook page, there was a posting on January 18, 2017, at 9:56am, which included a link to Black's formal written complaint. The posting stated: "Sheriff Clarke commented on complaint sent to the media: Next time he or anyone else pulls this stunt on a plane they may get knocked out. The Sheriff said he does not have to wait for some goof to assault him. He reserves the right to pre-empt a possible assault."

16. The FBI also discovered that on the MCSO's publicly available Facebook page, there was a posting on January 19, 2017, at 2:39pm, which included a picture of Black and stated: "CHEER UP SNOWFLAKE…IF SHERIFF CLARKE WERE TO REALLY HARASS YOU, YOU WOULDN'T BE AROUND TO WHINE ABOUT IT."

17. Through the investigation, including the evaluation of emails and statements between Sheriff Clarke and his staff, I believe these Facebook messages were either posted by Sheriff Clarke or he directed his staff to post the messages for him.

Email Records: David Clarke <dclarke.cowboy@gmail.com>

18. Within the ASD reports, I viewed a photocopy of a January 17, 2017, 7:28pm email which was sent from the email address, David Clarke dclarke.cowboy@gmail.com, to a MCSO subordinate employee, F.M. The email was in reference to Dan Black's formal written complaint against the Sheriff for the January 15, 2017 incident. The email stated in part, "FB. DO NOT RESPOND TO BICE. Link to the complaint. Sheriff has taken this asshole's complaint under advisement and summarily determined that he can go to hell. The next time he or anyone else pulls this stunt they may get knocked out. Sheriff does not have to wait for some goof to assault him.

He reserves the reasonable right to pre-empt a possible assault. Send FB post directly to vicki, weber, belling."

19. On January 18, 2017, F.M. sent an email to the email address, David Clarke dclarke.cowboy@gmail.com, which F.M. stated that the first sentence of the January 17, 2017 email could not be posted to Facebook. On the same day at 2:56pm, a response to F.M.'s email was sent from the email address, David Clarke dclarke.cowboy@gmail.com which stated, in part, "Can't? Is there a computer problem?..."

20. Further email correspondence between F.M. and the email address, David Clarke dclarke.cowboy@gmail.com on January 26, 2017 suggest that Sheriff Clarke was posting or directing staff to post memes and messages to the MCSO's Facebook account.

21. The content of the above emails from the email address, David Clarke dclarke.cowboy@gmail.com were official, and the substance and email address show that the emails appear to be sent by Sheriff David Clarke, and that he used the email address, David Clarke dclarke.cowboy@gmail.com to discuss the Dan Black incident and to direct his staff to post materials regarding the Dan Black incident to Facebook.

22. No explanation was given for Sheriff Clarke's use of a "gmail.com" email address by the subordinate employee, but it is reasonable to expect that this email may have been used by Sheriff Clarke to discuss or provide direction to his deputies on January 15, 2017 regarding the detention of Dan Black. It is further reasonable to expect that Sheriff Clarke used this "gmail.com" email address to discuss the January 15, 2017 incident with his staff after the incident occurred. Therefore, the content of the email would be useful to the investigation.

23. A review of subscriber information and usage date for the email address, David Clarke dclarke.cowboy@gmail.com shows the subscriber name is "David Clarke".

24. As described above, your affiant has investigative experience, and knows that a law enforcement executive will direct subordinate personnel by several means. Posted written notices, written communications, verbal instructions and electronic communications such as emails and texts are all common methods of delivering orders and instructions to subordinates. In an emergency situation or when an immediate response is required, a law enforcement executive will commonly utilize both verbal and electronic means of communication to ensure his or her subordinates receive and respond to orders as quickly as possible. Based on my experience as a law enforcement officer, I believe that in order to ensure his deputies would respond to his location upon debarking the aircraft, and knowing from personal experience that air travel inhibits verbal communication at certain points of travel, Sheriff Clarke could have utilized a combination of verbal, text, and email instruction. Additionally, it is known that in the days after the incident, Sheriff Clarke issued statements regarding the incident via this very email address. His statements, intended to provide justification for his actions, corroborate the incident.

25. In general, an email that is sent to a Gmail subscriber is stored in the subscriber's "mail box" on Google, Inc. servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc. servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google Inc.'s servers for a certain period of time.

26. It is a federal crime for anyone acting under "color of law" to willfully deprive or conspire to deprive a person of a right protected by the Constitution or the laws of the United States. "Color of law" simply means the person is using authority given to him or her by a local, state, or federal government agency. (18 U.S.C. § 242) The FBI has authority to investigate color

of law violations, which include acts carried out by government officials operating both within and beyond the limits of their lawful authority.

27. Your affiant concluded above information articulates a factual basis that reasonably indicates the existence of federal criminal activity, the burden the FBI has in order to open an investigation.

BACKGROUND CONCERNING EMAIL

28. In my training and experience, I have learned that Google, Inc. provides a variety of on-line services, including electronic mail ("email") access, to the public. Google, Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Gmail subscribers) and information concerning subscribers and their use of Gmail 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.

29. In my training and experience, email providers generally ask their 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). 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. 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.

30. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. 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, email providers often have records of the Internet Protocol address ("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 or other devices were used to access the email account.

31. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. 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.

32. This application seeks a warrant to search all responsive records and information under the control of Google, Inc., a provider subject to the jurisdiction of this court, regardless of where Google, Inc. 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, Inc.'s possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [1]

33. As explained herein, information stored in connection with an email 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 or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email 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. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may

---

[1] It is possible that Google, Inc. 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 that is in the possession, custody, or control of Google, Inc. The government also seeks the disclosure of the physical location or locations where the information is stored. In the Eastern District of Wisconsin, in case 17-MJ-1234 and 17-MJ-1235, 2017 U.D. Dist. LEXIS 24591 (Feb. 21, 2017), U.S. Magistrate Judge William E. Duffin rejected the Second Circuit's decisions in *Microsoft* and issued warrants that required Google and Yahoo! to disclose "all data responsive to the warrant regardless of whether that data may be stored on servers in or outside the United States."

indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

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

REQUEST FOR SEALING

35. I further request that the Court order 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 that is neither public nor known to all of the

targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with dclarke.cowboy@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at Mountain View, CA.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, Inc. (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) , the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account on or after January 15, 2017, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

g. The Provider is hereby ordered to disclose the above information to the government within two days, or an otherwise justifiable period of less than 14 days, of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of Title 18, USC, Section 242 and Title 18, USC, Section 241, those violations involving Milwaukee County Sheriff David Clarke, and occurring after January 15, 2017, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Communications between Sheriff David Clarke and others regarding the detention of Dan Black from January 15, 2017 to present.

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID about matters relating to the detention of Dan Black, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Google, Inc., and my official title is _____. I am a custodian of records for Google, Inc. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Google, Inc., and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Google, Inc.; and

c. such records were made by Google, Inc. as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature