



UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case Number:

**20M148**

the HP desktop computer, bearing serial number  
2UA8480JG51506, further described in  
Attachment A

**APPLICATION AND AFFIDAVIT FOR A SEARCH WARRANT**

I, Matt Loux, a Special Agent of the Department of Justice Office of the Inspector General, request a search  
warrant and state under penalty of perjury that I have reason to believe that on the following property or premises:

**See Attachment A**

located in the Northern District of Illinois, there is now concealed:

**See Attachment B**

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

The search is related to a violation of:

*Code Section*

*Offense Description*

Title 18, United States Code, Section 1030(a)(2)(B)

Unauthorized access of a computer, thereby obtaining  
information from the Federal Bureau of Prisons

The application is based on these facts:

**See Attached Affidavit,**

Continued on the attached sheet.

**FILED**

**FEB 27 2020**

**M. DAVID WEISMAN  
MAGISTRATE JUDGE  
UNITED STATES DISTRICT COURT**

Sworn to before me and signed in my presence.

*Applicant's Signature*

MATT LOUX, Special Agent  
Department of Justice Office of the Inspector General

*Printed name and title*

*Judge's signature*

Date: February 27, 2020

City and State: Chicago, Illinois

DAVID M. WEISMAN, U.S. Magistrate Judge

*Printed name and title*



4. The statements in this affidavit are based on my personal knowledge, and on information I have received from other law enforcement personnel and from persons with knowledge regarding relevant facts. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are sufficient to establish probable cause to believe that evidence and instrumentalities of violations of Title 18, United States Code, Section 1030(a)(2)(B), are located within the **Subject Computer**.

**I. FACTS SUPPORTING PROBABLE CAUSE TO SEARCH THE SUBJECT COMPUTER**

**Summary and Background Information**

5. As described in more detail below, OIG received information from the Federal Bureau of Prisons (“BOP”) that a BOP employee, Officer A, was suspected of accessing sensitive law enforcement information maintained on BOP’s electronic systems and providing that sensitive information to an individual who then released the information on social media platforms.

6. According to a BOP Special Investigative Agent, BOP’s TruView system is an application that contains information on inmates, including inmate emails, inmate telephone calls, inmate visitation lists, and inmate funds.

7. The TruView system contains information from various other applications and systems existing on BOP’s network infrastructure. The information available on Truview includes information from BOP application TRUFONE, the

inmate telephone system, which houses recordings of inmate telephone calls. TruView also contains records containing inmate visitation logs, inmate emails, and inmate funds.

8. According to BOP Office of Internal Affairs, the TruView system logs the activity of BOP employees. These logs indicate the date and time that a BOP employee accessed the TruView system, as well as the particular inmate whose files were accessed on TruView by BOP employee. These logs do not contain, however, any further specificity regarding which particular records from within the inmate's files were accessed by BOP employee.

9. According to Officer A's personnel file provided by BOP, Officer A is a former Federal BOP Disciplinary Hearing Officer. Officer A was assigned to the Thomson Correctional Center from May 14, 2019, through December 31, 2019. Officer A retired on December 31, 2019.

10. On November 22, 2019, Warden Russell A. Heisner of BOP Metropolitan Correctional Center ("MCC") in Chicago, Illinois, reported an allegation of staff misconduct to BOP Office of Internal Affairs. According to BOP Office of Internal Affairs, earlier in the month, MCC staff had become aware that a YouTube blogger known as "TashaK" and using the username "unWinewithTashaK" had revealed sensitive law enforcement information regarding Inmate A, who was being housed at the MCC. Inmate A is a nationally recognized celebrity whose criminal case has received media attention.

11. According to the BOP Office of Internal Affairs, and based on a review of a YouTube video posted by blogger TashaK about Inmate A, the content revealed by TashaK was contained in calls made by Inmate A that were recorded and maintained by BOP on the TruView system. In other words, TashaK revealed information that would have been known to BOP employees who had monitored Inmate A's telephone calls or accessed the recordings of those calls. According to the referral of incident report prepared by BOP, the BOP staff that had the authorization to monitor or review these calls were MCC Chicago staff and staff with "Special Investigative Systems" rights.

12. BOP provided OIG with logs that indicate which employee accessed records from its TruView system and when these actions occurred. These logs demonstrate which inmate's records a BOP employee accessed using the TruView system, but do not provide further specificity, such as which particular records within the inmate's file were accessed.

13. Based on my review of the access logs, for the period from July 15, 2019 through January 8, 2020, 60 BOP employees accessed Inmate A's TruView records, including Officer A.

14. Based on my review of the access logs, Officer A had accessed Inmate A's TruView records 153 times between July 15, 2019 and December 12, 2019. Because Officer A was not assigned to the MCC, Officer A was not authorized, and had no official reason, to access the records of Inmate A during that period.

15. On January 15, 2020, BOP provided OIG with the **Subject Computer**, which was used by Officer A during Officer A's employment at BOP during the period of December 1, 2019 through December 31, 2019. Since January 15, 2020, the **Subject Computer** has been in OIG's custody.

#### **TashaK's Internet Postings and Officer A's Access of Inmate A's Records**

16. Law enforcement officials conducted open-source research to obtain further information about the blogger "TashaK" and any online accounts associated with that username or the username "unWinewithTashaK." Law enforcement officials determined that "TashaK" reports on entertainment news and celebrity gossip on multiple social media accounts using the username "unWinewithTashaK," including a YouTube account and an Instagram account.

17. I reviewed the YouTube videos and Instagram posts posted by blogger TashaK that pertain to Inmate A.

#### TashaK's January 12, 2020 Instagram Post

18. On January 12, 2020, TashaK posted a photograph on Instagram that depicted Inmate A's BOP visitation list. The photograph appears to be a printout of Inmate A's visitation list that was obtained from BOP's TruView system. The printout header indicates that the visitation record is "Sensitive But Unclassified" information. The upper left corner of the photograph of the printout contains the date and time: December 5, 2019, 8:07 a.m. According to BOP information technology personnel, this information indicates the date and time that the record was accessed on the TruView system.

19. The TruView access logs show that Officer A accessed Inmate A's records on December 5, 2019 at 8:07 a.m., the same time that the printout of Inmate A's visitation log was accessed. Officer A was the only BOP employee to access Inmate A's TruView records on December 5, 2019 at 8:07 a.m. (other BOP employees accessed Inmate A's TruView records at other times that day).

TashaK's November 7, 2019 and November 8, 2019 YouTube Videos

20. On November 7, 2019, blogger TashaK posted a video on YouTube titled, "[Inmate A] Can't CONTROL his Girlfriends while BEHIND BARS." The video is publically available at <https://www.youtube.com/watch?v=JxvLlePM8Jk>. At the 26:25 minute mark of the video, TashaK shares information about Inmate A and two individuals with whom Inmate A has a romantic relationship. At approximately the 26:54 minute mark of the video, TashaK states that the information came from "a phone tap somewhere." TashaK then divulges information from phone calls involving Inmate A, including the specific content of the communications.

21. I also reviewed a YouTube video posted by blogger TashaK on November 8, 2019 titled "New [Inmate A] ENABLERS REVEALED." The video is publically available at <https://www.youtube.com/watch?v=LhcLNfkGLrc>. Beginning at approximately the 1:00:30 minute mark of the video, TashaK begins scrolling through her mobile phone, and at points in the video, appears to be reading a summary of a call involving Inmate A. TashaK then divulges information Inmate A's phone calls, including the specific content of the communications. Beginning at approximately the

1:01:34 minute mark, TashaK states that she has the “plug” and this information is “all facts.”

22. I have reviewed Inmate A’s jail calls from November 7, 2019, which were recorded and maintained on the TruView system. Based on my review of the recordings of Inmate A’s calls, some of the information that TashaK reveals regarding Inmate A is contained in the recordings of Inmate A’s jail calls from November 7, 2019.

23. The TruView access logs show that Officer A accessed Inmate A’s TruView records twice on November 7, 2019, the day that Inmate A made the phone calls that were discussed by TashaK during her November 7, 2019 and November 8, 2019 YouTube postings. Four other BOP employees accessed Inmate A’s TruView records on November 7, 2019.

#### December 22, 2019 YouTube Video

24. I reviewed a YouTube video posted by blogger TashaK on December 22, 2019 titled, “[Inmate A’s] RELEASED Emails PROVES he can’t read or write.” The video is publically available at <https://www.youtube.com/watch?v=I9Radx9V730>. At the 1:40 minute mark of the video, TashaK states that she has “exclusive messages” involving Inmate A. TashaK then proceeds to scroll through her phone and read portions of verbatim language of the email messages between Inmate A and another person. TashaK states that the dates of the emails are November 11, 2019 and November 14, 2019. I have reviewed Inmate A’s email communications, which are housed on the TruView system, and the information that TashaK reads during the



video is contained in Inmate A's email communications. The verbatim passages that TashaK reads are the email communications themselves that are housed on the TruView system.

25. I have also reviewed email communications that Officer A sent or received from Officer A's official BOP email address. These emails exist on the BOP network and BOP provided law enforcement with the emails.<sup>1</sup>

26. On November 13, 2019, Officer A sent an email from her official BOP email address to a Gmail address. The Gmail address bears Officer A's first initial and last name, and appears to be her personal email address.

27. The email contained an attachment named "Scan\_0001." The attachment is 12 pages long, and contains Inmate A's records from the TruView system.

28. The first four pages of the email attachment appear to be scans of printouts of Inmate A's visitor logs. The corner of each page has been ripped away or obscured in the scanning process. According to BOP information technology personnel, the corner of the page would have contained the date and time that the record had been accessed. Page five of the attachment contains Inmate A's funding log, which demonstrates transactions of funds flowing to Inmate A and details on

---

<sup>1</sup> As set forth more fully below, a warning banner appearing on all BOP electronic devices states "Users should have no expectation of privacy as to **any communication** on or information stored within the system, including information stored on the network..." (emphasis added).

those funds, including the name and address of the sender and the amount sent. Again, the corners of this page were torn away or obscured and there is no date or time visible.

29. Page seven of the attachment includes log information on email communications received by Inmate A. It lists the time of the communication and the sender's email address. In handwriting below this log, someone has written, "Calls her Cookie from Empire."

30. Pages nine through 12 contain what appears to be Inmate A's email communications. The email communications are dated from the period of November 11, 2019 through November 13, 2019.

31. Inmate A's email communications on pages 9–12 of the attachment appear to include the emails that TashaK divulged in her December 22, 2019 YouTube video.

### **The Subject Computer**

32. The **Subject Computer** is owned by BOP.

33. Officer A used the **Subject Computer** in the course of her duties as the Disciplinary Hearing officer at the Thomson Correctional Facility. According to BOP records, Officer A used the **Subject Computer** between December 1, 2019 through December 31, 2019, which includes some of the period during which Officer A accessed Inmate A's inmate records on the TruView system.

34. I have reviewed a BOP policy entitled "Computer User Rules of Behavior," which sets forth certain rules for using BOP computer equipment,

including certain prohibited uses. According to BOP Office of Internal Affairs, all BOP electronic devices, including the **Subject Computer**, are equipped with warning banners which display the “Computer User Rules of Behavior” and appear on the screen of the device each time an employee logs on to the computer.

35. I have reviewed a copy of the warning banner that appears on BOP electronic devices.

a. The warning banner states: “By accessing and using this computer, you are consenting to such monitoring and information retrieval for law enforcement and other purposes. Users should have no expectation of privacy as to any communication on or information stored within the system, including information stored on the network and stored locally on the hard drive or other media in use with this unit (e.g., floppy drives, CD-ROMS, etc.).”

36. The warning banner lists certain prohibitions on the use of government computer resources, including:

a. “[u]sing government-owned software, information, or equipment...for unofficial purposes exceeding what is licensed or authorized.”

b. “[d]ivulging sensitive government information to any person who is not authorized to have access to the information, e.g. by emailing such information.”

c. “Removing sensitive documents (electronic media) from the workplace without proper authority.”

## II. SPECIFICS REGARDING SEARCHES OF ELECTRONIC STORAGE MEDIA

37. Based upon my training and experience, and the training and experience of specially trained personnel whom I have consulted, searches of evidence from electronic storage media commonly require agents to download or copy information from the electronic storage media and their components, or remove most or all electronic storage media items (e.g. computer hardware, computer software, computer-related documentation, and cellular telephones) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

a. Electronic storage media can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site.

b. Searching electronic storage media for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of an electronic storage media system is an exacting scientific procedure which is designed

to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since electronic storage media evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

38. In order to fully retrieve data from a computer system, the analyst needs all storage media as well as the computer. The analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard disk drives or on external media).

39. In addition, electronic storage media such as a computer, its storage devices, peripherals, and Internet connection interface may be instrumentalities of the crime(s) and are subject to seizure as such if they contain contraband or were used to carry out criminal activity.

### III. PROCEDURES TO BE FOLLOWED IN SEARCHING ELECTRONIC STORAGE MEDIA

40. Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant will authorize the removal of electronic storage media and copying of electronically stored information found in the **Subject Computer** described in Attachment A so that information found in the **Subject Computer** may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol.

41. The review of electronically stored information and electronic storage media in the **Subject Computer** may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (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 offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B;

d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

42. The government will return to BOP any electronic storage media removed from the **Subject Computer** within 30 days of the removal, unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

#### IV. CONCLUSION

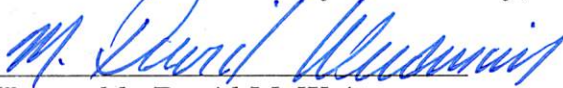
43. Based on the above information, I respectfully submit that there is probable cause to believe that the offense of unauthorized access of a computer to obtain information from the Federal Bureau of Prisons, in violation of Title 18, United States Code, Section 1030(a)(2)(B), has been committed, and that evidence and instrumentalities relating to this criminal conduct, as further described in Attachment B, will be found in the **Subject Computer**, as further described in Attachment A. I therefore respectfully request that this Court issue a search warrant for the **Subject Computer** more particularly described in Attachment A, authorizing the seizure of the items described in Attachment B, pursuant to the protocol described in the addendum to Attachment B.

FURTHER AFFIANT SAYETH NOT.



\_\_\_\_\_  
Matt Loux  
Special Agent  
Department of Justice  
Office of the Inspector General

Subscribed and sworn  
before me this 27th day of February, 2020



\_\_\_\_\_  
Honorable David M. Weisman  
United States Magistrate Judge



ATTACHMENT A

DESCRIPTION OF ITEM TO BE SEARCHED

The **Subject Computer** is a black HP "EliteDesk" desktop computer, bearing serial number 2UA8480JG51506. The **Subject Computer** is currently in the possession of OIG. A photograph of the **Subject Computer** is below.



**ATTACHMENT B**

**LIST OF ITEMS TO BE SEIZED**

Evidence and instrumentalities concerning violation of Title 18, United States Code, Section 1030(a)(2)(B), as follows:

1. All information (including documents, communications, or other items) related to Inmate A, any of Inmate A's associates, "TashaK," or "UnWineWithTashaK."
2. All information related to any relationship or interaction between Officer A and the blogger known as "TashaK" or "UnWineWithTashaK."
3. All information related to internet history, websites visited, and internet searches that relate to Inmate A, any of Inmate A's associates, "TashaK," or "UnWineWithTashaK."
4. All information related to BOP's Code of Conduct or Computer Rules of Behavior;
5. All information related to Officer A's access of the TruView system.
6. Items related to all names or contact information stored on the computer, including any electronically stored address books or contact lists;
7. All information related to any financial transactions or discussions of such transactions between Officer A and the blogger known as "TashaK,;"
8. Photographs relating to the **Subject Offense**, including screen shots of information pertaining to Inmate A, "TashaK" or "UnWineWithTashaK."

## ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the **Subject Computer** described in Attachment A so that the information found in the **Subject Computer** may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (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 offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.

UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNDER SEAL

In the Matter of the Search of:

Case Number:

**20M148**

the HP desktop computer, bearing serial number  
2UA8480JG51506, further described in  
Attachment A

**SEARCH AND SEIZURE WARRANT**

To: Matt Loux and any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Northern District of Illinois:

**See Attachment A**

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

**See Attachment B**

**YOU ARE HEREBY COMMANDED** to execute this warrant on or before March 4, 2020 in the daytime (6:00 a.m. to 10:00 p.m.).

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the issuing United States Magistrate Judge.

Date and time issued: February 27, 2020 @ 12:40p.m.

  
\_\_\_\_\_  
Judge's signature

City and State: Chicago, Illinois

DAVID M. WEISMAN, U.S. Magistrate Judge  
Printed name and title

**Return**

Case No:

Date and Time Warrant Executed:

Copy of Warrant and Inventory Left With:

Inventory made in the presence of:

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Executing officer's signature*

\_\_\_\_\_  
*Printed name and title*

ATTACHMENT A

DESCRIPTION OF ITEM TO BE SEARCHED

The **Subject Computer** is a black HP "EliteDesk" desktop computer, bearing serial number 2UA8480JG51506. The **Subject Computer** is currently in the possession of OIG. A photograph of the **Subject Computer** is below.



## ATTACHMENT B

### LIST OF ITEMS TO BE SEIZED

Evidence and instrumentalities concerning violation of Title 18, United States Code, Section 1030(a)(2)(B), as follows:

1. All information (including documents, communications, or other items) related to Inmate A, any of Inmate A's associates, "TashaK," or "UnWineWithTashaK."
2. All information related to any relationship or interaction between Officer A and the blogger known as "TashaK" or "UnWineWithTashaK."
3. All information related to internet history, websites visited, and internet searches that relate to Inmate A, any of Inmate A's associates, "TashaK," or "UnWineWithTashaK."
4. All information related to BOP's Code of Conduct or Computer Rules of Behavior;
5. All information related to Officer A's access of the TruView system.
6. Items related to all names or contact information stored on the computer, including any electronically stored address books or contact lists;
7. All information related to any financial transactions or discussions of such transactions between Officer A and the blogger known as "TashaK;"
8. Photographs relating to the **Subject Offense**, including screen shots of information pertaining to Inmate A, "TashaK" or "UnWineWithTashaK."

## ADDENDUM TO ATTACHMENT B

Pursuant to Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure, this warrant authorizes the removal of electronic storage media and copying of electronically stored information found in the **Subject Computer** described in Attachment A so that the information found in the **Subject Computer** may be reviewed in a secure environment for information consistent with the warrant. That review shall be conducted pursuant to the following protocol:

The review of electronically stored information and electronic storage media removed from the premises described in Attachment A may include the following techniques (the following is a non-exclusive list, and the government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein):

- a. examination of all the data contained in such computer hardware, computer software, and/or memory storage devices to determine whether that data falls within the items to be seized as set forth in Attachment B;
- b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B (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 offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. surveying file directories and the individual files they contain to determine whether they include data falling within the list of items to be seized as set forth in Attachment B; and
- d. opening or reading portions of files, and performing key word searches of files, in order to determine whether their contents fall within the items to be seized as set forth in Attachment B.

The government will return any electronic storage media removed from the premises described in Attachment A within 30 days of the removal unless, pursuant to Rule 41(c)(2) or (3) of the Federal Rules of Criminal Procedure, the removed electronic storage media contains contraband or constitutes an instrumentality of crime, or unless otherwise ordered by the Court.