

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Ronald Farnsworth, being duly sworn, do hereby state the following.

I. INTRODUCTION

1. I am a Special Agent with Federal Bureau of Investigation (FBI) assigned to the Washington Field Office. I have been a Special Agent of the FBI since 2003. I have been involved in the investigation of numerous types of offenses against the United States, including domestic terrorism investigations, international terrorism investigations, and violent crime investigations.
2. In the course of conducting and participating in criminal investigations, I have been involved in interviewing and debriefing informants; conducting physical surveillance; and preparing and executing search and arrest warrants. My knowledge of the facts and circumstances contained within this affidavit is based on my personal interaction with those possessing on-scene knowledge and their review of the crime scene and camera surveillance, as well as reports made to me by other law enforcement agencies, such as the Washington D.C. Metropolitan Police Department, United States Park Police, the Federal Bureau of Investigation Washington Field Office, and other government agencies. This affidavit does not set forth every fact discerned throughout the investigation; rather, it contains a summary of the investigation to date and sets forth only those facts that I believe necessary to establish probable cause to search the property described herein.
3. This affidavit supports an application for a warrant of electronic and video stored media

including one Promedia 2000 Desktop model KG2500, one HP Pavillion Elite M9350 and PC serial number [REDACTED], one Buy Power Desktop model NZX7 serial number [REDACTED] and one Dell Dimension 2400, [REDACTED], thumb drives, compact discs, floppy disks, memory cards, and video and audio cassettes. These items will collectively be referred to as Von Brunn's "COMPUTERS." Von Brunn's computers were recovered from the residence of James Wencker Von Brunn, located at [REDACTED], Annapolis, Maryland 21401. There exists probable cause to believe that a search of these computers will produce evidence and instrumentalities of criminal offenses against the United States, to wit 18 U.S.C. § 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Minors). The facts and circumstances are as follows:

II. PROBABLE CAUSE

4. On or about Wednesday, June 10, 2009, at approximately 12:44 p.m., a white male, later identified to be James Wencker Von Brunn, drove up to the front of the United States Holocaust Memorial Museum, located at 100 Raoul Wallenberg Place, S.W., Washington, D.C. 20024. The U.S. Holocaust Memorial Museum is located on federal property pursuant to 36 U.S.C. § 2301 which states, "The United States Holocaust Memorial Museum is an independent establishment of the United States Government." Thus, federal government jurisdiction is established pursuant to 18 U.S.C. § 7 (Special maritime and territorial jurisdiction of the United States). The defendant was driving a 2002 red Hyundai bearing Maryland license plate number [REDACTED]. The defendant double parked his vehicle facing southbound in the traffic lane. He stepped out of the driver's side of the vehicle and approached the entrance to the museum. The defendant was carrying a rifle at his side as he approached the building.

5. As the defendant approached the entrance to the museum, Special Police Officer ("SPO")

Steven Tyrone Johns, who was employed as a security guard for the museum, opened the door for the defendant. The defendant raised his rifle, aimed it at SPO Johns and fired one time, striking SPO Johns in the left, upper chest area. The defendant continued through the door and raised his firearm as if to fire again, at which time two other Special Police Officers on duty immediately returned fire at the defendant. The defendant was shot in the face and fell backwards outside the door.

6. All of these events were captured on videotape. The videotape was viewed by members of the Federal Bureau of Investigation and the Washington D.C. Metropolitan Police Department.

7. When officers responded to the scene, they found the defendant suffering from a gunshot wound to the face. A .22 caliber rifle was recovered next to the defendant. U.S. Park Police officers also retrieved a wallet from the defendant's pants pocket. The wallet contained a license bearing the name James Wenneker Von Brunn with a date of birth of [REDACTED]. The wallet also contained multiple other items (insurance cards, bank card, social security card, other identification cards) in the name of James Von Brunn.

8. Stephen Tyrone Johns was transported by DC EMS 4 to George Washington Hospital, suffering from a gunshot wound to the upper chest. All life-saving efforts failed and Steven Tyrone Johns was pronounced dead by Dr. Najan at approximately 3:08 pm on June 10, 2009.

9. An SPO, hereinafter identified as W-1, was interviewed and indicated the following: W-1 was working as an armed SPO at the Holocaust Museum on June 10, 2009. As W-1 was working at the 14th Street entrance to the Museum he heard two to three shots fired. He looked to his right and saw the barrel of a rifle pointing into the entrance door. W-1 returned fire as did a second SPO. The gunman then fell to the ground just outside the door. W-1 secured the gunman's rifle and awaited the arrival of the police and emergency medical personnel. W-1

indicated that the gunman's firearm appeared to be a .22 caliber rifle.

10. MPD evidence technicians recovered several items of evidence from the scene, including eight .38 caliber cartridge casings, three .22 caliber cartridge casings, and a .22 caliber rifle loaded with ten live rounds of ammunition.

11. Officers responding to the scene secured the 2002 Red Hyundai. Further investigation revealed that the vehicle, a 2002 red Hyundai bearing Maryland license plate number [REDACTED] and vehicle identification number [REDACTED] is registered to James Wenneker Von Brunn, date of birth of [REDACTED]

12. Bomb dogs were brought to the scene and indicated a positive hit for the possibility of explosives. Officers did a cursory search of the vehicle for explosives, but did not find any indication of an explosive device. Officers did, however, recover a notebook that had handwritten notations stating the following: "You want my weapons – this is how you'll get them. The Holocaust is a lie. Obama was created by Jews. Obama does what his Jew owners tell him to do. Jews captured America's money. Jews control the mass media. The 1st Amendment is abrogated – henceforth. See: holywesternempire.org. JVB swore (LT USNR) to defend the Constitution against all enemies, foreign and domestic. Jews – Bolsheviks – Zionist are America's enemies. See: Talmud – Sanhedrin "Kill the Best Gentiles!" At the end of the above writings appears the signature: "James W. Von Brunn."

13. On June 11, 2009, a search warrant was executed on the vehicle. Evidence technicians recovered .22 caliber ammunition.

14. Further investigation revealed that James Wenneker Von Brunn used the address [REDACTED], Annapolis, Maryland 21401. FBI agents responded to that address.

15. W-2 was located in the apartment. W-2 consented to an interview with FBI agents. W-2 stated that James Wenneker Von Brunn moved to the apartment approximately two years ago and it is his only known address. The apartment is leased to W-2 and W-3, a relative of the defendant. James Wenneker Von Brunn has his own room and pays rent in the amount of \$400.00 per month. W-2 also stated that when James moved to the apartment approximately two years ago he came with two weapons, a 30/30 rifle and a .22 caliber rifle.

16. Further investigation of James Wenneker Von Brunn, date of birth of [REDACTED] revealed that Von Brunn is a known white supremacist who has espoused hate speech directed specifically towards Jews for an extensive period of time. Specifically, Von Brunn claimed to have written a short novel entitled "Kill the Best Gentiles", which can be found on the website he created www.holywesternempire.com. The novel detailed how Von Brunn believed the government was being run by Jews and the Jews were looking to extinguish the white race.

17. Members of the Metropolitan Police Department ("MPD") traveled to George Washington University Hospital and obtained the defendant's fingerprints. MPD fingerprint examiners compared these fingerprints to the known prints of James Wenneker Von Brunn. The prints were a match, thus confirming the identification of the defendant. Additionally, officers visually confirmed that the individual being treated at the hospital for a gunshot wound to the face is the same individual whose photograph appears on the above-described Maryland driver's license carrying the name James Wenneker Von Brunn.

18. Agents with the Federal Bureau of Investigation applied for a search warrant for [REDACTED], Annapolis, Maryland 21401. On June 11, 2009, a search warrant was executed. The following evidence was recovered: a 30/30 rifle, Promedia 2000 Desktop model KG2500, one HP Pavillion Elite M9350 and PC serial number [REDACTED]

one Buy Power Desktop, model NZX7, serial number [REDACTED], and one Dell Dimension 2400, [REDACTED], thumb drives, compact discs, floppy disks, memory cards, and video and audio cassettes; photographic evidence to include Fuji film 7000 camera serial number [REDACTED] and memory cards; communication equipment to include Palm Pilot serial number [REDACTED], Samsung (Verizon) cellular telephone model SCH-A930, serial number [REDACTED], and Samsung (Verizon) cellular telephone model SCH-A930, serial number [REDACTED] and other evidence. The evidence is currently in the custody of the FBI-WFO.

19. During the subsequent search of these items, child pornography was discovered on Promedia 2000 Desktop model KG2500.

20. Based on the foregoing facts, it is believed that the defendant possesses child pornography in violation of Title 18 United States Code Section 2252. Therefore, the application for this warrant is within this Court's warrant authority pursuant to Rule 41(b)(5)(A).

21. Based on the facts and circumstances described above, there is probable cause to believe that if the defendant's computers are searched and examined there will be evidence of possession of child pornography.

**III. METHODS TO BE USED TO SEIZE AND SEARCH COMPUTERS
AND COMPUTER-RELATED EQUIPMENT**

22. Based upon my training, experience, and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that searching computerized information for evidence or instrumentalities of a crime commonly requires agents to seize most or all of a computer system's input/output peripheral devices, related software documentation,

and data security devices (including passwords) so that a qualified computer expert can accurately retrieve the system's data in a laboratory or other controlled environment. This is true for the following reasons:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law-enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing up to 40 gigabytes of data are now commonplace in desktop computers. Consequently, each non-

networked, desktop computer found during a search can easily contain the equivalent of millions of pages of data.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

23. In searching for data capable of being read, stored or interpreted by a computer, law-enforcement personnel executing this search warrant will employ the following procedure:

a. The computer equipment and storage devices will be seized and transported to an appropriate law-enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

b. The analysis of electronically stored data may entail any or all of several different techniques. Such techniques may include, but shall not be limited to, “mirroring” or copying the hard drive or any other magnetic or digital storage device such as floppy disks or CD-ROMs;

surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files); “opening” or reading the first few “pages” of such files in order to determine their precise contents; “scanning” storage areas to discover and possibly recover recently deleted data; scanning storage areas for deliberately hidden files; and performing electronic “key-word” searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

24. Any data that is encrypted and unreadable will not be returned unless law-enforcement personnel have determined that the data is not (1) an instrumentality of the offense, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offense specified above.

25. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover “deleted,” “hidden” or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

26. If the computer personnel determine that the computer equipment and storage devices are no longer necessary to retrieve and preserve the data, and the items are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b), such materials and/or equipment will be returned within a reasonable time.

27. In order to search for data that is capable of being read or interpreted by a computer, law-enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

a. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software;

b. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

c. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

d. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

28. For any computer hard drive or other electronic media (hereinafter, "MEDIA") that is called for by this warrant, or that might contain things otherwise called for by this warrant, this affidavit seeks authorization to search for:

a. evidence of user attribution showing who used or owned the MEDIA at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved usernames and passwords, documents, and browsing history;

b. passwords, encryption keys, and other access devices that may be necessary to access the MEDIA;

c. documentation and manuals that may be necessary to access the MEDIA or to conduct a forensic examination of the MEDIA.

29. Additionally, this warrant seeks authority to search for records and things evidencing the use of the Internet, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies)

30. It may be necessary for programmers and other outside experts to assist the FBI during the examination of the property.

31. As stated herein, this affidavit seeks authorization to search for all records relating to violation of 18 U.S.C. § 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Minors), including any information related to defendant's possession, production, reproduction, distribution, or sale of such material.

IV. CONCLUSION

32. Based on the information contained in this affidavit and any attachments herein, probable cause exists to believe that Von Brunn's computers contain evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 2252 (Certain Activities Relating to Material Involving the Sexual Exploitation of Minors). Therefore, I respectfully request the issuance of a search warrant for Von Brunn's computers described herein.

Ronald Farnsworth

Special Agent, FBI

Sworn to and subscribed to

before me this _____ day

of June, 2009

United States Magistrate Judge