

FILED ENTERED
LOGGED RECEIVED

AO 91 (Rev. 11/11) Criminal Complaint

12:30 pm, Apr 03 2023
AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

UNITED STATES DISTRICT COURT

for the
District of Maryland

United States of America
v.

ADAM MICHAEL NETTINA

Case No. 23-mj-01123-BAH

Defendant(s)

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 March 28, 2023 in the county of Howard in the
_____ District of Maryland, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 875(c)	Interstate Communications with a Threat to Injure

This criminal complaint is based on these facts:

See affidavit.

Continued on the attached sheet.

[Signature]
Complainant's signature

Keith Murray, Special Agent FBI
Printed name and title

Sworn to before me over the telephone and signed by me pursuant to Fed. R. Crim. P. 4.1 and 4(d).

Date: March 31, 2023

[Signature]
Judge's signature



City and state: Baltimore, Maryland

Hon. Brendan A. Hurson, U.S. Magistrate Judge
Printed name and title

AT BALTIMORE
CLERK, U.S. DISTRICT COURT
DISTRICT OF MARYLAND
BY _____ Deputy

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT AND CRIMINAL COMPLAINT

I, Special Agent Keith Murray, being duly sworn, depose and state that::

1. This affidavit is made in support of an application for a search and seizure warrant to search the following:

- a. the premises located at 2760 Wynfield Road, West Friendship, Maryland 21794 (the “TARGET ADDRESS”);
- b. a Ford Mustang, bearing Virginia license plate UEB7564; and
- c. The person of Adam Michael Nettina;

(collectively the “TARGET LOCATIONS”), for evidence of violations of Title 18, United State Code, Section 875(c) (Interstate Threatening Communications) (the “TARGET OFFENSE”); more fully described in Attachments A1, A2, and A3, which is incorporated by reference.

2. This affidavit is also made in support of a criminal complaint and arrest warrant for Adam Michael Nettina (“NETTINA”), born in 1988, 2760 Wynfield Road, West Friendship, Maryland 21794, for a violation of the TARGET OFFENSE.

AGENT BACKGROUND

3. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since July 2017. I am currently assigned to the Baltimore Field Office of the FBI and have worked matters involving Civil Rights violations to include Hate Crimes, Federally Protected Activities, Damage to Religious Property, and Criminal Interference with Rights to Fair Housing. I have conducted numerous Civil Rights trainings to colleges and universities and to police municipalities across the state of Maryland.

4. I have received extensive training in interview and interrogation techniques, arrest procedures, and the preparation and execution of search and seizure warrants. I have conducted

and assisted in public corruption investigations in various capacities. As a Special Agent, I have written and executed multiple search warrants and have planned and executed multiple arrest operations. I have participated in the seizure of evidentiary items, the transport of defendants, and testified in court proceedings.

5. As a federal agent, I am authorized to investigate violations of laws of the United States and am a law enforcement officer with the authority to execute warrants issued under the authority of the United States. I am an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for violation of laws of the United States, including the TARGET OFFENSE.

6. The statements contained in this affidavit are based in part on: information provided by other agencies, written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; independent investigation; and my experience, training, and background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of establishing probable cause to believe that NETTINA, committed the TARGET OFFENSE as described below, I have not included every detail of the investigation. In addition, unless otherwise indicated, all statements contained in this affidavit are summaries in substance and in part. The following is true to the best of my knowledge and belief.

PROBABLE CAUSE

7. On March 28, 2023, at approximately 11:21 p.m., the Human Rights Campaign (HRC), located at 1640 Rhode Island Ave NW, Washington DC, 20036, received a threatening voicemail from phone number 410-336-5742 (“the TARGET PHONE”). HRC is an American LBGTQ advocacy group and political lobbying organization based in Washington D.C. The

transcription of the voicemail is as follows:

You guys going to shoot up our schools now? Is that how it's going to be? You just gonna to kill little kids. You're just going to slaughter fucking little kids. Let me tell you something, we're waiting, we're waiting. And if you want a war, we'll have a war. And we'll fucking slaughter you back. We'll cut your throats. We'll put a bullet in your head. We're not going to give a fuck. You started this bullshit. You're going to kill us? We're going to kill you ten times more in full.

8. I believe this voicemail was referencing the March 27, 2023, mass shooting at The Covenant School, in Nashville, Tennessee, involving multiple fatalities by a firearm, where the perpetrator was publicly identified as being transgender.

9. An open-source search of phone number 410-336-5742 revealed the following information: The registered owner is Daniel Nettina with a physical address of 2760 Wynfield Road, West Friendship, Maryland, 21794 (the TARGET ADDRESS). The phone is associated with phone provider AT&T.

10. An open-source search of the physical address 2760 Wynfield Road, West Friendship, Maryland revealed the following potential occupants: Daniel Nettina, Sandra Nettina, and Adam Michael NETTINA.

11. A search of the Maryland Motor Vehicle Administration (“MVA”) for “Adam Michael Nettina” generated the following information:

Address: 2760 Wynfield Road, West Friendship, Maryland, 21794
Height: 5 feet, 5 inches
Race: Caucasian
Date of Birth: December 8, 1988

12. An open-source search of the TARGET PHONE revealed that on April 20, 2021, the NETTINA was involved in a vehicular accident in Herndon, Virginia. NETTINA provided the TARGET PHONE number while filing an insurance claim with his insurance provider.

13. A search of the social media platform LinkedIn for “Adam Nettina” revealed the

following profile: Adam Nettina, employed by HSP Direct, located in Ashburn, Virginia. The photo attached to the LinkedIn account matches the physical characteristics of the MVA photo for NETTINA. The profile indicates that NETTINA was employed by HSP until February 2023.

14. On March 30, 2023, Special Agents (SA) with the Federal Bureau of Investigation (FBI) interviewed an employee with HSP Direct in Herndon, Virginia. The employee informed the agents that Adam NETTINA was no longer employed at the business, consistent with NETTINA's LinkedIn profile. The employee also informed the agents that NETTINA's cell phone number was 410-336-5742 (TARGET PHONE).

15. A search of the Maryland Department of Assessments and Taxation website revealed the TARGET ADDRESS is a 3,095 square foot single-story residence located in Howard County, Maryland, and is owned by Daniel Nettina and Sandra Nettina.

16. A search of Facebook for Adam Nettina resulted in the publicly accessible account with the profile name, "Adam Nettina." The publicly accessible photos in the account matched the physical characteristics of NETTINA's MVA photo. On November 24, 2021, NETTINA posted several pictures of a rifle which he had identified in previous posts as an "AKM" produced by the Imperial Tula Arms Plant. In the November 24 post, NETTINA identified the rifle as being a "1969 build."

17. On March 7, 2023, an article attributed to "Adam Nettina" was posted on the personal blogging website Substack. In the article, NETTINA wrote that he recently moved back to his childhood home in Maryland. At the end of the article is a byline that reads, "Adam Nettina grew up in Ellicott City and has spent most of his life trying to escape Maryland. He likes to drive his Mustang into the West Texas Desert and shoot Coors light cans with his 1969 Tula AKM." I believe that in this byline, NETTINA is referencing the 1969 Tula AKM semi-automatic rifle

which he posted pictures of on November 24, 2021.

18. Due to the threatening and imminent content of the voicemail, investigators obtained an emergency, exigent precision location request for the purpose of locating the suspect using the TARGET PHONE.

19. On March 30, 2023, investigators received the results of the precision location request which showed that on March 30, 2023, the TARGET PHONE was located in the area of the TARGET ADDRESS.

20. On March 31, 2023, physical surveillance was conducted in and around the area of the TARGET ADDRESS. Investigators observed a red Ford Mustang parked in the driveway of the TARGET ADDRESS bearing Virginia license plate UEB7564.

21. A search of the Virginia Department of Motor Vehicles revealed UEB7564 is registered to Adam NETTINA, with physical address 13564 Davinci Lane, Herndon, VA 20171.

**SUMMARY REGARDING USE OF MOBILE PHONES AND THE STORAGE OF
EVIDENCE IN CONNECTION WITH CRIMINAL ACTIVITY**

22. Based on the training, knowledge, experience, and participation gained in other investigations, I know the following characteristics of participants involved in criminal schemes:

a. Participants will keep evidence of these crimes and the planning and execution of the crimes in their residence, on their person, and/or in their vehicles. This evidence is often obtained and maintained through the use of digital devices and the internet.

b. This evidence could include notes, records, and receipts that document locations, approach and escape routes, or other intelligence about the victim as well as documents that reveal financial transactions between co-conspirators and/or purchases of equipment related to crimes.

c. This evidence could include computers and other devices on which a person can gather information about possible targets, as well as surveillance equipment such as tracking devices, binoculars, and other implements used to gather intelligence and prepare for the commission of a crime.

d. I know that home and vehicle surveillance systems will sometimes capture the planning of crimes by conspirators as well as evidence from the crimes including dates and times the subject entered or left the residence, locations of the vehicles, and or the destruction or hiding of evidence.

e. I know that due to the use of computers, cell phones, and digital devices by individuals and groups committing and planning criminal acts, that search histories, documents, images, and other data including historical cell site location data, and mapping data is created. I also know that certain accounts will have data connected to online applications that are downloaded by the user. I know that this data can provide evidence about the individual using the computer, cell phones, and digital devices, other co-conspirators involved in the crime, and evidence regarding the planning and execution of the crime.

f. I know that stored email content can help identify the user of the account as well as associates and possible co-conspirators. Furthermore, I know that subscriptions to certain online databases and/or mobile applications require an email account and that stored email content can verify the user of these accounts and applications.

g. I know that mobile devices have the capability to record the times, dates, and lengths of incoming and outgoing calls and messages; record the location from which calls were placed, and to access the Internet through internet web browsers and various applications. As a result, significant business activity, including activity in furtherance of criminal schemes, can be conducted using a mobile device, including smartphones. Here, such activity could include using internet searches to gather intelligence on the intended victim(s), otherwise planning the crimes, and mapping routes. Mobile devices can store information, such as documents, videos, images, and the previously mentioned computer activity, as well as the use of applications, internet browser history, and search history.

h. Subjects who plan and commit crimes in the manner described in the affidavit often harbor intense biases towards other individuals and groups. Such persons often look for likeminded people and communicate with them regularly through mobile phones, email, and other internet and phone based applications. Such individuals also often visit and read websites, chat rooms and other internet platforms where like-minded people share their views. Additionally, such individuals often share their views in private, via text message, email, other computer and phone based applications, including on the Dark Web, with other like-minded individuals. Such individuals also frequently have tattoos or other markings indicating their views, and they collect books, papers, and paraphernalia reflecting their biases.

i. I know that most people use their computers, phones, and other internet capable devices to obtain news.

j. I know that mobile phones are utilized for purposes other than making phone calls, including sending and receiving SMS or "text" messages, taking, sending, and receiving photographs and video, as well as sending or receiving emails. Individuals involved with illegal activities tend to take photographic images of the property, locations, or items in connection with the crimes committed to share that information with others, or to store it on

electronic devices. I also know that this information is often stored in the memory of cellular phones for a period of time.

k. Mobile devices such as laptop computers, smartphones, iPods, iPads and digital media storage devices are known to be used and stored in vehicles, on persons or other areas outside of a business or residence. Many people generally carry their smartphone on their person.

l. I know that information and related evidence stored on digital devices can be recovered through forensic analysis up to an indefinite time after it has been created or stored on the device, even if the user believes that they have deleted the information and related evidence. Thus, there is probable cause to believe that electronic information related to the TARGET OFFENSES will still be found on any seized digital devices, notwithstanding the passage of time.

m. I know that subjects routinely keep their cell phones on their person. I also know that the cell phone itself could have data stored on it that is not captured in online accounts or cell phone/cell tower records. This data is stored locally and could contain evidence of past crimes or future crimes.

n. I know that subjects routinely save data from their cell phones, tablets, and other mobile devices “backing up” their cell phones to their computers. Subjects also routinely save data from their cell phones, tablets, and other mobile devices to cloud-based services, such as iCloud. I know that subjects can then access the data from the cloud-based services and save that data their computers.

o. I know that people involved in violent crimes and violent crime conspiracies will often change their cellphones or telephone numbers following the arrest of a co-conspirator or at random to frustrate law enforcement efforts. I am also aware that individuals involved in criminal conspiracies frequently involve friends, family, and significant others, both knowing and unknowing, in furthering their crimes. The involvement of friends, family, and significant others is also coordinated through the use of cellphones.

UNLOCKING BIOMETRICALLY SECURED DEVICES

23. Unlocking the device(s) with biometric features. The warrant I am applying for would permit law enforcement to compel Adam Nettina, the subject identified herein, to unlock any device on their person or on the TARGET PREMISES believed to be owned, used, or accessed by Adam Nettina. I seek this authority based on the following:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These

biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes and records data based on the user’s facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

d. If a device is equipped with an iris recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called “Windows Hello.” During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user’s face and activates an infrared-sensitive camera to record data based on patterns within the user’s irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device’s contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

f. As discussed in this affidavit, based on my training and experience I believe that one or more digital devices will be found during the search. The passcode or password that would unlock the device(s) subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the device(s), making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that

biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device (such as an iPhone) has been restarted, inactive, or has not been unlocked for a certain period of time. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

h. Due to the foregoing, if law enforcement personnel encounter a device belonging to or utilized by any of the subjects identified here which may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of any of the subjects identified herein, to the fingerprint scanner of the seized device; (2) hold the device in front of the face of any of the subjects identified herein, to activate the facial recognition feature; and/or (3) hold the device in front of the face of any of the subjects identified herein, and activate the iris recognition feature, for the purpose of attempting to unlock the device, and attempting to access data contained in the device, in order to search the contents as authorized by this warrant.

**SUMMARY REGARDING USE OF MOBILE PHONES AND ONLINE
ACCOUNTS/APPLICATIONS IN CONNECTION WITH CRIMINAL ACTIVITY**

24. Through training and experience, I have become familiar with the manner in which suspects use electronic communication devices to facilitate their illegal activities and thwart law enforcement investigations. I am familiar with the methods of operation employed by suspects, such as those under investigation here.

25. Based on this familiarity, I know that cellphones are an indispensable tool of those involved in violent crimes and violent crime conspiracies, including interstate threatening communications. People involved in violent crime conspiracies use cellphones, Short Message Service (“SMS”), Multimedia Messaging Service (“MMS”), electronic mail (“e-mail”), cellular applications and similar electronic means and/or devices, often under fictitious names or names other than their own, to commit their crimes and sometimes to communicate with other conspirators. In addition, participants in violent crimes will often change their cellphones or telephone numbers following the arrest of a co-conspirator or at random to frustrate law enforcement efforts. I am also aware that individuals involved in criminal conspiracies frequently involve friends, family, and significant others, both knowing and unknowing, in furthering their

crimes. The involvement of friends, family, and significant others is also coordinated through the use of cellphones.

26. Based upon my knowledge, training, experience and participation in other violent crime investigations, I also know that:

a. The fruits and instrumentalities of criminal activity are often concealed in digital form. Furthermore, digital camera technology is often used to capture images of the tools and instrumentalities of pending criminal activity. Many cell phones, as well as electronic tablets such as iPads, have both digital storage capacity and digital camera capabilities.

b. Individuals committing the TARGET OFFENSE frequently use telephones and other digital storage devices to maintain telephone number “contact lists” of individuals or businesses who may have assisted, wittingly or unwittingly, in the planning and execution of the criminal activity, and these devices often retain and store GPS data reflecting the physical locations of the phones if they were turned on and operational.

c. Individuals committing the TARGET OFFENSE frequently use cellular telephones to commit the target offense and/or to make voice calls and to exchange text messages with other coconspirators regarding their criminal offenses. Cellular telephones frequently store those records of crime-related voice and text message communications.

d. Individuals committing the TARGET OFFENSE frequently scout out locations, and frequently use mobile devices to conduct Internet research on their victims and to map routes to and from the victims’ locations.

e. Individuals planning the TARGET OFFENSE often use photography to document planned targets, victims’ locations, and areas of egress to be used after the commission of the crime.

f. Individuals who possess or own firearms or other weapons frequently photograph themselves holding the firearms or other weapons.

g. Individuals involved with illegal activities tend to use their electronic devices to call or text friends or accomplices after a crime has been committed. Sometimes coconspirators will be nearby as a look out for local police or security while an individual commits a crime. Individuals may contact an accomplice via an electronic device for a ride to flee the crime. Additionally, an individual may communicate with another person to strategize and attempt to hide evidence of the crime committed.

h. Individuals involved with illegal activities tend to search the internet for, and or take, photographic images of the property, locations, or items in connection with the crimes committed to share that information with others, or to store it on electronic devices.

27. Based on my training, knowledge, and experience, I also know that the location of a cellular phone at a particular time (based on data stored in the mobile device) may constitute evidence of a crime. Such location information allows investigators to determine, for example, whether a particular telephone was in the vicinity of a victim's location at a particular time, or in a certain location at the time of the offense. Based on my training, knowledge, and experience, I further know that nearly everyone has a mobile phone, which they carry with them virtually everywhere they go.

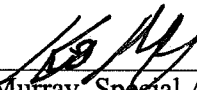
28. Further, based on my knowledge, training, and experience, I know that evidence of violent crimes often can be located on an individual's digital devices (e.g., phone, tablet, and computer) through the use of forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

CONCLUSION

29. Based on a review of this case, and based on my training and experience, I believe that NETTINA is the user of the TARGET PHONE, and further, that NETTINA placed the threatening phone call to HRC on March 28, 2023. Further, based upon all of the information set forth in this application, I respectfully submit that there is probable cause to believe that Adam Michael NETTINO violated Title 18, United States Code, Section 875(c)2251(a) (Interstate Threatening Communications).

30. Based on the foregoing information, I have probable cause to believe that contraband, and evidence, fruits, and instrumentalities of the TARGET OFFENSE as set forth herein and in Attachment B are currently contained in the TARGET LOCATIONS more fully described in Attachments A1, A2 and A3. I therefore respectfully request that a search warrant be

issued authorizing a search of the TARGET LOCATIONS for the items described above and in Attachment B, and authorizing the seizure and examination of any such items found therein.



Keith Murray, Special Agent
Federal Bureau of Investigation

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3) this 31st day of March, 2023.



HONORABLE BRENDAN HURSON
UNITED STATES MAGISTRATE JUDGE



ATTACHMENT A1

DESCRIPTION OF RESIDENTIAL PREMISES TO BE SEARCHED

The premises to be searched is located at 2760 Wynfield Road, West Friendship, Maryland 21794 (hereinafter the “TARGET RESIDENCE”) and all outbuildings on the property. It is a tan colored, brick residence, with a black colored roof. There is a white awning over a red front door to the residence. There is a white garage door on the North West corner of the residence. The TARGET RESIDENCE includes any Electronic Media contained therein.



ATTACHMENT A2

DESCRIPTION OF PREMISES TO BE SEARCHED

The premises to be searched is a red 2020 Ford Mustang, bearing Virginia license plate UEB7564, registered to Adam Nettina.



ATTACHMENT A3

DESCRIPTION OF PERSON TO BE SEARCHED

ADAM MICHAEL NETTINA (“NETTINA”) who is a white male, with the following date of birth (12/08/1988). A photo of NETTINA is shown below.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED AND SEARCHED

2760 Wynfield Road, West Friendship, Maryland 21794;
2020 Ford Mustang, bearing Virginia license plate UEB7564; and
ADAM MICHAEL NETTINA,

as well as any locked or closed containers or electronic devices therein, for the following fruits, evidence and instrumentalities of violations of 18 U.S.C. 875 (c) (Interstate Threatening Communications) (TARGET OFFENSE) including:

1. Computer(s), computer hardware, software, related documentation, passwords, data security devices (as described below), videotapes, and or video recording devices, and data that may constitute instrumentalities of, or contain evidence related to, this crime. The following definitions apply to the terms as set out in this affidavit and attachment:

a. Computer hardware: Computer hardware consists of all equipment, which can receive, capture, collect analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Hardware includes any data processing devices (including but not limited to cellular telephones, central processing units, laptops, tablets, eReaders, notes, iPads, and iPods; internal and peripheral storage devices such as external hard drives, thumb drives, SD cards, flash drives, USB storage devices, CDs and DVDs, and other memory storage devices); peripheral input/output devices (including but not limited to keyboards, printer, video display monitors, and related communications devices such as cables and connections), as well as any devices mechanisms, or parts that can be used to restrict access to computer hardware (including but not limited to physical keys and locks).

b. Computer software is digital information, which can be interpreted by a computer and any of its related components to direct the way they work. Software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

c. Documentation: Computer related documentation consists of written, recorded, printed, or electronically stored material, which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Passwords and Data Security Devices: Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation or data. Data security devices may consist of hardware, software or other programming code. A password (a string of alpha numeric characters) usually operates a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software of digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre set security functions when touches. Data security software or code may also encrypt, compress, hide, or "booby trap" protected data

to make it inaccessible or unusable, as well as reverse the progress to restore it.

2. Any and all notes, documents, records, or correspondence pertaining to interstate threatening communications as defined under Title 18, U.S.C. § 875(c).
3. Any and all firearms and ammunition.
4. Any and all communications related to the TARGET OFFENSE, including records of incoming and outgoing voice communications; records of incoming and outgoing text messages; records of incoming and outgoing emails; the content of incoming and outgoing text messages and emails; voicemails; voice recordings; contact lists; notes; and associated geographic location data;
5. Any and all browsing history, including internet searches, search terms, and search results, and associated geographic location, related to the TARGET OFFENSES;
6. Any and all records, documents, invoices and materials that concern any accounts with Facebook, Instagram, AT&T, or any other Internet Service Provider, screen names, online accounts, or email accounts.
7. Any and all web cameras, cameras, film, cell phones with cameras and/or internet capability, or other photographic equipment.
8. Any and all documents, records, or correspondence pertaining to occupancy, ownership or other connection to **2760 Wynfield Road, West Friendship, Maryland 21794**.
9. Any and all diaries, notebooks, notes, address books, pictures, emails, chats, directions, maps, banking, travel, documents, and any other records reflecting contact or threats made to the Human Rights Campaign (HRC) or any other LGBTQ advocacy group.
10. As used above, the terms "records, documents, messages, correspondence, data, and materials" includes records, documents, messages, correspondence, data, and materials, created, modified or stored in any form, including electronic or digital form, and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices.
11. For any computer, computer hard drive, or other physical object upon which computer data can be recorded (hereinafter, "COMPUTER") that is called for by this warrant, or that might contain things otherwise called for by this warrant:
 - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

- b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER; documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- h. contextual information necessary to understand the evidence described in this attachment; AND

12. With respect to the search of any of the items described in paragraphs 1 through 10 above which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment (including CDs, DVDs, thumb drives, flash drives, hard disk drives, or removable digital storage media, software or memory in any form), the search procedure may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, to minimize the review of information not within the list of items to be seized as set forth herein, while permitting government examination of all the data necessary to determine whether that data falls within the items to be seized):

- a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);
- b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
- c. "scanning" storage areas to discover and possible recover recently deleted files;
- d. "scanning" storage areas for deliberately hidden files; or
- e. performing key word searches or other search and retrieval searches through

all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

13. If after performing these procedures, the directories, files or storage areas do not reveal evidence of interstate threatening communications or other criminal activity, the further search of that particular directory, file or storage area, shall cease.

14. **DEVICE UNLOCK:** During the execution of the search of the property and person described in Attachments A1, A2 and A3, and with respect to (1) any device reasonably believed to be owned or accessed by Adam Michael Nettina, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Adam Michael Nettina to the fingerprint scanner of the seized device(s); (2) hold the seized device(s) in front of the face of Adam Michael Nettina and activate the facial recognition feature; and/or (3) hold the seized device(s) in front of the face of Adam Michael Nettina and activate the iris recognition feature, for the purpose of attempting to unlock the device(s), and attempting to access data contained in the device, in order to search the contents as authorized by this warrant.