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

BRIAN HUDDLESTON, Plaintiff, vs. **FEDERAL BUREAU OF INVESTIGATION and UNITED STATES DEPARTMENT OF JUSTICE** Defendant	**Case No. 4:20-cv-447-ALM**

PLAINTIFF'S MOTION FOR SUMMARY JUDGMENT

NOW COMES Brian Huddleston, the Plaintiff, moving the Court for summary judgment in his favor pursuant to Fed. R. Civ. P. 56, ordering the Defendant Federal Bureau of Investigation ("FBI") to produce the records and metadata responsive to his FOIA requests concerning Seth Rich's work laptop and personal laptop, and granting such other relief as the Court deems just and proper:

Introduction

Six years into this litigation, the FBI has still failed to comply with the Freedom of Information Act ("FOIA") and with this Court's repeated orders. Plaintiff respectfully urges the Court to re-read his motion to show cause (Dkt. #190) before proceeding further with this motion, primarily so the Court can fully appreciate the FBI's ongoing defiance. Faced with the Court's March 24, 2026 Memorandum Opinion and Order (Dkt. #214), the FBI produced new declarations from Isabel Marie Lara, Asst. U.S. Attorney Michael P. Spence, and Special Agent

William R. Wickman (collectively, the "May 2026 Declarations"), along with a revised *Vaughn* index for Seth Rich's personal laptop, *see* Notice of Compliance (Dkt. #223), but the May 2026 Declarations do not cure the deficiencies in the FBI's *Vaughn* indexes at all. Consider, for example, the bullet-point deficiencies that Plaintiff highlighted on pages 10-11 of the show-cause motion (Dkt. #190). The FBI made no attempt to address those deficiencies despite the fact that this Court ordered the FBI to provide *specific* explanations for all exemptions in its new *Vaughn* index. As demonstrated below and in the accompanying June 10, 2026 Declaration of Yaacov Apelbaum (the "2026 Apelbaum Decl.")(Exhibit 1),[1] the May 2026 Declarations actually confirm the deficiencies and introduce new ones.

Most significantly, the Lara Declaration now reveals — for the first time in this litigation — that Seth Rich's work laptop contains **more than 217,000 items totaling more than 474 gigabytes**. *See* Lara Decl. ¶ 9; 2026 Apelbaum Decl. ¶ 14. The original *Vaughn* index for the work laptop accounted for approximately 2,095 records. The FBI has therefore failed to account for more than 215,000 items — over 99 percent of the contents of the work laptop. *See* 2026 Apelbaum Declaration ¶ 14. That is a tacit admission that the motion to show cause was right: the FBI concealed the vast majority of records on the laptop until it got caught red-handed. Even now, the FBI's only explanation is that the unaccounted-for items are "system files" not subject to FOIA review, but the FBI has provided no count-based file-type breakdown, no hash-set exclusion report, no known-file exclusion report, and no other accounting sufficient to reconcile the gap. *Id.* The FBI is, in effect, asking the Court to blindly trust its assertion that more than

[1] Mr. Apelbaum's qualifications as an expert witness can be found in his previous declarations. *See, e.g.,* Dkt. #141-3. Notably, Mr. Apelbaum has contradicted the FBI's sworn testimony repeatedly, yet no witness for the FBI has ever contradicted any of Mr. Apelbaum's testimony.

215,000 previously-concealed files do not include anything responsive to Plaintiff's FOIA requests.

The May 2026 Declarations also confirm that the FBI never conducted the type of forensic investigation that would actually answer the central question in this case: whether Seth Rich downloaded Democratic National Committee ("DNC") emails onto an external storage device prior to his death. The Wickman Declaration claims that determining whether files were transferred to external devices "is not achievable through examination of the Work Laptop alone." Wickman Decl. ¶ 14. That assertion is materially misleading at best. *See* 2026 Apelbaum Decl. ¶ 13. As Mr. Apelbaum explains, the Wickman Declaration does not identify which standard forensic artifacts the FBI actually examined on the work laptop image, does not state what those artifacts showed, and dodges the question of whether a USB storage device was ever connected to the laptop. *Id.* ¶ 6.

The remaining deficiencies are equally serious. The *Vaughn* indexes still fail to satisfy the three-element standard set forth in *Pomares v. Dep't of Veterans Affs.*, 113 F.4th 870, 881 (9th Cir. 2024). The FBI has reasserted privacy exemptions for the decedent Seth Rich that this Court rejected nearly four years ago in its September 29, 2022 Order (Dkt. #70). The FBI still refuses to disclose tens of thousands of filenames — metadata distinct from file contents — without articulating any exemption applicable to the filenames themselves. And the FBI has, for the first time in 2026, attempted to invoke new exemptions (Exemptions 3 and 4) that should have been raised during the document-by-document review the Court ordered nearly two years ago.

FOIA places the burden of proof on the agency to justify each withholding. *U.S. Dep't of Just. v. Landano*, 508 U.S. 165, 171 (1993). The FBI has repeatedly and systematically failed to

meet that burden. The Court should grant summary judgment for the Plaintiff and grant further relief to ensure production of responsive records.

Background

The Court is intimately familiar with the procedural history of this case. The following is a brief summary of the events that bear directly on this motion.

On August 16, 2024, the Court ordered the FBI to conduct "a document-by-document review of 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" and to either produce *Vaughn* indexes or move for summary judgment. Amended Memorandum Opinion and Order (Dkt. #178) 6-7. The Court had previously ordered the FBI to address the metadata on the work laptop in its *Vaughn* index. November 28, 2023 Order (Dkt. #136) 25.

On March 10, 2025, the FBI produced *Vaughn* indexes for both laptops. Those indexes were grossly deficient. The Plaintiff moved for an order to show cause (Dkt. #190), and on March 24, 2026 the Court denied the motion but ordered the FBI to supplement the record with affidavits and a revised *Vaughn* index. Order (Dkt. #214). Specifically, the Court directed the FBI to file affidavits explaining: (a) the absence of harm explanations from the *Vaughn* indexes; (b) the failure to include all withheld documents in the indexes; (c) the use of conclusory descriptions such as "This file contains 1 item"; and (d) the adequacy of categorical descriptions. The Court further ordered the FBI to produce a supplemental *Vaughn* index identifying (a) the total number of files on the work laptop; (b) the total storage used; and (c) whether and how many files were downloaded to external storage devices. Finally, the Court ordered the FBI to follow through on its offer to produce an amended *Vaughn* index addressing what measures, if any, the FBI took to open, view, or otherwise restore any allegedly corrupted or unreadable files.

On May 26, 2026, the FBI filed its Notice of Compliance (Dkt. #223), attaching the Lara, Spence, and Wickman Declarations and a revised *Vaughn* index for the personal laptop. The May 2026 Declarations did not cure the deficiencies in the FBI's prior submissions. Indeed, they confirmed that those deficiencies are not the result of misunderstanding or oversight, but of the FBI's settled refusal to comply with FOIA and with this Court's orders. The accompanying 2026 Apelbaum Declaration (Exhibit 1) details these failings from a forensic perspective.

Standard of Review

"FOIA cases are typically resolved on motions for summary judgment." *Cooper Cameron Corp. v. U.S. Dep't of Labor*, 280 F.3d 539, 543 (5th Cir. 2002). Summary judgment is appropriate where "the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c).

In a FOIA case, "the burden is on the agency to sustain its action." 5 U.S.C. § 552(a)(4)(B). "To prevail on summary judgment, the agency must demonstrate that no material facts are in dispute, that it has conducted an adequate search for responsive records, and that each responsive record that it has located has either been produced to the plaintiff or is exempt from disclosure." *Cause of Action Inst. v. IRS*, 253 F. Supp. 3d 149, 156 (D.D.C. 2017). FOIA exemptions are "narrowly construed" in favor of disclosure. *Dep't of Air Force v. Rose*, 425 U.S. 352, 361 (1976). The agency must provide "a relatively detailed justification" for invoking each exemption, *Mead Data Cent., Inc. v. U.S. Dep't of Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977), and "conclusory and generalized allegations of exemptions" are insufficient. *Founding Church of Scientology v. NSA*, 610 F.2d 824, 830 (D.C. Cir. 1979).

Where the agency fails to meet its burden, summary judgment must be entered for the requester. *See Pomares*, 113 F.4th at 887 (reversing grant of summary judgment to agency where *Vaughn* index was inadequate); *Wiener v. FBI*, 943 F.2d 972, 988-89 (9th Cir. 1991) (same).

Argument

I. The FBI has failed to account for more than 215,000 items on the work laptop.

The Lara Declaration reveals a discrepancy so large that it cannot be reconciled with the FBI's prior representations to the Court. The work laptop contains more than **217,000 items totaling more than 474 gigabytes of data**. Lara Decl. ¶ 9; 2026 Apelbaum Decl. ¶ 14. The original *Vaughn* index for the work laptop, however, accounts for only approximately 2,095 records. The discrepancy is on the order of 215,000 items, or roughly 99 percent of the work laptop's contents.

The FBI's only explanation is that the unaccounted-for items are "system files" not subject to FOIA review. Lara Decl. ¶ 7; Wickman Decl. ¶ 13. But as Mr. Apelbaum explains, that explanation is insufficient on the present record:

> Although Lara provides a general list of broad categories, including operating system/application files, text files, image files, documents, file folders, and unpartitioned/unallocated space, the declaration does not provide a count-based file-type breakdown, category count, hash-set exclusion report, known-file exclusion report, or other accounting sufficient to reconcile the [217,000+] total items with the [2,095] items listed in the Work Laptop index.

2026 Apelbaum Decl. ¶ 14. As Mr. Apelbaum further explains, the FBI's reliance on a generic "system files" label is overbroad:

> Genuine operating-system binaries may not be meaningfully reviewable as FOIA records. But many forensic artifacts and user-related records reside in system or application locations, including AppData, browser caches, application logs, Jump Lists, LNK files, MRU lists, registry hives, email databases, and other files that may contain user activity or metadata. The declaration does not provide enough information to determine whether the excluded files were truly non-reviewable

> operating-system files or whether relevant user and forensic artifacts were excluded under an overbroad "system files" label.

2026 Apelbaum Decl. ¶ 15.

The Court's August 16, 2024 Order required the FBI to conduct "a document-by-document review of the information it possesses" on the laptops, Dkt. #178 at 6. Once again, the FBI has refused to do that. The plain text of the order requires review of *the information it possesses* — not just the small percentage of files that the FBI unilaterally deemed worthy of review.

Where an agency excludes a substantial volume of material from its search or review, the agency bears the burden of justifying that exclusion. *Oglesby v. U.S. Dep't of the Army*, 920 F.2d 57, 68 (D.C. Cir. 1990) (agency must show "it made a good faith effort to conduct a search for the requested records, using methods which can be reasonably expected to produce the information requested"). The FBI's blanket assertion that 215,000 files are non-reviewable "system files" — without categorization, without count, and without any explanation of how that determination was made on a file-by-file basis — does not meet that burden. The FBI's failure to produce a categorized inventory of the work laptop's contents is, by itself, sufficient grounds to enter summary judgment for the Plaintiff on the adequacy-of-search issue.

II. The Vaughn indexes fail to satisfy the Pomares standard.

"Specificity is the defining requirement of the *Vaughn* index." *Wiener*, 943 F.2d at 979. An adequate *Vaughn* index must: "(1) identify each document withheld; (2) state the applicable statutory exemption; and (3) explain how disclosure would harm the interests protected by the statutory exemption." *Pomares*, 113 F.4th at 881. "An agency must provide more than 'boilerplate or conclusory statements,' and allow 'a meaningful opportunity to contest, and . . .

an adequate foundation to review,' the agency's withholdings." *Id.* (citations omitted). The FBI's *Vaughn* indexes fail all three elements.

A. The FBI failed to identify each document withheld.

The work laptop *Vaughn* index repeatedly describes records as "This file contains 1 item" without identifying what the item is. *See* Work Index (Dkt. #190-1) pp. 3, 4, 5, 9, 12. The FBI's explanation for these descriptions — that they refer to directory structure rather than file contents (Lara Decl. ¶¶ 7-8) — only deepens the problem. If the entries describe folders rather than files, then the underlying files have not been described in the index at all, and the index does not "identify each document withheld" as *Pomares* requires.

The personal laptop *Vaughn* index suffers from a different but equally serious defect. Every single filename on the personal laptop index is redacted. *See* Personal Index (Dkt. #190-2) and Revised Personal Index (Dkt. #223-4). The FBI has provided generic content descriptions — "Rental Application," "Dental Bill," "Poem" — without disclosing the actual filenames. Filenames are metadata distinct from file contents. *See Frazier v. Se. Georgia Health Sys., Inc.*, No. 2:21-CV-21, 2023 WL 10366708, at *9 (S.D. Ga. Nov. 8, 2023) (file name is metadata), *aff'd*, No. 24-10976, 2024 WL 4357399 (11th Cir. Oct. 1, 2024); *United States v. Sawatzky*, 994 F.3d 919, 923 (8th Cir. 2021). The FBI has not invoked any exemption applicable to filenames themselves — only the underlying file contents — and the personal laptop *Vaughn* index therefore fails to even identify the documents it has withheld.

B. The FBI failed to explain how disclosure would harm the protected interests.

The third element of *Pomares* — explaining how disclosure of each document would harm the interest protected by the claimed exemption — is absent from every entry in both *Vaughn* indexes. The FBI does not dispute this. Rather, it argues that harm explanations belong

in the supporting declarations rather than the *Vaughn* indexes themselves. Notice of Compliance (Dkt. #223) at 6 ("the explanation as to how disclosure of information would harm the interest claimed by the statutory exemptions is contained in the declarations rather than in the *Vaughn* indices").

That position cannot be reconciled with *Pomares*, which holds that the *Vaughn* index *itself* must "explain how disclosure would harm the interests protected by the statutory exemption." 113 F.4th at 881; *see also King v. U.S. Dep't of Justice*, 830 F.2d 210, 223-24 (D.C. Cir. 1987) ("A more particularized record — a *Vaughn* Index — must be furnished" when supporting declarations are conclusory). Even if harm explanations could properly appear elsewhere, the May 2026 Declarations do not actually provide document-specific harm analysis. They provide categorical and generic statements that any release of "any data of any kind" would interfere with the investigation. Spence Decl. ¶ 7.

Categorical and generic statements are precisely what *Vaughn* forbids. "'[B]road categorical descriptions' such as these are inadequate to allow 'a reviewing court to engage in a meaningful review of the agency's decision' and therefore must be rejected." *Defs. of Wildlife v. U.S. Border Patrol*, 623 F. Supp. 2d 83, 88-89 (D.D.C. 2009) (citations omitted); *see also Campbell v. U.S. Dep't of Justice*, 164 F.3d 20, 30 (D.C. Cir. 1998) (the government must furnish "detailed and specific information demonstrating that material withheld is logically within the domain of the exemption claimed"); *Watkins L. & Advoc., PLLC v. United States Dep't of Just.*, 78 F.4th 436, 451-52 (D.C. Cir. 2023) (rejecting conclusory *Vaughn* index).

C. The FBI's descriptions are too conclusory to permit meaningful review.

The personal laptop *Vaughn* index applies the same boilerplate exemptions — typically 6, 7(A), 7(C), and 7(E) — to every record without explaining how those exemptions apply to the specific document. Examples include:

- Records 18 and 64: "PowerPoint Depicting Editorial Cartoon" last modified in 2008 — nearly eight years before Mr. Rich's death and the alleged DNC "hack";
- Records 16, 31, 66, 67, and 92: "PowerPoint Concerning Time Spent Campaigning for Scott Kleeb," the 2008 Democratic Senate candidate;
- Record 83: a "Written School Assignment, Essay, or Term Paper" last modified November 17, 2008, when Mr. Rich was a college freshman;
- Record 85: "Video Game Notes" from 2010;
- Records 71 and 131: "List of quotations" from 2008;
- Record 287: "Experian Credit Report" from 2013;
- Records 258-263, 268, 287-288, 324, 330-332: undated forms, bills, certificates, applications, party menus, and quiz feedback; and
- Record 1297: an undated "Poem."

How, exactly, would the release of any of the foregoing information – all of which occurred years before the murder and the purported "hacking" by Russian agents – interfere with the murder investigation or the "hacking" investigation? In other words, how could exemptions 6, 7(A), 7(C), and 7(E) or possibly apply? The Court, the Plaintiff, and the public can only guess at the answer.

The work laptop index is no better, describing records as "Image of a small black circle with a white arrow pointing down to 6 o'clock" and "Image of a small black circle with a white arrow pointing down between 4 and 5 o'clock." Work Index (Dkt. #190-1) at p. 5. These descriptions do not, and cannot, satisfy *Vaughn*. Among other things, they make it impossible to

determine how a 2008 PowerPoint about an editorial cartoon, a 2008 college term paper, 2010 video game notes, or a 2013 credit report could possibly relate to (1) a 2016 homicide investigation; (2) a 2016 alleged hack of the DNC; or (3) any of the FOIA exemptions invoked. The FBI "rubber-stamped" the same exemptions on every record without any attempt to apply them to the actual content.

III. The FBI's assertion of Exemption 7(A) cannot survive document-specific scrutiny.

FOIA Exemption 7(A) protects from disclosure "records or information compiled for law enforcement purposes" when disclosure "could reasonably be expected to interfere with enforcement proceedings." 5 U.S.C. § 552(b)(7)(A). The Supreme Court has held that an agency may invoke Exemption 7(A) on a *category-by-category* basis, but "only to the extent that the records categorized contain similar information that can be evaluated together." *NLRB v. Robbins Tire & Rubber Co.*, 437 U.S. 214, 236 (1978). The agency must define categories that are "sufficiently distinct to allow a court to grasp how each . . . category of documents, if disclosed, would interfere with the investigation." *Bevis v. Dep't of State*, 801 F.2d 1386, 1389-90 (D.C. Cir. 1986).

The FBI has failed that test. It has invoked Exemption 7(A) categorically across the contents of two entire laptops, asserting that "the production of any data of any kind from any computer possessed or used by Seth Rich at the time of his death reasonably could be expected to interfere with law enforcement proceedings." Spence Decl. ¶ 7 (emphasis added). That is not a category-based justification — it is a sweeping, blanket assertion of exemption that the D.C. Circuit and other courts have repeatedly rejected. *See Crooker v. Bureau of Alcohol, Tobacco & Firearms*, 789 F.2d 64, 66-67 (D.C. Cir. 1986) (rejecting categorical Exemption 7(A) claim

where agency failed to explain how each category of records would interfere with enforcement); *Campbell*, 164 F.3d at 30.

The FBI's position is particularly implausible as applied to records that bear no conceivable relationship to either the homicide investigation or the alleged hacking investigation. Plaintiff has identified above documents created six to eight years before either event — college term papers, video game notes, editorial cartoons, political campaign PowerPoints for a 2008 Senate race. The FBI has not even attempted to articulate how releasing such records would "interfere" with the investigation of a 2016 "botched robbery" or a 2016 cyber intrusion. To accept the FBI's position would be to hold that Exemption 7(A) authorizes the FBI to withhold *any* record found anywhere on a device *ever* possessed by a homicide victim, no matter how old or unrelated. That is not the law.

The Spence Declaration's only effort to articulate a specific harm — that release would "lead to a flood of spurious tips to law enforcement" (Spence Decl. ¶ 6) — is not the type of interference contemplated by Exemption 7(A). "Interference" under the exemption means interference with the ability to gather evidence, develop a case, identify witnesses, or otherwise prosecute the matter — not the inconvenience of fielding public inquiries. *See Citizens for Resp. & Ethics in Wash. v. U.S. Dep't of Justice*, 746 F.3d 1082, 1098 (D.C. Cir. 2014). Indeed, if "spurious tips" justified withholding, virtually every high-profile criminal investigation could be cloaked in permanent FOIA secrecy.

IV. The FBI has reasserted privacy exemptions this Court already rejected.

On September 29, 2022, this Court squarely rejected the FBI's attempt to assert global privacy exemptions on behalf of the decedent Seth Rich. Dkt. #70 at 43-48. The Court explained that decedents have greatly diminished privacy interests and that privacy exemptions may be

asserted on behalf of survivors only in very narrow circumstances limited to death-scene images, autopsy reports, and audio recordings of final moments. *Id.* at 44.

The personal laptop *Vaughn* index contains no death-scene images, no autopsy reports, and no audio files of Mr. Rich's final moments. Nevertheless, the FBI has reasserted Exemptions 6 and 7(C) for every single record in the index. The Lara Declaration concedes the prior ruling but states the FBI is reasserting the exemption "to preserve the issue for appeal." Lara Decl. ¶ 26.

That is not a legitimate basis to defy a standing order of this Court. The Supreme Court has long held that "an order issued by a court with jurisdiction over the subject matter and person must be obeyed by the parties until it is reversed by orderly and proper proceedings." *United States v. United Mine Workers of Am.*, 330 U.S. 258, 293 (1947); *see also Maness v. Meyers*, 419 U.S. 449, 458 (1975) ("[A]ll orders and judgments of courts must be complied with promptly. If a person to whom a court directs an order believes that order is incorrect the remedy is to appeal, but, absent a stay, he must comply promptly with the order pending appeal."); *Howat v. Kansas*, 258 U.S. 181, 189-90 (1922) (an order "must be obeyed . . . however erroneous the action of the court may be" until reversed). The Fifth Circuit has applied these principles directly to federal agencies, holding the Department of the Interior in civil contempt for taking steps to circumvent rather than to obey a district court's order. *Hornbeck Offshore Servs., L.L.C. v. Salazar*, 713 F.3d 787, 792 (5th Cir. 2013).

These authorities defeat the FBI's "preserve for appeal" theory at the threshold. The way to preserve an issue for appellate review is to raise the objection on the record and maintain it; it is not to defy the order in the meantime. The FBI fully preserved its position regarding privacy exemptions for Seth Rich by litigating the issue in 2022 and obtaining a ruling. Nothing more was required to preserve the issue for an eventual appeal from final judgment. Continued

reassertion of the same global privacy exemptions — in defiance of the Court's ruling — was not necessary to preserve anything. It was simply non-compliance dressed up in appellate clothing.

Nor are the FBI's interlocutory remedies still available. To obtain interlocutory review of the September 29, 2022 Order, the FBI had to invoke one of two procedures, and it invoked neither. *First*, the FBI could have asked this Court to certify the order for interlocutory appeal under 28 U.S.C. § 1292(b), then petitioned the Fifth Circuit for permission to appeal within 10 days of certification. *See* 28 U.S.C. § 1292(b); Fed. R. App. P. 5(a)(2). The FBI never sought certification — not within 30 days of the order, not within 30 months, and not at any subsequent time. *Second*, the FBI could have sought a writ of mandamus from the Fifth Circuit. *See In re Volkswagen of Am., Inc.*, 545 F.3d 304, 309-11 (5th Cir. 2008) (en banc) (discussing standards for mandamus). Mandamus, however, is subject to laches and must be sought with reasonable promptness. The Fifth Circuit has denied mandamus petitions filed only *three months* after the challenged order. *In re Red Barn Motors, Inc.*, 794 F.3d 481, 485 (5th Cir. 2015) (denying petition where petitioners offered "no explanation for waiting more than three months before filing"). Nearly four years have now elapsed since the September 29, 2022 Order. Both interlocutory routes are firmly closed.

Compounding the problem, the September 29, 2022 Order is the law of the case. "The law-of-the-case doctrine posits that when a court decides upon a rule of law, that decision should continue to govern the same issues in subsequent stages in the same case." *Arizona v. California*, 460 U.S. 605, 618 (1983). The Fifth Circuit applies the doctrine to bar relitigation of issues previously decided in the same litigation, including issues resolved by interlocutory rulings. *See Royal Ins. Co. of Am. v. Quinn-L Cap. Corp.*, 3 F.3d 877, 880-81 (5th Cir. 1993) (law-of-the-case principles apply to interlocutory rulings within a single continuing lawsuit); *United States v.*

Lee, 358 F.3d 315, 320 (5th Cir. 2004) ("Under the law of the case doctrine, an issue of law or fact decided on appeal may not be reexamined either by the district court on remand or by the appellate court on a subsequent appeal."). The Court's rejection of global privacy exemptions for Seth Rich is the law of the case. The FBI cannot relitigate that ruling by simply re-asserting the same exemptions in a new *Vaughn* index nearly four years after the ruling was issued.

Even on the merits, the FBI's privacy claims fail. The personal-privacy exemption requires the agency to weigh the privacy interest against the public interest in disclosure. *U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 776 (1989). The privacy interest of a decedent is, at best, attenuated, and the surviving-family interest extends only to a narrow category of records this Court has already identified. The public interest in disclosure here is significant: the records sought may shed light on whether the FBI built and maintained a false narrative regarding the source of the DNC emails published by Wikileaks in 2016, which is a matter of substantial public concern.

V. The Wickman Declaration does not establish that the work laptop was forensically examined for evidence of file transfers.

This Court's March 24, 2026 Order directed the FBI to produce a supplemental *Vaughn* index identifying "whether and/or how many files were downloaded from the Work Laptop to one or more external storage device(s)." Dkt. #214 at 20. The Wickman Declaration purports to respond to this directive, but it does not. *See* 2026 Apelbaum Decl. ¶¶ 3, 17.

A. The Wickman Declaration relies on narrow statements that are materially misleading.

The Wickman Declaration's technical claims, when examined closely, consist largely of narrowly-true statements presented in a misleading way. For example, Wickman states that "neither Windows or macOS natively generate a file that records or logs file transfer activity

from a computer to an external storage device." Wickman Decl. ¶ 5. As Mr. Apelbaum explains, that statement is, read narrowly, true — but it is materially incomplete:

> The absence of a single native "file-transfer log" does not mean that forensic artifacts cannot identify external storage activity, USB device connection history, mounted volumes, user activity involving external devices, or relevant timeline correlations.

2026 Apelbaum Decl. ¶ 4. Standard Windows forensic analysis routinely uses numerous artifact categories to determine "whether external storage devices were connected, when they were connected, which user profile interacted with mounted volumes, and what files or folders were accessed around those times." *Id.* ¶ 5. These include:

- USBSTOR registry keys and other USB registry keys (recording device connection history, vendor IDs, product IDs, and serial numbers);
- MountedDevices and MountPoints2 registry keys (recording mounted volume history, including per user profile);
- SetupAPI logs (logging USB device installation events with timestamps);
- Windows Event Logs (recording device connection events);
- LNK files in Recent folders (automatically created when files are opened, often referencing external paths and volume serial numbers);
- Jump Lists (recording recently accessed files);
- Shellbags (preserving folder browsing history, including folders on external drives);
- RecentDocs and Office MRU data (referencing recently accessed documents and external paths);
- Prefetch, AmCache, and ShimCache (recording program execution and file-system activity);
- File-system timeline artifacts; and
- NTFS metadata, including $MFT, $LogFile, and $UsnJrnl.

2026 Apelbaum Decl. ¶¶ 5, 18.

The Court need not rely on Mr. Appelbaum's testimony alone. The peer-reviewed digital forensics literature has, for two decades, established that Windows generates multiple artifact categories that, in combination, allow forensic examiners to reconstruct external storage activity and develop a timeline of USB device connections. *See* Harlan Carvey & Cory Altheide, *Tracking USB Storage: Analysis of Windows Artifacts Generated by USB Storage Devices*, 2 Digital Investigation 94, 94 (2005) ("These artifacts can be used to develop a timeline for USB storage devices being connected to the system, as well as demonstrate that particular devices were connected to other Windows systems."); Ayesha Arshad, Waseem Iqbal & Haider Abbas, *USB Storage Device Forensics for Windows 10*, 63 J. Forensic Sci. 856 (2018) (presenting systematic methodology for Windows 10 USB forensic analysis). The U.S. Government's own National Institute of Standards and Technology has similarly confirmed that operating-system audit records "can provide valuable information, including the time that an event occurred and the origin of the event." Karen Kent, Suzanne Chevalier, Tim Grance & Hung Dang, *Guide to Integrating Forensic Techniques into Incident Response*, NIST Special Publication 800-86, § 3.1.1, at 3-2 to 3-3 (Aug. 2006).[2]

B. The Wickman Declaration nowhere identifies which artifacts the FBI actually examined.

The Wickman Declaration acknowledges the existence of some of the artifacts described above — specifically, USBSTOR keys, setup API logs, and event logs (Wickman Decl. ¶ 9) — but as Mr. Apelbaum observes:

> [T]he declaration never states whether the FBI actually examined those artifacts on the Work Laptop image. It never states what those artifacts showed. It never states that no USB storage device was connected. It never identifies any connected devices,

[2] Inosfar as these facts were well-known twenty years ago in forensic science, one must ask how the supervisor of the computer forensics lab of the nation's "premier law enforcement agency" was unaware of them.

> timestamps, serial numbers, volume identifiers, drive letters, or user-profile correlations. That omission is significant.

2026 Apelbaum Decl. ¶ 6. A competent declaration from a CART Supervisory Special Agent responding to a court order about external device activity would identify each artifact category examined, the tool used, and the results obtained. *Id.* ¶ 19. The Wickman Declaration provides none of that information. "The declaration presents a conclusion without the analysis needed to evaluate it." *Id.* ¶ 8. [3]

C. Wickman's reasoning about USB artifacts is circular.

Wickman states that USB and external-device artifacts are "not useful in this instance because we do not have an identified external device that was connected." Wickman Decl. ¶ 9. Wickman's testimony is akin to a homicide detective looking at a gunshot victim and then declaring, "We have not recovered the firearm, so we cannot say whether the victim was shot." Obviously, one need not recover the firearm to determine whether the victim was shot, because, among other things, there will be one or more bullets in the victim. Similarly, one need not recover the external device to determine whether such a device had been connected to the Work Laptop, namely because there will be one or more artifacts in the laptop data. As Mr. Apelbaum explains, Wickman's testimony reverses the forensic sequence:

> One purpose of examining USBSTOR, USB registry artifacts, SetupAPI logs, MountedDevices, MountPoints2, event logs, and related artifacts is to determine whether external devices were connected in the first place. If those artifacts were examined and showed no connected external storage devices, that would be a direct and important finding. Wickman does not say that.

[3]The federal forensic standard requires the documentation Wickman omitted: "Analysts should use a methodical approach in analyzing the available data so that analysts can either draw appropriate conclusions based on the available data or determine that no conclusion can yet be drawn. If evidence might be needed for legal or internal disciplinary actions, analysts should carefully document the findings and all steps taken." NIST Special Publication 800-86, § 3.5, at 3-8 (Aug. 2006).

2026 Apelbaum Decl. ¶ 7. Wickman cannot rely on the absence of an identified device to excuse the failure to examine the artifacts that would identify such a device. The artifacts Wickman dismisses as "not useful" are precisely the artifacts that identify previously-connected USB devices in the first place. *See* Arshad, Iqbal & Abbas, *supra*, at 858-62 (demonstrating that USBSTOR registry keys, setupapi.dev.log, and Windows Event Logs collectively reveal device "Device ID," "Friendly Name" (manufacturer and model), serial number, and first and last connection timestamps). NIST instructs that "[a]nalysts should be aware of the range of possible data sources" and "should be prepared to use alternate data sources if it is not feasible to collect data from a primary source." NIST Special Publication 800-86, § 3.5, at 3-7 to 3-8 (Aug. 2006). If the FBI had examined the artifacts and found no record of any external storage device connection, the declaration could and should have said so directly. Instead, it appears that the FBI never looked at the artifacts.

D. Wickman reframes the question this Court asked.

Equally significant, the Wickman Declaration recharacterizes the question this Court asked. The Court asked whether files were downloaded to external storage devices. Dkt. #214 at 20. Wickman reframes the question as whether every transferred file could be conclusively identified. Wickman Decl. ¶¶ 6, 14. These are materially different questions. As Mr. Apelbaum explains:

> Wickman's summary statement that determining whether files were transferred from the Work Laptop to an external drive is "not achievable through examination of the Work Laptop alone" is overbroad and materially misleading. A more accurate statement would be: examination of the Work Laptop alone may not always identify every file copied to external media with certainty. That is very different from saying that external-device activity is not achievable or not meaningfully examinable from the source computer.

2026 Apelbaum Decl. ¶ 13. Standard forensic analysis can frequently establish that file transfers occurred (through USB connection events combined with file access timestamps) even when it cannot establish *which specific files* were copied.[4] By answering only the narrower question, Wickman avoids the broader question the Court actually asked.

E. Wickman's "new records" claim conflates legal and forensic categories.

Wickman further claims that determining whether files were downloaded would require the FBI to "create new records," which he argues exceeds FOIA's requirements. Wickman Decl. ¶ 7. That argument conflates a legal characterization with a forensic limitation:

> Wickman's statement that the FBI would have to "create new records" is a legal characterization, not a forensic limitation. The FBI already possesses a forensic image of the Work Laptop. The relevant artifacts, if present, are existing data within that forensic image. Parsing, extracting, or reporting the contents of existing forensic artifacts is not the same technical act as inventing new evidence.

2026 Apelbaum Decl. ¶ 9. The Court ordered the FBI to investigate and report on a specific factual question. The data needed to answer that question — the standard Windows forensic artifacts — already exists within the forensic image of the work laptop that the FBI already possesses.[5] Extracting and reporting that data is not the creation of a new record; it is the review

[4] *See* Bhupendra Singh & Upasna Singh, *A Forensic Insight into Windows 10 Jump Lists*, 17 Digital Investigation 1, 3 (2016) (Jump Lists record "MAC (Modified, Accessed, and Created) timestamps" and "volume name from which the file was accessed," persisting "even after the files and their target applications are removed from the system"); Yuandong Zhu, Pavel Gladyshev & Joshua James, *Using Shellbag Information to Reconstruct User Activities*, 6 Digital Investigation S69, S69 (2009) (presenting methodology to "prove that certain interactions between the user and system must have, or must not have happened during a certain time period"); Graeme Horsman, Anda Caithness & Christos Katsavounidis, *A Forensic Exploration of the Microsoft Windows 10 Timeline*, 64 J. Forensic Sci. 577 (2019). The federal forensic standard identifies multi-source correlation as foundational. NIST Special Publication 800-86, § 3.3, at 3-6 (Aug. 2006) ("The foundation of forensics is using a methodical approach to reach appropriate conclusions based on the available data. . . . Often, this effort will include correlating data among multiple sources.").

[5] Bit-stream forensic imaging "generates a bit-for-bit copy of the original media, including free space and slack space." NIST Special Publication 800-86, § 4.2.1, at 4-6 (Aug. 2006). The FBI has accordingly possessed all the artifact data necessary to perform this analysis for the duration of this litigation. *Cf. id.* § 4.1.3, at 4-4 to 4-5 (identifying deleted files, slack space, free space, and Alternate Data Streams as recoverable categories of data within an existing forensic image).

of existing records the FBI has had in its possession for years. And regardless of what FOIA requires, Wickman had a duty to answer the Court's question.

Notably, Plaintiff never asked the FBI to extract files, create new records, or repair "corrupted" files. Plaintiff sought (and seeks) the laptop data in its native format. Plaintiff's experts are quite capable of extracting files and repairing them on their own without any help from the FBI. The FBI ostensibly wants to extract and repair the files so it can first review them before producing them, but that's a separate issue. If the nation's "premier law enforcement agency" lacks the competence to perform basic forensic tasks, then that's all the more reason why a special master should be appointed to extract and review the data.

F. Wickman's discussion of "alternative transfer methods" is incomplete.

Wickman speculates that files might have been transferred via command-line copying, third-party tools, ZIP files, encrypted containers, direct disk access, or imaging tools — each of which, he suggests, could leave "little to no forensic footprint." Wickman Decl. ¶ 11. As Mr. Apelbaum explains, that speculation is incomplete:

> Those methods may complicate analysis, but they commonly create their own artifacts unless anti-forensic steps were taken. Examples may include program execution artifacts, Prefetch, AmCache, ShimCache, command history, PowerShell artifacts where available, application installation or execution traces, archive creation metadata, and file-system timeline artifacts. Wickman does not state whether the FBI examined the Work Laptop for evidence of such tools or methods.

2026 Apelbaum Decl. ¶ 11. The relevant question — whether such tools were ever installed or used on the work laptop — is one the FBI is uniquely positioned to answer through forensic examination. [6] The Wickman Declaration is silent on whether the FBI performed that

[6]The peer-reviewed literature has comprehensively cataloged the artifacts that persist even when sophisticated anti-forensic tools are used. *See* Bhupendra Singh & Upasna Singh, *Program Execution Analysis in Windows: A Study of Data Sources, Their Format and Comparison of Forensic Capability*, 74 Computers & Security 94 (2018) (identifying eleven distinct sources of program-execution evidence — Prefetch, Jump Lists, Shortcut/LNK, UserAssist, Amcache.hve, IconCache.db, AppCompatFlags,

examination, much less what it found. Plaintiff would very much like to know whether any such tools or artifacts were found, and the FBI offers no explanation why such records would be exempted by FOIA (or exempted from the Court's order). The Wickman Declaration, however, offers nothing more than bald speculation about something that *might* have happened. It appears, in context, that Wickman is offering a speculative rationalization for why the FBI should not have to search for – or produce – the actual tools or artifacts.

G. The forensic question is critical to the central factual dispute.

This matters because the central factual question in this litigation — whether DNC emails were downloaded from Seth Rich's laptop to an external storage device — turns precisely on the type of forensic analysis the Wickman Declaration does not say was performed. *See* Apelbaum Decl. (May 9, 2025, Dkt. #198-1) ¶ 5 (citing prior expert testimony of William Binney and Peter Clay that the DNC emails appeared to have been downloaded to a thumb drive rather than "hacked" remotely); 2026 Apelbaum Decl. ¶ 20. The FBI cannot avoid its FOIA and Court-ordered obligations by recharacterizing the inquiry to make it appear futile.

VI. The FBI's newly-invoked exemptions are improper post-hoc rationalizations.

The Lara Declaration invokes two new FOIA exemptions — Exemption 3 (pursuant to the Cybersecurity Information Sharing Act, or "CISA") and Exemption 4 (trade secrets and confidential commercial information) — that were nowhere asserted in the original *Vaughn* indexes or in any prior filing. Lara Decl. ¶¶ 18-21. This Court ordered the FBI to conduct a

AppCompatCache, RunMRU, MuiCache, and SRUDB.dat — and evaluating the scrubbing capabilities of five popular anti-forensic tools); Bhupendra Singh & Upasna Singh, *Leveraging the Windows Amcache.hve File in Forensic Investigations*, 11 J. Digital Forensics, Security & Law, art. 7, at 7-9 (2016) (Amcache.hve artifacts "persist even after the applications have been deleted from the system"). NIST confirms that "[m]any collection tools can recognize some or all of these methods of hiding data and recover the associated data." NIST Special Publication 800-86, § 4.2.4, at 4-9 to 4-10 (Aug. 2006).

document-by-document review and produce *Vaughn* indexes in August 2024. The FBI produced its indexes in March 2025. It is now May 2026 — fourteen months later — and the FBI is identifying for the first time exemptions it claims apply to the documents it reviewed more than a year ago. The Court should deem those exemptions waived insofar as they were not timely asserted. *See Maydak v. U.S. Dep't of Justice*, 218 F.3d 760, 764 (D.C. Cir. 2000) (Government "must assert all exemptions at the same time").

The new exemptions are also substantively defective. CISA-based Exemption 3 protects "cyber threat indicators" and "defensive measures" that have been shared with the federal government under the Act. 6 U.S.C. §§ 1501, 1504. The Lara Declaration provides no specifics suggesting that the contents of the DNC-imaged work laptop qualify as CISA-protected material. To the contrary, the Lara Declaration describes the contents as including "documents relating to campaign strategy and voter-demographic information" (Notice of Compliance n.3) — categories that have nothing to do with cyber threat indicators or defensive measures. Accordingly, the government failed to meet its burden with respect to Exemption 3.

The Exemption 4 claim is similarly conclusory. Exemption 4 protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." 5 U.S.C. § 552(b)(4). The information must be both "customarily and actually treated as private by its owner" and "provided to the government under an assurance of privacy." *Food Mktg. Inst. v. Argus Leader Media*, 588 U.S. 427, 440 (2019). The Lara Declaration provides no evidence that the contents of the work laptop meet either prong, beyond a conclusory assertion that the DNC "objects to the release" of the contents. Lara Decl. ¶ 14(B). An objection to release is not equivalent to a contemporaneous assurance of confidentiality at the time of provision, thus the government failed to meet its burden.

The Exemption 7(D) claim suffers from the same defect. Exemption 7(D) protects confidential sources who provide information to law enforcement under express or implied assurances of confidentiality. *U.S. Dep't of Justice v. Landano*, 508 U.S. 165, 174 (1993). The Supreme Court has held that confidentiality is not presumed and must be established with specific evidence regarding the source's relationship to the agency. *Id.* The DNC was not a typical confidential informant. The DNC was the alleged victim of a high-profile cyber intrusion and provided the work laptop (or an image of it) in connection with the resulting criminal investigation. The Lara Declaration provides no evidence of any express assurance of confidentiality. Nor are the circumstances sufficient to support an implied assurance under *Landano*: the DNC's provision of the laptop was a matter of significant public discussion at the time, was the subject of contemporaneous press reporting, and was central to a federal criminal indictment. *See United States v. Netyksho*, No. 1:18-cr-00215 (D.D.C.). There is no plausible argument that the DNC reasonably expected its laptop's contents to remain forever sealed from public scrutiny.

VII. The FBI's treatment of "corrupted" files is inadequate.

This Court's March 24, 2026 Order required the FBI to address "what measures, if any, the FBI took to 'open,' view, or otherwise restore any allegedly corrupted or unreadable files." Dkt. #214 at 20. The Spence Declaration's response is that files on the personal laptop were opened in their native applications using a tool called Magnet Forensics, and if an error message appeared the file was marked "File corrupted/would not open." Spence Decl. ¶ 9. The Wickman Declaration adds that any effort to repair such files would amount to creating new records not contemplated by FOIA. Wickman Decl. ¶ 12. As Mr. Apelbaum explains, neither response is adequate:

> The Spence declaration, addressing the Personal Laptop, states that files were opened in native format through a review tool called Magnet Forensics and that some generated error messages, generated no content, or failed to load. That does not establish that recovery was impossible. It only establishes that some files did not open through that workflow. The Lara declaration, addressing the Work Laptop, states generally that RIDS personnel used "other software," but it does not identify the software, file types, errors encountered, recovery tools used, or results.

2026 Apelbaum Decl. ¶ 16. The FBI's methodology amounts to: try to open the file once in its native application; if that fails, mark it corrupted and exclude it from review. Industry-standard forensic recovery tools — including The Sleuth Kit, EnCase, FTK, X-Ways Forensics, R-Studio, and various hex editors — are routinely used to recover and analyze partially corrupted files. *See* Apelbaum Decl. (May 9, 2025, Dkt. #198-1) ¶ 3. A file that fails to open in Microsoft Word may open without difficulty in LibreOffice, in a hex editor, or after passing through a recovery tool. *Id*.

Moreover, even accepting that some files are genuinely beyond recovery, the FBI had at minimum two options. First, it could have produced the corrupted files in their original, uncorrected format and let the requester or its experts attempt recovery. *See* 5 U.S.C. § 552(a)(3)(B) ("an agency shall provide the record in any form or format requested by the person if the record is readily reproducible by the agency in that form or format"). Second, it could have used industry-standard recovery tools that would not have required the creation of new records (only the restoration of existing records). The FBI did neither, then pretended it could do nothing more.

VIII. The FBI has failed to release segregable portions of the records.

FOIA requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt." 5 U.S.C. § 552(b). "[A]n agency must release any segregable portions of a record that is otherwise exempt,

typically by proceeding 'line-by-line.'" *Ctr. for Immigr. Stud. v. U.S. Citizenship & Immigr. Servs.*, No. 1:22-CV-02107 (TNM), 2025 WL 405115, at *2 (D.D.C. Feb. 5, 2025), *quoting Porup v. CIA*, 997 F.3d 1224, 1239 (D.C. Cir. 2021).

The FBI has not conducted any segregability analysis at the document level. It has withheld in full every record on both laptops, redacted every filename, and provided no explanation of what (if any) non-exempt material exists within the records or what efforts (if any) were made to identify segregable portions. The Spence Declaration's sweeping claim that "the production of any data of any kind" would interfere with the investigation cannot substitute for the document-by-document segregability analysis FOIA requires. *See Mead Data Cent.*, 566 F.2d at 261 ("unless the segregability provision of the FOIA is to be nothing more than a precatory precept, agencies must be required to provide the reasons behind their conclusions in order that they may be challenged").

The filename redactions are particularly indefensible. The FBI has provided generic content descriptions in the *Vaughn* index (e.g., "Rental Application") while redacting the actual filenames. The filename of a 2013 rental application has no plausible nexus to a 2016 homicide or hacking investigation. Yet the FBI has produced no segregability analysis for filenames or any other metadata.

Relief Requested

For the foregoing reasons, the Plaintiff respectfully moves the Court to enter summary judgment in his favor and order the FBI to produce all data and metadata from Seth Rich's electronic devices in its native format within 30 days. In the alternative, Plaintiff moves the Court to appoint a special master at the government's expense and empower that special master to retain such experts as are needed to extract the records and review them for exemption analysis and production. Any lesser form of relief will ensure another six-years' worth of delays and trickery from the FBI.

Respectfully submitted,

/s/ Ty Clevenger
Ty Clevenger
Texas Bar No. 24034380
212 S. Oxford Street #7D
Brooklyn, New York 11217
(979) 985-5289
(979) 530-9523 (fax)
tyclevenger@yahoo.com

Counsel for Plaintiff

Certificate of Service

On June 15, 2026, I filed a copy of this request with the Court's ECF system, which should result in automatic notification via email to Asst. U.S. Attorney James Gillingham, Counsel for the Defendants, at james.gillingham@usdoj.gov.

/s/ Ty Clevenger
Ty Clevenger