EXHIBIT 3

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

BRIAN HUDDLESTON, Plaintiff, v. FEDERAL BUREAU OF INVESTIGATION and UNITED STATES DEPARTMENT OF JUSTICE, Defendants.	CIVIL ACTION No. 4:20CV00447

DECLARATION OF WILLIAM R. WICKMAN

I, William R. Wickman, declare as follows:

1. I am the Acting Supervisory Special Agent of the Philadelphia Regional Computer Forensics Laboratory, Philadelphia Division, Federal Bureau of Investigation (FBI), located in Philadelphia, Pennsylvania. I have been a certified FBI Digital Forensic Examiner since 2016. I joined the FBI in September 2005, and prior to my current position, I was assigned to the Violent Gangs Task Force. Prior to joining the FBI, I served as a Special Agent with the United States Customs Service and was assigned to work international drug smuggling investigations.

2. The statements contained in this declaration are based upon my personal knowledge, upon information provided to me in my official capacity, and upon conclusions and determinations reached and made in accordance therewith.

3. I submit this declaration to demonstrate that the FBI has complied to the fullest extent possible with the Court's Memorandum Opinion and Order dated March 24, 2025 (ECF

No. 214), the Cour's Memorandum Opinion and Order dated November 28, 2023 (ECF No. 136) and its Amended Memorandum Opinion and Order dated August 15, 2024 (ECF No. 176) collectively requiring the FBI to conduct and complete a document-by-document review of the information it possesses on the compact disk (CD) containing the image of Seth Rich's personal laptop (hereinafter as "Personal Laptop"), Seth Rich's Work Laptop, the DVD and the tape drive that is responsive to Plaintiff's FOIA requests and to either (1) produce *Vaughn* Indexes addressing the information it possesses on the compact disk containing images of Seth Rich's personal laptop, Seth Rich's Work Laptop, the DVD, and the tape drive that is responsive to Plaintiff's FOIA requests;[1] or (2) file a motion for summary judgment regarding the information it possesses on the compact disk containing images of Seth Rich's personal laptop, Seth Rich's Work Laptop, the DVD, and the tape drive that is responsive to Plaintiff's FOIA requests.

4. Based on my professional background, knowledge, and familiarity with this case, the FBI maintains a forensic image of the Work Laptop. A forensic image is a bit-for-bit copy of the contents of the Work Laptop hard drive, capturing every addressable sector of the drive, not just active files. That forensic image is a sound replica that preserves the original evidence without alteration. Part of the forensic imaging process included a directory file listing and verification hashing to ensure integrity of the original evidence. The forensic image is an E01 file, which cannot be natively viewed because it is a containerized forensic format. Forensic software and tools are required to parse out the data from the E01 file.

5. Based on my training and experience, I know that neither Windows or macOS natively generate a file that records or logs file transfer activity from a computer to an external storage device. Absent enterprise auditing tools or third-party monitoring software, no such file

[1] The *Vaughn* Index must address the metadata contained within Seth Rich's work laptop.

would exist on the Work Laptop. Therefore, the FBI cannot produce a record that shows whether there were transfers to external media or what the contents of the transfers may have been.

6. Moreover, determining whether files were downloaded from a laptop to an external storage device is extremely difficult from a digital forensics perspective. Before any analysis could begin, the forensic image would first need to be restored from its archived state and processed using forensic software. The analysis itself, determining whether files were transferred to an external storage device, would require extensive time and effort and would likely be inconclusive.

7. Because the Work Laptop does not contain a file (record) that identifies transfers to external storage media and discloses the contents of the transfer, any possible result from the time-consuming forensic analysis would require the FBI to create new record(s) such as taking screen shots or cutting and pasting information from one document into another or creating entirely new records from existing records, none of which the FBI would have otherwise had before.

8. By way of further explanation, operating systems do not natively log file copy events between an internal storage and an external device. Operating systems do not have a default audit trail to track whether files were copied from the device to USB devices. Operating systems do retain file system metadata, specifically Modified, Accessed, and Created timestamps (MAC). MAC times can reflect file activity on the source or destination drive but not a file transfer itself. MAC times were provided in the file directory listing.

9. Universal Serial Bus (USB) and external device artifacts are limited. Artifacts such as the Windows registry USBSTOR keys, setup API logs, and event logs, if they are captured, may indicate a device was connected and the approximate timeframe of that

connection. But operating system metadata is insufficient, by itself, to determine whether and/or how many files were copied to one or more external storage devices. These artifacts are not useful in this instance because we do not have an identified external device that was connected. So these artifacts will not show what files were accessed or copied, the number of files transferred, or whether a transfer occurred at all.

10. Even if an external device were identified, external devices often lack file system journals to review.

11. In addition, the method by which files are copied to an external device can add additional levels of complexity. Files can be transferred in ways that leave little to no forensic footprint. As described above, operating systems do not natively log file copy events between an internal storage and an external device (native operating system copy and paste). There are multiple transfer methods besides the native operating system's copy and paste. Copying can be performed at the command line, third party tools, in ZIP files, in encrypted containers, direct disk access, or using imaging tools, just to name a few. These alternative transfer methods bypass traditional operating system artifacts and generate inconsistent or no logs at all.

12. Concerning corrupted files, file corruption can range from minor file inconsistencies to damage affecting the file's data. Recovery efforts depend entirely on the type and extent of the file corruption. While some minor corruption can be repaired with recovery tools, more complex data corruption requires manual reconstruction which is extremely time consuming and requires specialized expertise. Even if recovery is successful, verifying the accuracy of the repaired file may not be possible. A repaired file is not the original record. A repaired file is a newly generated file produced through deliberate intervention. In essence, the

forensic examiner is creating a new file which did not exist in its repaired form on the original evidence.

13. The Vaughn indices submitted in this case omit system files. System files are not created by the government or the computer user. System files are generated by the operating system or by software installations and are common to all computers. Unlike user-created files such as .docx, .xlsx, and .pdf, system files are not practically reviewable in the common understanding of the term. While it may be theoretically possible to open certain system files, doing so typically involves specialized software and the contents would not yield information susceptible to a meaningful FOIA exemption analysis.

14. In summary, operating systems do not natively log file transfer activity to external media. Determining if files were transferred from the Work Laptop to an external drive, and if so what those files were, is not achievable through examination of the Work Laptop alone.

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

Executed this 22 day of May 2026.

William R. Wickman
Special Agent
Philadelphia Division
Federal Bureau of Investigation
Philadelphia Pennsylvania