AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of Maryland

United States of America
v.

SIDHARTHA KUMAR MATHUR

Defendant(s)

Case No. 1:20-mj-3211-TMD

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of December 10, 2020 in the county of Howard in the ____ District of Maryland, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. § 115(a)(1)(B)	Threats Against a Federal Official

This criminal complaint is based on these facts:

As further described in the attached affidavit.

❒ Continued on the attached sheet.

Complainant's signature

SA Tucker Kleitsch, U.S. Capitol Police
Printed name and title

Sworn to before me and signed in my presence.

Date: _____

Judge's signature

City and state: Baltimore, Maryland

Thomas M. DiGirolamo, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND APPLICATIONS FOR SEARCH AND SEIZURE WARRANTS

I, Tucker Kleitsch, 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 the issuance of a criminal complaint and arrest warrant against Sidhartha Kumar MATHUR ("MATHUR"), charging him with a violation of 18 U.S.C. § 115(a)(1)(B)(Threats Against a Federal Official), committed on or about December 10, 2020.

2. This affidavit is also made in support of applications under Rule 41 of the Federal Rules of Criminal Procedure for the issuance of warrants to search (1) the person of Sidhartha Kumar MATHUR; and, (2) the personal residence of MATHUR, located at 12340 Fox Meadow Lane, West Friendship, MD 21794, to include the residence's curtilage (the "SUBJECT PREMISES") further described in Attachments A1 and A2 for evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 115(a)(1)(B)(Threats Against a Federal Official), 875(c) (Interstate Threats), and 1001(False Statements), (the "TARGET OFFENSES"), as listed in Attachment B1.

3. This affidavit is also submitted in support of an application for a search warrant, pursuant to the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et. seq., to search the contents of the Google account **desidster@gmail.com**, (the "SUBJECT ACCOUNT") described in Attachment A3, stored at premises owned, maintained, controlled or operated by Google LLC, a business with offices located at 1600 Amphitheatre Parkway, Mountain View, California, 94043, for evidence, fruits, and instrumentalities of violations of the TARGET OFFENSES, as listed in Attachment B2.

4. I am a Special Agent with the United States Capitol Police (the "USCP") where I have served since July 11, 1995. I am currently assigned to the USCP Investigations Division, Threat Assessment Section ("USCP TAS"). I have completed hundreds of hours of training in numerous areas of law enforcement investigation and techniques, including but not limited to the following: the Criminal Investigator Training Program and the Mixed Basic Police Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia; the Federal Protective Service, Protective Investigations Program (PIP); National Threat Assessment Center (NTAC) with the U.S. Secret Service; and the Basic Crisis Negotiation Course with the FBI/Department of Justice (DOJ). In the course of my employment as a Special Agent with the USCP, I have received training regarding the application for and execution of both search and arrest warrants. I have received training in assessing and managing individuals who have communicated threats and engaged in behaviors associated with targeted violence. In my current assignment, I have participated in and conducted numerous investigations involving illegal activity including stalking and threatening communications, both locally and interstate. As a federal law enforcement officer, I am authorized to execute search and seizure warrants under Rule 41 of the Federal Rules of Criminal Procedure.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for issuance of the Criminal Complaint and the requested warrants and does not set forth all of my knowledge about this matter.

6. Based on the facts set forth in this affidavit, I submit that there is probable cause to believe that a violation of 18 U.S.C. § 115(a)(1)(B)(Threats Against a Federal Official), has been committed by Sidhartha Kumar MATHUR. There is also probable cause to believe that evidence

and instrumentalities of the crime, as more particularly described in Attachments B1 and B2, will be found within the locations to be searched, which are described more particularly in Attachments A1, A2, and A3.

THE TARGET OFFENSES

7. Pursuant to 18 U.S.C. § 115(a)(1)(B), in relevant part, "[w]hoever . . . threatens to assault, kidnap, or murder, a [Member of Congress], with intent to impede, intimidate, or interfere with such official, while engaged in the performance of official duties, or with intent to retaliate against such official . . . on account of the performance of official duties, shall be punished [by not more than 10 years in prison]".[1]

8. Pursuant to 18 U.S.C. § 875(c), "[w]hoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years."

9. Pursuant to 18 U.S.C. § 1001(a)(2), in relevant part, "whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully—makes any materially false, fictitious, or fraudulent statement or representation . . .shall be fined under this title [and] imprisoned not more than 5 years."

---

[1] 18 U.S.C. § 115(b) reads in relevant part:
(b)(1) The punishment for an assault in violation of this section is--
(A) a fine under this title; and
(B) **(i)** if the assault consists of a simple assault, a term of imprisonment for not more than 1 year;
(ii) if the assault involved physical contact with the victim of that assault or the intent to commit another felony, a term of imprisonment for not more than 10 years;

PROBABLE CAUSE

10. On December 10, 2020, at approximately 5:45 PM EST, a male person believed to be MATHUR, using phone number 919-360-5595, left a voicemail at the Maryland district office of Representative A, a member of the United States House of Representatives. The voicemail, which was subsequently reported to USCP TAS on December 11, 2020, included the following statements: "I just want to say, I'm going fucking to kill you. If you even mess with my vote, I'm going to come and I'll slit your throat and I'll kill your family. Okay. You shut, you fucking, don't touch my vote. You represent me. I'll kill you."

11. An online database search of the number 919-360-5595 revealed that the current cellular carrier for that number is Verizon Wireless and that the associated user is MATHUR.

12. Verizon Wireless subscriber records, which were provided by Verizon Wireless following an emergency disclosure request made pursuant to 18 U.S.C. § 2702(c)(4) for the phone number 919-360-5595, showed MATHUR's father to be the accountholder, and MATHUR to be the possible account user, with a billing address of 12340 Fox Meadow Lane, West Friendship, Maryland (the SUBJECT PREMISES).

13. Location information, also provided by Verizon Wireless as a result of the emergency disclosure request, showed that on December 11, 2020, MATHUR's cell phone was in the proximity of the SUBJECT PREMISES.

14. Additionally, on December 10, 2020, at approximately 5:43 PM EST, a person accessed Representative A's website, and sent a webmail (A message through the Representative A's website, where the author provides their zip code and +4 extension which filters the author to their correct Representative, without sending an email) which returned to the U.S. Capitol office of Representative A, which is located in the District of Columbia. The author

of the message provided contact information including the name of Person A, a street address in West Friendship, Maryland, near the SUBJECT PREMISES, and the **SUBJECT ACCOUNT.**

15. The webmail, which was subsequently reported to USCP TAS on December 11, 2020, consisted of the following:

> I will fucking kill you and blow up your office if you try to take my vote away. I know where you and your family lives. You will be ended. You're a fucking animal that needs to be tortured and skinned alive.

16. Leidos Digital Solutions, a company that provides Internet Technology support to Representative A, supplied the webmail author's originating IP address 96.244.249.207, owned by Verizon Business.

17. Verizon Business subscriber records, which were provided by Verizon Business following an emergency disclosure request made pursuant to 18 U.S.C. § 2702(c)(4) for the originating IP address 96.244.249.207, showed MATHUR's father to be the account subscriber, with a billing address of 12340 Fox Meadow Lane, West Friendship, Maryland (the SUBJECT PREMISES).

18. According to information provided by Google, the account **desidster@gmail.com** was created on May 12, 2005 with the name "John Lacey" and the alternate email address smathur@unc.edu. The account recovery email is smathur@alumni.unc.edu,[2] and the recovery SMS number is +1 (919) 360-5595.

19. On 12/11/2020 at approximately 5:30 PM EST, your affiant and other law enforcement officers conducted a voluntary interview of MATHUR at the SUBJECT PREMISES.

---

[2] The internet domain "unc.edu" belongs to the University of North Carolina at Chapel Hill. According to information publically available on the internet, a "Sidhartha Kumar Mathur" graduated from the University of North Carolina at Chapel Hill in 2009 with a B.S. in Public Health.

MATHUR acknowledged that phone number 919-360-5595 belonged to him. MATHUR admitted to making the December 10, 2020, 5:45 PM EST call to Representative A's office and leaving the voicemail. MATHUR advised that his statement was made out of anger. MATHUR acknowledged that he may have taken his statements too far and indicated that his statements were conditional. MATHUR said that he does, "take the threat seriously that my vote is going to be taken away" and believes that he made the preconditions associated with his threat clear.

20. MATHUR acknowledged that he knew Person A as a neighbor and former schoolmate from years ago. MATHUR was asked if he authored the December 10, 2020, 5:43 PM EST webmail to Representative A, but denied writing it even though the IP address came back to MATHUR's residence and had similar verbiage to the aforementioned voicemail. After being warned that lying to federal agents was a felony offense, MATHUR again reaffirmed that he made the telephone threat but did not send the webmail, and suggested that his internet network may be insecure.

21. Based on my training and experience and discussions with other law enforcement officers, I know that persons committing or intending to commit threat-related offenses often utilize computers, data storage devices, and other electronic communications equipment, including cellular telephones, to search the internet, to store plans and conduct research related to attacks or threat-related activities, and to communicate and transmit threats to recipients of threat-related activities (as was done here through Representative A's website).

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

22. As described above and in Attachment B1, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, and MATHUR's person, in whatever form they are found. One form in which the records might be found is data stored on a

computer's hard drive or other storage media such as hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media. Thus, the warrants applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

23. *Probable cause.* I submit that if a computer or storage medium is found on or in the SUBJECT PREMISES, or on MATHUR's person, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

24. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES or on MATHUR's person, because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, "chat," instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

25. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

26. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrants I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrants, and would authorize a later review of the media or information consistent with the warrants. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrants.

AUTHORIZATION REQUEST

27. Based on the foregoing, I respectfully submit that there is probable cause to believe that MATHUR made threats against Representative A on December 10, 2020, in violation of 18 U.S.C. § 115 (a)(1)(B). I request that a criminal complaint, arrest warrant and search and seizure warrants be issued, as prayed.

CONCLUSION

28. Based on the information set forth above, I submit there is probable cause to believe that contraband, and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 115(a)(1)(B)(Threats Against a Federal Official), 875(c) (Interstate Threats), and 1001(False Statements), as set forth herein and in Attachments B1 and B2, are currently located in the locations and account more fully described in Attachments A1, A2, and A3. I therefore respectfully request that a search warrant be issued authorizing a search of MATHUR, the SUBJECT PREMISES, and the SUBJECT ACCOUNT, described in Attachments A1, A2, and

A3, for the items described above and in Attachments B1 and B2, and authorizing the seizure and examination of any such items found therein.

29. I anticipate executing the warrant to search the SUBJECT ACCOUNT under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Attachment A3. Upon receipt of the information described in Attachment B2, government-authorized persons will review that information to locate the items described in the Attachment.

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

31. Because the warrant will be served electronically on Google who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Tucker Kleitsch
Special Agent
U.S. Capitol Police

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4(d), 4.1 and 41(d)(3) this 21 day of December, 2020

The Honorable Thomas M. DiGirolamo
United States Magistrate Judge