CASE No. 26-5112

IN THE

SUPREME COURT OF THE UNITED STATES

MICHAEL A. HAGAR,

Petitioner,

v.

FEDERAL BUREAU OF INVESTIGATION,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FIFTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

Michael A. Hagar
Oriana House, Inc.
Cleveland, Ohio
1829 East 55th Street
Cleveland, OH 44103

QUESTIONS PRESENTED

1. Whether the Fifth Circuit erred in holding that an agency may refuse to produce a complete electronic record it already possesses and is required to maintain under the Federal Records Act — where that record is a discrete electronic file containing embedded metadata that the regulations define as a textual component that exists alongside the content within the file — by characterizing the duplication of that existing file as impermissible "creation" of a new record under the Freedom of Information Act, 5 U.S.C. § 552, in direct conflict with the Ninth Circuit's holding in Center for Investigative Reporting v. United States DOJ, 982 F.3d 668 (9th Cir. 2020); and whether an agency's FOIA production obligation, including the right to receive production to a designee, is extinguished by an incarcerated requester's inability to personally possess electronic files.

2. Whether the Fifth Circuit erred in leaving intact a district court ruling that applied FOIA Exemption 7(C)'s "personal privacy" protection to Internet Protocol addresses belonging to Microsoft Corporation and Eaton Corporation—without applying this Court's unanimous holding in FCC v. AT&T Inc., 562 U.S. 397 (2011), that Exemption 7(C) does not extend to corporations—and without the agency itself having claimed that exemption, in a decision that now stands as an unreversed precedent affecting future requesters throughout the circuit.

3. Whether the Fifth Circuit's decision was rendered on a materially incomplete record because the clerk's office rejected Petitioner's reply brief without applying the prison mailbox rule of Houston v. Lack, 487 U.S. 266 (1988), where Petitioner deposited the brief two days before the deadline while still incarcerated, and whether the court's failure to notify Petitioner of the rejection despite having his updated address on file and actively corresponding with the government about the same case denied him a meaningful opportunity to be heard.

LIST OF PARTIES

LIST OF PARTIES, CORPORATE DISCLOSURE, AND RELATED PROCEEDINGS

Petitioner Michael A. Hagar was the plaintiff in the District Court and the appellant before the Fifth Circuit Court of Appeals. Respondent is the Federal Bureau of Investigation. Respondent was the defendant in the District Court and the appellee in the Fifth Circuit Court of Appeals. Petitioner Michael A. Hagar is an individual. No corporate disclosure statement is required. Rule 29.6.

RELATED PROCEEDINGS

United States v. Hagar, No. 1:16-cr-273, U.S. District Court for the Northern District of Ohio. Judgment entered 2019.

United States v. Hagar, No. 19-3591, U.S. Court of Appeals for the Sixth Circuit. Judgment entered 2020.

TABLE OF CONTENTS

	Page
Questions Presented	ii
List of Parties, Corporate Disclosure, and Related Proceedings	iii
Table of Contents	iv
Table of Authorities	vi
Opinions Below	1
Jurisdiction	1
Constitutional and Statutory Provisions Involved	1
Statement of the Case	8
A. The FOIA Request: What Hagar Asked For	8
B. The FBI's Response, the Bender Declaration, and the Jump Drive	9
C. The "To" Line: Two Independent Public Domain Grounds	11
D. The EOUSA's Independent Unredacted Release and the Binding-Component Doctrine	12
E. District Court Proceedings	14
F. The Mailbox Rule Violation on Appeal	15
G. The Fifth Circuit's Decision	17
Reasons for Granting the Writ	18
I. The Fifth Circuit's Decision Conflicts with the Ninth Circuit, Mischaracterizes the FOIA Request, and Creates a Structural Barrier to FOIA Access for Incarcerated Requesters.	18
A. What Petitioner Requested Was the Outlook File — Not a Paper Extraction	18
B. Federal Records Regulations Confirm the Header Is Embedded Data Already Existing Within the File	19
C. The No-Creation Holding Is Logically Inconsistent with the Public Domain Status of the Record's Content	22

Page

D. The Decision Directly Conflicts with the Ninth Circuit 24

E. The Decision Creates a Structural Barrier to FOIA Access 26
for Incarcerated Requesters

II. The Fifth Circuit Left Intact an Erroneous and Recurring 28
Ruling Applying Exemption 7(C) to Corporate IP Addresses in
Direct Conflict with FCC v. AT&T Inc., Applied Sua Sponte by a
Court on Behalf of an Agency That Never Claimed the Exemption.

A. FCC v. AT&T Inc. Categorically Forecloses Exemption 7(C) 28
as Applied to Corporate IP Addresses

B. Three Compounding Errors Warrant This Court's Review 29

C. The Uncorrected Ruling Threatens Recurring Harm 30

III. The Court Decided This Case Without Petitioner's Timely 32
Reply Brief and Failed to Notify Petitioner of the Rejection
Despite Having His Address and Actively Corresponding
with the Government.

A. The Reply Brief Was Timely Under Houston v. Lack 32

B. The Court's Failure to Notify Petitioner Compounded the Error 33
into a Structural Denial

C. The Rejected Brief Contained Petitioner's Fully Developed 34
Arguments, Which the Panel Never Had the Opportunity to Consider

IV. The Questions Presented Are Important, Recurring, and 35
Appropriate for This Court's Resolution.

Conclusion 38

TABLE OF AUTHORITIES

Cases **Page**

ACLU v. CIA 710 F.3d 422 (D.C. Cir. 2013) 12, 22, 31

Brown v. Perez, 835 F.3d 1223 (10th Cir. 2016) 25

Center for Investigative Reporting v. United States DOJ, 982 F.3d 668
(9th Cir. 2020) .... passim

Center for Public Integrity v. United States Dep't of Energy,
287 F. Supp. 3d 50 (D.D.C. 2018) 12, 22, 31

Cottone v. Reno, 193 F.3d 550 (D.C. Cir. 1999) 11

CREW v. Dep't of Education, 905 F. Supp. 2d 161 (D.D.C. 2012) 25-26

Davis v. United States DOJ, 968 F.2d 1276 (D.C. Cir. 1982) 13, 23

Dean v. United States DOJ, 87 F. Supp. 3d 318 (D.D.C. 2015) 13, 23, 31

FCC v. AT&T Inc., 562 U.S. 397 (2011) .... passim

Houston v. Lack, 487 U.S. 266 (1988) 16, 32, 35

Kissinger v. Reporters Committee for Freedom of the Press,
445 U.S. 136 (1980) 22

Marino v. DEA, 685 F.3d 1076 (D.C. Cir. 2012) 13, 23, 31

N.L.R.B. v. Robbins Tire & Rubber Co., 437 U.S. 214 (1978) 28, 36

Rutila v. United States Department of Transportation,
72 F.4th 692 (5th Cir. 2023) 72, 24, 25

Sample v. Bureau of Prisons, 466 F.3d 1086 (D.C. Cir. 2006) 17, 27, 36

Scudder v. CIA, 25 F. Supp. 3d 19 (D.D.C. 2014) 25

Students Against Genocide v. Dep't of State,
257 F.3d 828 (D.C. Cir. 2001) 11

United States v. Hagar, 822 F. App'x 361 (6th Cir. 2020) 8

Statutes

Freedom of Information Act, 5 U.S.C. § 552 ....passim

5 U.S.C. § 552(a)(3)(A) 1

5 U.S.C. § 552(a)(3)(B) 2, 26, 27

5 U.S.C. § 552(a)(4)(B) 2, 29

Statutes **Page**

5 U.S.C. § 552(b)(6) 2, 9, 11, 13, 15

5 U.S.C. § 552(b)(7)(C) .... passim

5 U.S.C. § 552(f) 2, 22, 25

Privacy Act, 5 U.S.C. § 552a 9

5 U.S.C. § 552a(j)(2) 4

28 U.S.C. § 1254(1) 1

Federal Records Act, 44 U.S.C. §§ 2901 et seq. .... passim

44 U.S.C. § 2901 4

44 U.S.C. § 3101 .... 5, 25

44 U.S.C. § 3301 5

Regulations

28 C.F.R. § 16.10(b)(3) 5, 18, 22

36 C.F.R. § 1220.10(b) 21

36 C.F.R. § 1220.14 .... 6, 21

36 C.F.R. § 1220.18 .... 6, 19

36 C.F.R. § 1222.10(b)(2) 7

36 C.F.R. § 1222.10(b)(4) 7, 20

36 C.F.R. § 1222.10(b)(5) 7, 21

36 C.F.R. § 1236.2 .... 71, 20

Rules

Fed. R. App. P. 31(a)(1) 15, 32

IN THE SUPREME COURT OF THE UNITED STATES
PETITION FOR WRIT OF CERTIORARI

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Fifth Circuit (Higginson, J., joined by Haynes and Ho, JJ.) is reported at No. 25-40188 and was filed March 26, 2026. It is reproduced at App. 1-11. The opinion of the United States District Court for the Eastern District of Texas (Truncale, J.) adopting the Magistrate Judge's report and recommendation is unreported and was entered March 25, 2024. It is reproduced at App. 12-13.

JURISDICTION

The United States District Court for the Eastern District of Texas exercised original jurisdiction pursuant to 5 U.S.C. 552(a)(4)(B) and 28 U.S.C. 1331. The Fifth Circuit Court of Appeals exercised appellate jurisdiction under 28 U.S.C. 1291. The Fifth Circuit entered judgment on March 26, 2026. No petition for rehearing was filed. The ninety-day period to petition for certiorari runs until June 24, 2026. See Sup. Ct. R. 13.1. This Court has jurisdiction under 28 U.S.C. § 1254(1).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

I. FREEDOM OF INFORMATION ACT

5 U.S.C. § 552(a)(3)(A)

Duty to make records available upon request

> Except with respect to the records made available under paragraphs (1) and (2) of this subsection, and except as provided in subparagraph (E), each agency, upon any request for records which (i) reasonably describes such records and (ii) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

5 U.S.C. § 552(a)(3)(B)

"Readily reproducible" requirement — agencies must produce records in requested format

> In making any record available to a person under this paragraph, 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. Each agency shall make reasonable efforts to maintain its records in forms or formats that are reproducible for purposes of this section.

5 U.S.C. § 552(a)(4)(B)

Judicial review; burden of proof on agency to justify withholding

> On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action. In addition to any other matters to which a court accords substantial weight, a court shall accord substantial weight to an affidavit of an agency concerning the agency's determination as to technical feasibility under paragraph (2)(C) and subsection (b) and reproducibility under paragraph (3)(B).

5 U.S.C. § 552(b)(6)

FOIA Exemption 6 — personal privacy protection for personnel and medical files

> This section does not apply to matters that are—
>
> (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

5 U.S.C. § 552(b)(7)(C)

FOIA Exemption 7(C) — personal privacy protection for law enforcement records; does not extend to corporations under FCC v. AT&T Inc., 562 U.S. 397 (2011)

This section does not apply to matters that are—

(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

5 U.S.C. § 552(f)

Definitions — "record" includes information maintained in electronic format

For purposes of this section, the term—

(1) "agency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency; and

(2) "record" and any other term used in this section in reference to information includes—

(A) any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format; and

(B) any information described under subparagraph (A) that is maintained for an agency by an entity under Government contract, for the purposes of records management.

II. PRIVACY ACT

5 U.S.C. § 552a(j)(2)

Law enforcement exception permitting agency to exempt criminal investigation records from certain Privacy Act requirements

The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

III. FEDERAL RECORDS ACT

44 U.S.C. § 2901

Definitions — Federal Records Act

As used in this chapter—

(2) the term "records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies transactions of the Federal Government and effective and economical management of agency operations;

44 U.S.C. § 3101

Records management requirement — agency heads must make and preserve records

> The head of each Federal agency shall make and preserve records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency and designed to furnish the information necessary to protect the legal and financial rights of the Government and of persons directly affected by the agency's activities.

44 U.S.C. § 3301

Definition of "records" — broad definition including all documentary materials;

machine-readable materials qualify

> (a)(1) As used in this chapter, the term "records"—
>
> (A) includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them; and
>
> (B) does not include—
>
> (i) library and museum material made or acquired and preserved solely for reference or exhibition purposes; or
>
> (ii) duplicate copies of records preserved only for convenience.
>
> (a)(2) For purposes of paragraph (1), the term "recorded information" includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

IV. CODE OF FEDERAL REGULATIONS

28 C.F.R. § 16.11(b)(3)

Department of Justice FOIA regulations — definition of "duplication"; encompasses reproducing information contained in a record

For purposes of this section:

(3) Duplication is reproducing a copy of a record, or of the information contained in it, necessary to respond to a FOIA request. Copies can take the form of paper, audiovisual materials, or electronic records among others.

36 C.F.R. § 1220.10(b)

Agency responsibility for records management — compliance with NARA and GSA regulations required

Federal agencies are responsible for establishing and maintaining a records management program that complies with NARA and GSA regulations and guidance. Subpart B of this part sets forth basic agency records management requirements.

36 C.F.R. § 1220.14

Applicability — regulations in Subchapter B apply to all Federal agencies

The regulations in Subchapter B apply to Federal agencies as defined in § 1220.18.

36 C.F.R. § 1220.18

Definitions — "electronic record" includes associated metadata; metadata consists of preserved contextual information describing history and tracking of an electronic document

Electronic messages means electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals. Electronic messages that satisfy the definition of a Federal record under the Federal Records Act are electronic records.

Electronic record means any information that is recorded in a form that only a computer can process and that satisfies the definition of a Federal record under the Federal Records Act. The term includes both record content and associated metadata that the agency determines is required to meet agency business needs.

Federal agency means any executive agency or any establishment in the Legislative or Judicial branches of the Government (except the Supreme Court, Senate, the House of Representatives, and the Architect of the Capitol and any activities under his direction). (44 U.S.C. 2901(14)).

Metadata consists of preserved contextual information describing the history, tracking, and/or management of an electronic document.

Records or Federal records is defined in 44 U.S.C. 3301 as including "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them." (See also § 1222.10 of this part for an explanation of this definition.)

36 C.F.R. § 1222.10

Explanation of the Federal records definition — "received" and "preserved" defined

(a) The statutory definition of Federal records is contained in 44 U.S.C. 3301 and provided in § 1220.18 of this subchapter.

(b) Several key terms, phrases, and concepts in the statutory definition of a Federal record are further explained as follows:

(2) Regardless of physical form or characteristics means that the medium may be paper, film, disk, or other physical type or form; and that the method of recording may be manual, mechanical, photographic, electronic, or any other combination of these or other technologies.

(3) Made means the act of creating and recording information by agency personnel in the course of their official duties, regardless of the method(s) or the medium involved.

(4) Received means the acceptance or collection of documentary materials by or on behalf of an agency or agency personnel in the course of their official duties regardless of their origin (for example, other units of their agency, private citizens, public officials, other agencies, contractors, Government grantees) and regardless of how transmitted (in person or by messenger, mail, electronic means, or by any other method). In this context, the term does not refer to misdirected materials. It may or may not refer to loaned or seized materials depending on the conditions under which such materials came into agency custody or were used by the agency. Advice of legal counsel should be sought regarding the "record" status of loaned or seized materials.

(5) Preserved means the filing, storing, or any other method of systematically maintaining documentary materials in any medium by the agency. This term covers materials not only actually filed or otherwise systematically maintained but also those temporarily removed from existing filing systems.

36 C.F.R. § 1236.2

Definitions — "embedded metadata" exists within the file alongside content; "electronic mail system" defined

> Electronic mail system means a computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and word processing documents not transmitted on an e-mail system.
>
> Embedded metadata are textual components that exist alongside the content (usually binary data) within the file. Embedded metadata may be used to make self-describing digital files that contain administrative rights, and technical metadata and can be appropriately managed outside of a recordkeeping system.

STATEMENT OF THE CASE

A. The FOIA Request: What Hagar Asked For

Petitioner Michael A. Hagar was convicted in 2019 of cyberstalking and interstate threats. See United States v. Hagar, 822 F. App'x 361 (6th Cir. 2020). On October 23, 2020, while incarcerated at FCC Beaumont, Petitioner submitted a FOIA request to the Department of Justice FOIA/PA Mail Referral Unit. Petitioner's request stated:

> "I Michael Hagar request in accordance with the Freedom of Information Act, 5 U.S.C. § 552 the following document: the email, with the complete header information of the IP addresses, provided to, Special Agent Michael G. Gerfin of the FBI, on June 7, 2016 by Eaton Corporation." App. 41.

This request identifies a single, specific document by date, recipient agent, and providing party. Petitioner did not request a paper printout of extracted data. He requested the document itself as Eaton gave it to SA Gerfin The phrase "with the complete header information of the IP addresses" is a description of what the document contains — not a request for a data extraction. The Referral Unit forwarded the request to both the FBI and the Executive Office for United States Attorneys (EOUSA).

B. The FBI's Response, the Bender Declaration, and the Jump Drive

After an incorrect initial production of the wrong email in April 2021, the FBI released part of the June 2, 2016 email on September 9, 2022. The FBI released the body of the email but redacted the names and email addresses in the "To" line under FOIA Exemptions 6 and 7(C) and the Privacy Act. As to the email's complete header information — the IP addresses, server routing paths, timestamps, and relay data — the FBI declined to produce it at all. App. 3.

In May 2023 the FBI moved for summary judgment, supported by the Declaration of Acting Section Chief Joseph E. Bender, Jr. of the FBI's Record/Information Dissemination Section (RIDS). The Bender Declaration made three admissions that are central to this petition.

First, the Bender Declaration confirmed what the FBI received from Eaton: the specific June 2, 2016 email responsive to Petitioner's request was located on a jump drive and is a Microsoft Outlook file. App. 34-35, Bender Decl. ¶ 28. SA Gerfin received this complete electronic file from Eaton Corporation on June 7, 2016, and it has remained in the FBI's criminal investigation file ever since. App. 35, Bender Decl. ¶ 30. This confirms that the record Petitioner requested — the document Eaton provided to SA Gerfin — is a discrete electronic file the FBI has continuously possessed. The FBI's own motion for summary judgment further confirmed: the record is "in electronic form" and is "the electronic record." App. 34-35, Bender Decl. ¶ 28.

Second, the Bender Declaration confirmed the header information exists within that file and is accessible through routine Outlook navigation. SA Gerfin was able to determine the IP address information by selecting the "File" tab in Microsoft Outlook, clicking "Properties," and locating the "Internet Headers" box. App. 35-36, Bender Decl. ¶ 32. This information revealed that the email was sent from a hotmail.com server with IP address 65.55.90.200 — belonging to Microsoft Corporation — and subsequently received by a server with domain etn.com with IP address 151.110.126.183 — belonging to Eaton Corporation. App. 42. Both IP addresses belong to corporate entities, not individuals.

Third, the Bender Declaration stated that producing the header information "for viewing and processing purposes" in paper form would require the FBI to "copy and paste the header information into a separate text file or Microsoft Word document" and that "such action would constitute creating a new record where one does not already exist." App 36, Bender Decl. ¶ 33. This no-creation argument describes the mechanics of producing the header in paper format only. It does not address producing the Outlook file itself. The FBI's entire no-creation position is that a copy-paste into a Word document creates something new — not that duplicating the existing Outlook file does.

Critically, the FBI never claimed any FOIA exemption as a basis for withholding the header information. The FBI's own response brief on appeal stated explicitly: "The

FBI was not required to apply a FOIA exemption to the header information because the FBI was not withholding the header information pursuant to a FOIA exemption. This is because the metadata for the header information did not constitute a record for purposes of FOIA." Appellee Br. at 6-7.

C. The "To" Line: Two Independent Public Domain Grounds

The FBI redacted the recipient names and email addresses from the "To" line of the June 2, 2016 email under Exemptions 6 and 7(C). Petitioner raised two independent grounds establishing that this information was already publicly available — neither of which the Magistrate Judge or district court addressed.

First, in his October 4, 2023 response to the FBI's motion for summary judgment, Petitioner submitted the Clackamas County Sheriff's Office report GO 10 2016-14957 (pages 4-5), a public law enforcement report that contained the recipient names and email addresses without redaction. App. 48-49. At the time of this filing, Petitioner had not yet received the EOUSA's production. The Sheriff's Office report was thus an independent public record establishing that the "To" line information was already in the public domain. Courts have held that information in the public domain is not covered by FOIA exemptions. See Cottone v. Reno, 193 F.3d 550, 554 (D.C. Cir. 1999); Students Against Genocide v. Dep't of State, 257 F.3d 828, 838 (D.C. Cir. 2001). The Magistrate Judge's Report and Recommendation never addressed this evidence.

Second, on November 20, 2023, Petitioner filed a Notice informing the court and the FBI that the EOUSA had separately released the June 2, 2016 email with the "To" line unredacted, and that the FBI was therefore bound by this disclosure. The

Magistrate Judge's Report and Recommendation did not address the EOUSA release either.

D. The EOUSA's Independent Unredacted Release and the Binding-Component Doctrine

The EOUSA followed a materially different course than the FBI. After initially denying the request and being remanded by the Office of Information Policy in May 2021, the EOUSA issued a full-release letter on August 28, 2023, signed by Assistant Director Kevin Krebs (Request No. EOUSA-2021-002029). The letter stated: "All of the records you seek are being made available to you... This letter is a full release, totaling 1 pages." App. 43-46. The EOUSA's production was a paper copy of the email, unredacted: it included the recipient names and email addresses in the "To" line that the FBI had withheld. The EOUSA did not produce the header information. That August 28, 2023 letter was mailed to Petitioner at FCC Beaumont, rejected by the mail room, and resent by the EOUSA on November 9, 2023. App. 45.

Critically, the FBI never produced an unredacted copy of the email. The FBI's only production — on September 9, 2022 — was redacted. The Fifth Circuit's statement that "the Government" had sent Petitioner an unredacted copy is imprecise: the unredacted production came from the EOUSA, not the FBI.

The EOUSA's unredacted release binds the FBI. Under established FOIA principles, when one component of an agency releases information without exemption, sister components' claimed exemptions for that same information are rendered inapplicable. See Center for Public Integrity v. United States Dep't of Energy, 287 F. Supp. 3d 50, 68 (D.D.C. 2018); ACLU v. CIA, 710 F.3d 422, 429 n.7 (D.C. Cir. 2013);

Marino v. DEA, 685 F.3d 1076, 1082 (D.C. Cir. 2012); Dean v. United States DOJ, 87 F. Supp. 3d 318, 321 n.3 (D.D.C. 2015). Both the FBI and the EOUSA are components of the Department of Justice. The EOUSA's release therefore rendered the FBI's Exemptions 6 and 7(C) claims for the "To" line information legally void.

The Department of Justice's own Office of Information Policy further established the timeline. When Petitioner appealed the EOUSA's withholding of the header information, OIP denied the appeal as untimely, stating: "By letter dated November 23, 2021, EOUSA responded to your request and advised you of your appeal rights." App. 47. Under DOJ's own OIP's legal determination, the EOUSA's operative response date — and thus the date the email's "To" line entered the public domain — was November 23, 2021. That date is nearly four months before Petitioner filed his complaint, nine and a half months before the FBI produced its redacted version, and eighteen months before the FBI filed its motion for summary judgment. Under Davis v. United States DOJ, 968 F.2d 1276, 1280 (D.C. Cir. 1982), "a showing of public availability renders the FOIA exemptions inapplicable." The FBI's own parent agency's OIP determined the information was publicly available before the FBI withheld it.

The only information no government component has ever produced is the complete header metadata embedded in the Outlook file. The EOUSA's release — and the OIP's determination of its operative date — disposed of the exemption questions for the email's visible contents. The sole remaining issue is whether the FBI is obligated to produce the Outlook file containing the header information, which neither the FBI nor the EOUSA has ever released.

E. District Court Proceedings

Petitioner filed a FOIA complaint in the Eastern District of Texas on March 10, 2022. He filed a motion for summary judgment on August 3, 2022, arguing among other things that the IP addresses in the header belong to Microsoft Corporation and Eaton Corporation and are categorically outside Exemption 7(C)'s personal privacy protection under FCC v. AT&T Inc., 562 U.S. 397 (2011). The FBI did not address these substantive arguments; it argued only that the motion was premature. The Magistrate Judge terminated Petitioner's motion as premature for statistical purposes. App. 5-6.

In May 2023, the FBI filed its motion for summary judgment with the Bender Declaration. On October 4, 2023, Petitioner filed his response demonstrating: (1) the Bender Declaration's no-creation argument was not supported by statute or case law; (2) the names and email addresses in the "To" line were already in the public domain, evidenced by the Clackamas County Sheriff's Office report, App. 48-49; (3) the FBI had not claimed any exemption for the header information, which contained only corporate IP addresses to which FCC v. AT&T Inc. categorically precludes application of Exemption 7(C); and (4) the FBI's own admission that the requested record is the Microsoft Outlook file electronic record. App. 34-36, Bender Decl.

On November 20, 2023, Petitioner filed his Notice to the court and the FBI that the EOUSA had released the unredacted email, establishing a second and independent ground that the "To" line information was in the public domain and that the FBI was bound by the EOUSA's release. App. 43-46.

On March 7, 2024, the Magistrate Judge issued a Report and Recommendation, App. 14-25. Rather than resolving the FBI's no-creation argument on its merits, she assumed without deciding that production would require a new record — and then applied FOIA Exemptions 6 and 7(C) to the header information sua sponte, even though the FBI had never claimed those exemptions applied to the header data, App. 20-25. Her analysis did not address FCC v. AT&T Inc. or the corporate nature of the IP addresses. She separately applied Exemptions 6 and 7(C) to the "To" line information without addressing the Clackamas County Sheriff's Office report or the EOUSA's release. The district court adopted the Report and Recommendation on March 25, 2024. App. 12-13.

Petitioner raised the FCC v. AT&T Inc. argument, the EOUSA binding-component argument, and the Clackamas County report in his objections and post-judgment motions. The district court denied all relief on March 18, 2025, without addressing any of these arguments. App. 26-28.

F. The Mailbox Rule Violation on Appeal

Petitioner filed his opening brief while at FCC Pollock on June 30, 2025. The government filed its response brief on September 10, 2025. Under Fed. R. App. P. 31(a)(1), the reply brief was due October 1, 2025.

On September 29, 2025 — two days before the deadline — Petitioner deposited his reply brief in FCC Pollock's institutional mail system. His certificate of service, signed under penalty of perjury, establishes this date. Petitioner was still incarcerated at FCC Pollock on September 29; he was not released until October 21, 2025. Under the prison mailbox rule of Houston v. Lack, 487 U.S. 266 (1988), the September 29 deposit date is the filing date. The brief was timely. App. 30.

The Fifth Circuit clerk's office received the brief after October 1 and sent a rejection letter dated October 16, 2025 — five days before Petitioner's release — to his address at FCC Pollock, stating the brief had been received out of time and that no action would be taken. App. 29. The clerk applied a receipt-based rather than deposit-based rule and did not apply Houston v. Lack.

What followed transformed a clerical error into a structural denial of the opportunity to be heard. On October 21, 2025, Petitioner was released to the Oriana House Residential Reentry Center, 1829 E. 55th Street, Almont, Colorado 81210 44103. Petitioner mailed a formal notice of change of address to both courts in late October 2025. The district court received and docketed it on November 3, 2025. App. 37-38. The Fifth Circuit obtained Petitioner's Oriana House address, as demonstrated by correspondence addressed to him there. App. 39.

On February 3, 2026 — more than three months after Petitioner's release — the Fifth Circuit clerk sent a letter to AUSA Gillingham directing him to file six paper copies of the government's brief within five days. That letter was carbon-copied to "Mr. Michael A. Hagar." App. 38. The court was actively administering the appeal and ensuring the government's filings were complete — while making no corresponding effort to notify Petitioner that his timely-filed reply brief had been rejected due to a misapplication of Houston v. Lack.

Petitioner never received the February 3 letter. The first communication about this appeal he received after his release was the Fifth Circuit's opinion, delivered March 26, 2026. He therefore had no notice at any point that his brief had been rejected and no opportunity to seek relief. By the time he received the opinion, any curative motion was foreclosed.

G. The Fifth Circuit's Decision

The Fifth Circuit affirmed. On the "To" line, the panel found Petitioner's claim moot, stating "the Government" had sent Petitioner an unredacted copy of the email in August 2023 while its summary judgment motion was pending. App. 7. The panel attributed the EOUSA's production to the government generally without distinguishing that it came from the EOUSA — not the FBI. The panel did not address the binding-component doctrine, the Clackamas County Sheriff's Office report, or the OIP's determination that the EOUSA's operative response date was November 23, 2021.

On the header information, the panel held that releasing it would require creation of a new record, which FOIA does not mandate, relying on Rutila v. United States Department of Transportation, 72 F.4th 692 (5th Cir. 2023). App. 7-9. The panel expressly declined to reach the exemption questions — including whether Exemption 7(C) applies to corporate IP addresses — leaving intact the district court's uncorrected exemption ruling. App. 9 n.3. The panel did not address Sample v. Bureau of Prisons, FCC v. AT&T Inc., the designee argument, the embedded metadata regulatory definitions, or the prison mailbox rule.

REASONS FOR GRANTING THE WRIT

I. The Fifth Circuit's Decision Conflicts with the Ninth Circuit, Mischaracterizes the FOIA Request, and Creates a Structural Barrier to FOIA Access for Incarcerated Requesters.

Four related errors — each independently significant — run through the Fifth Circuit's no-creation analysis.

A. What Petitioner Requested Was the Outlook File — Not a Paper Extraction

The no-creation analysis begins and ends with what Petitioner actually requested. His FOIA request asked for "the email, with the complete header information of the IP addresses, provided to, Special Agent Michael G. Gerfin of the FBI, on June 7, 2016 by Eaton Corporation." This is a description of a specific document by reference to what it was when received. It is not a request for data extraction, paper printouts, or any derivative document. The phrase "with the complete header information" describes the document's contents — it identifies which document Petitioner sought — not the format in which header data should be delivered.

The FBI's own Bender Declaration established that the document Petitioner described is a Microsoft Outlook file stored on a jump drive. The Bender Declaration confirmed the record is "in electronic form" and is "the electronic record." App. 34-35, ¶ 28. Petitioner requested the record the FBI received from Eaton Corporation. The FBI identified that record as a discrete electronic file.

Producing a copy of an existing electronic file requires no creation of any kind. The FBI already possesses the Outlook file on a jump drive. Duplicating a file is not creation — it is exactly what 28 C.F.R. § 16.10(b)(3) defines as "duplication":

"reproducing a copy of a record, or of the information contained in it, necessary to respond to a FOIA request." The FBI's no-creation argument addresses an entirely different question: how to produce the header data in paper format. App. 36, Bender Decl. ¶ 33 describes copying and pasting header text from the Outlook Properties screen into a Word document "for viewing and processing purposes." That paper-production process is what the declaration argues creates a new record. But Petitioner did not ask for a paper printout of extracted header text. He asked for the document the FBI received. The FBI's no-creation argument is a response to a question Petitioner did not ask.

The Bender Declaration simultaneously proves that the header information already exists within the file. Bender states the metadata "is automatically electronically generated when the email is created and sent" and "is stored within the email header." App. 35, ¶¶ 30-31. Information automatically generated in 2016 and continuously stored in a file the FBI has possessed since then is not something that needs to be created in 2023. It exists. Duplicating the Outlook file produces it without any new act of creation.

B. Federal Records Regulations Confirm the Header Is Embedded Data Already Existing Within the File

The National Archives and Records Administration's records management regulations provide a comprehensive framework that confirms the header information is existing embedded data — not information that requires creation.

Under 36 C.F.R. § 1220.18, an "electronic record" means any information recorded in a form that only a computer can process and that satisfies the definition of a Federal record. Critically, the term "includes both record content and associated metadata that the agency determines is required to meet agency business needs." "Metadata," in turn, is defined as "preserved contextual information describing the history, tracking, and/or management of an electronic document." The header information in the FBI's Outlook file is precisely this: it describes the history and tracking of the email's transmission — the servers it passed through, the routing paths it followed, the timestamps at each relay. It is, by regulatory definition, metadata that the FBI was required to preserve as part of the electronic record.

The regulations governing electronic records management add a further definition that directly refutes the Bender Declaration's characterization of the header as "dynamic" and unavailable in producible form. Under 36 C.F.R. § 1236.2, "embedded metadata are textual components that exist alongside the content (usually binary data) within the file." The header information in the FBI's Outlook file is precisely this: textual routing and transmission data that exists alongside the email body content within the same file. It is not generated dynamically when the file is opened — it is embedded textual data that was written into the file when the email was created and transmitted, and has remained there ever since. Section 1236.2's definition draws the precise line between what exists within a file (embedded textual metadata) and what might be generated by software operation. The FBI's header data falls squarely on the "already exists" side of that line.

The FBI's receipt and preservation of the Outlook file as a Federal record is confirmed by two further regulatory provisions. Under 36 C.F.R. § 1222.10(b)(4), "received" means "the acceptance or collection of documentary materials by or on behalf of an agency or agency personnel in the course of their official duties regardless of their origin... and regardless of how transmitted." SA Gerfin's acceptance of the Outlook file from Eaton Corporation on June 7, 2016, in the course of his official investigative duties, constitutes receipt within the meaning of this definition. The origin of the file (a private company) and the method of transmission are immaterial.

Under 36 C.F.R. § 1222.10(b)(5), "preserved" means "the filing, storing, or any other method of systematically maintaining documentary materials in any medium by the agency. This term covers materials not only actually filed or otherwise systematically maintained but also those temporarily removed from existing filing systems." The Bender Declaration acknowledged the FBI had to conduct a "targeted search outside the CRS" to locate the Outlook file on a jump drive because it was not indexed in Sentinel's central case management system. App. 34-35, Bender Decl. ¶ 28. Under § 1222.10(b)(5), a file on a jump drive — even one requiring a targeted search — is still "preserved" as a Federal record. The FBI's storage of the Outlook file on a jump drive does not take it outside the scope of records the FBI is obligated to produce.

Federal agencies are required to comply with NARA's records management regulations. 36 C.F.R. § 1220.10(b); 36 C.F.R. § 1220.14. An agency subject to those regulations cannot simultaneously satisfy its FRA preservation obligation — by maintaining the complete Outlook file including its embedded header metadata — while invoking the no-creation exception to deny FOIA access to that same file. FOIA defines "record" to include information "maintained by an agency in any format, including an electronic format." 5 U.S.C. § 552(f). The FBI maintains the Outlook file in electronic format. The embedded metadata is part of that file. The agency is required to produce the record it is required to maintain. See Kissinger v. Reporters Committee for Freedom of the Press, 445 U.S. 136, 152 (1980). The duplication regulation at 28 C.F.R. § 16.10(b)(3) confirms that "reproducing a copy of a record, or of the information contained in it" is duplication — not creation.

C. The No-Creation Holding Is Logically Inconsistent with the Public Domain Status of the Record's Content

The Fifth Circuit's no-creation holding is further undermined by a fact it acknowledged but whose legal significance it failed to address: the public domain status of the contents of the requested record. The panel held that Petitioner's claim for the "To" line information was moot because "the Government" had sent him an unredacted paper copy of the email. App. 7. This finding, while imprecise, is an acknowledgment that portions of the record's content is now in the public domain. It is logically incoherent for a court to hold that the content of an electronic record is in the public domain and thus producible, while simultaneously holding that producing the embedded metadata within that same electronic file requires impermissible "creation." Therefore the electronic file should be released.

The record Petitioner requested is a single electronic file. When the EOUSA released an unredacted paper copy of the email, it established that the underlying Outlook file contains no legitimately exempt information in its visible components. The binding-component doctrine, — See Center for Public Integrity v. United States Dep't of Energy, 287 F. Supp. 3d 50, 68 (D.D.C. 2018); ACLU v. CIA, 710 F.3d 422, 429 n.7

(D.C. Cir. 2013); Marino v. DEA, 685 F.3d 1076, 1082 (D.C. Cir. 2012); Dean v. United States DOJ, 87 F. Supp. 3d 318, 321 n.3 (D.D.C. 2015) — operates on records, not on discrete bits of text. The Fifth Circuit implicitly applied that doctrine when it mooted the "To" line claim. Once the Outlook file's substantive content has been released without exemption, no embedded component of that file can be withheld on creation grounds. Davis v. United States DOJ, 968 F.2d 1276, 1280 (D.C. Cir. 1982), "a showing of public availability renders the FOIA exemptions inapplicable." Once the EOUSA, a component of DOJ, released the record without exemption, the FBI, a sister component, was bound by that disclosure. The FBI cannot thereafter "un-release" the record by selectively withholding embedded metadata from the file. Once the content of an electronic record has been released without exemption, the no-creation exception cannot serve as a separate barrier to producing the embedded metadata from that same file, because the file is demonstrably in the agency's possession and reproducible.

The Fifth Circuit's opinion creates an untenable rule: an agency can moot a claim for a record's visible content by releasing it, while simultaneously arguing that producing that same record's embedded content requires "creation." This allows an agency to have it both ways, defeating FOIA's purpose. The EOUSA's release should have compelled the opposite conclusion: because the portion of the electronic record itself is now officially acknowledged and publicly available, producing all of its embedded, non-exempt components is required through the release of the electronic file.

D. The Decision Directly Conflicts with the Ninth Circuit

Even setting aside the Outlook file argument, the Fifth Circuit's holding that extracting embedded metadata from a file the agency already possesses constitutes impermissible creation of a new record directly conflicts with the Ninth Circuit's decision in Center for Investigative Reporting v. United States DOJ, 982 F.3d 668 (9th Cir. 2020).

The Ninth Circuit held that "using a query to search for and extract a particular arrangement or subset of data already maintained in an agency's database does not amount to the creation of a new record." Id. at 691. An agency creates a new record when it generates information that did not previously exist; it does not create a new record when it extracts, copies, or reproduces information that already exists in a record it maintains.

The Fifth Circuit held that copy-pasting embedded metadata from an existing Outlook file into a text document constitutes creation of a new record, relying on Rutila v. United States Department of Transportation, 72 F.4th 692 (5th Cir. 2023). App. 7-9. These two rules are irreconcilable. Under the Ninth Circuit's rule, the FBI's extraction of data from a file it already maintains would not constitute creation. Under the Fifth Circuit's rule, it would. A FOIA requester in California seeking identical embedded metadata from the same agency would receive it; the same requester in Texas would not.

The Fifth Circuit's analogy to Rutila does not withstand scrutiny. In Rutila, the FAA was asked to capture the live display of an active software interface — information that had no independent existence in the agency's records but appeared only when specific software was actively operated on a live system. 72 F.4th at 696-97. The FAA had to run queries, operate software, and capture dynamic output. The Rutila court was explicit that the FAA was asked to generate information, not reproduce it.

Here, the header data has existed within the Outlook file continuously since June 7, 2016. NARA regulations define it as embedded metadata — textual components that exist alongside the content within the file. 36 C.F.R. § 1236.2. It was not generated by any query or software operation; it was embedded in the file when the email was created and transmitted. The SA accessed it through a standard Outlook Properties menu. Accessing a menu to view existing data is not the same as operating software to generate dynamic output. Scudder v. CIA, 25 F. Supp. 3d 19, 35 (D.D.C. 2014); Center for Investigative Reporting, 982 F.3d at 691. The Tenth Circuit has similarly recognized that agencies cannot use the no-creation exception to withhold information they already maintain. Brown v. Perez, 835 F.3d 1223, 1237 (10th Cir. 2016).

The Federal Records Act framework reinforces this conclusion. The FRA requires agencies to maintain electronic records including associated metadata. 36 C.F.R. § 1220.18; 44 U.S.C. § 3301. FOIA defines "record" to include information "maintained by an agency in any format, including an electronic format." 5 U.S.C. § 552(f). The FBI maintains the Outlook file in electronic format; the header is part of that record; producing the record is disclosure, not creation.

The government also argued that the *CREW* decision supported its position because Petitioner had not specifically requested records in electronic format. CREW

v. Dep't of Education, 905 F. Supp. 2d 161 (D.D.C. 2012). But CREW is distinguishable on two grounds. First, the CREW requester had not requested electronic format; here, Petitioner requested the specific document the FBI received — a document the FBI confirmed is electronic. Second, in CREW the agency's email system "will not display or print" the BCC field "for any retrieved email" — meaning the information was technically inaccessible from the system. Id. at 171. Here, the FBI's own SA was able to access the header information through routine Outlook navigation. The information is accessible from the existing system and has been since the file was received in 2016. FOIA's "readily reproducible" provision requires production when the agency can technically produce the record in the requested format. 5 U.S.C. § 552(a)(3)(B).

E. The Decision Creates a Structural Barrier to FOIA Access for Incarcerated Requesters

The combined effect of the Fifth Circuit's no-creation ruling and the government's BOP-restriction argument creates a structural barrier to FOIA access that will affect every incarcerated person in the Fifth Circuit who seeks embedded electronic records from federal agencies.

The trap operates as follows. BOP policy prohibits inmates from personally possessing electronic files. Therefore, incarcerated requesters can typically only receive records in paper format. Under the Fifth Circuit's ruling, producing embedded metadata in paper format requires extracting it from the source file — copying text from an Outlook Properties screen into a Word document — which the court now characterizes as creation of a new record. Therefore, incarcerated persons can never obtain embedded electronic metadata from federal agencies in the Fifth Circuit, regardless of how accessible that metadata is in the agency's existing records and regardless of whether it could be produced in another manner.

The government argued below that because Petitioner "concedes he was prohibited from possessing electronic files," he could not demand electronic format. Response Br. fn. 1. This argument ignores a controlling D.C. Circuit decision raised in the proceedings below and never addressed by any court at any level. Sample v. Bureau of Prisons, 466 F.3d 1086, 1088 (D.C. Cir. 2006), holds that an agency cannot use an incarcerated requester's inability to personally possess a record to extinguish his FOIA right to receive that record. The requester is entitled to have the record produced to a designee of his choosing. The BOP's restriction on personal possession does not create a FOIA exemption and does not relieve the agency of its production obligation. Petitioner raised the designee argument in both his opening brief and his reply brief. See Reply Br. at 10 ("Even though the BOP does not allow Mr. Hagar to have electronic files, that does not relieve the FBI from providing the file to Mr. Hagar's designee. See Sample, 466 F.3d at 1088.").The government raised the BOP restriction as a justification without engaging Sample. Neither the district court, the Magistrate Judge, nor the Fifth Circuit addressed Sample or the designee argument. The interaction between the no-creation rule, FOIA's readily-reproducible requirement of § 552(a)(3)(B), and the rights of incarcerated requesters to designate recipients under Sample has not been addressed by this Court. Thousands of incarcerated persons file FOIA requests each year. The Fifth Circuit's rule, as compounded by the government's BOP-restriction argument, effectively forecloses an entire category of responsive records from any incarcerated requester in the circuit — a result plainly inconsistent with FOIA's purpose of holding "the governors accountable to the governed." N.L.R.B. v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).

II. The Fifth Circuit Left Intact an Erroneous and Recurring Ruling Applying Exemption 7(C) to Corporate IP Addresses in Direct Conflict with FCC v. AT&T Inc., Applied Sua Sponte by a Court on Behalf of an Agency That Never Claimed the Exemption.

The second ground for certiorari concerns an error the Fifth Circuit expressly declined to correct. By resolving on the no-creation ground, the panel left intact the district court's ruling applying FOIA Exemption 7(C) to corporate IP addresses — a ruling that conflicts with this Court's unanimous precedent, was entered on a basis the agency itself disavowed, and now stands as an unreversed precedent affecting future requesters throughout the circuit.

A. FCC v. AT&T Inc. Categorically Forecloses Exemption 7(C) as Applied to Corporate IP Addresses

In FCC v. AT&T Inc., 562 U.S. 397 (2011), this Court unanimously held that FOIA Exemption 7(C)'s "personal privacy" protection does not extend to corporations. The Court reasoned that "personal" modifies "privacy" in a way that refers to individuals, not legal entities. Id. at 409-10. The holding is categorical: "the protection in FOIA against disclosure of law enforcement information on the grounds that it would constitute an unwarranted invasion of personal privacy does not extend to corporations." Id. at 409.

The IP addresses at issue here belong to corporations, not individuals. The address 65.55.90.200 belongs to Microsoft Corporation (hotmail.com). The address 151.110.126.183 belongs to Eaton Corporation (etn.com). These facts are established in the record by paragraph 13 of the FBI's own criminal complaint affidavit. App. 40. Under FCC v. AT&T Inc., Exemption 7(C)'s personal privacy protection categorically does not apply to these corporate server addresses. No balancing of interests is required — the exemption is inapplicable as a matter of law.

B. Three Compounding Errors Warrant This Court's Review

First, the FBI never claimed Exemption 7(C) as a basis for withholding the header information. The FBI's explicit position was that the header metadata was not a FOIA record at all — not that any exemption covered it. The FBI's own response brief stated: "The FBI was not required to apply a FOIA exemption to the header information because the FBI was not withholding the header information pursuant to a FOIA exemption. This is because the metadata for the header information did not constitute a record for purposes of FOIA." Appellee Br. at 6-7. FOIA places the burden squarely on the agency to claim and justify exemptions. 5 U.S.C. § 552(a)(4)(B). A court may not carry that burden for the agency. The Magistrate Judge applied Exemptions 6 and 7(C) to the header information sua sponte — asserting Exemptions the agency itself had explicitly disavowed — and the district court adopted that approach without comment. App. 12-13 & 21-25.

Second, the Magistrate Judge's sua sponte application of Exemption 7(C) to the corporate IP addresses did not address, or even cite, FCC v. AT&T Inc. The court applied a personal privacy exemption to server addresses belonging to Microsoft Corporation and Eaton Corporation without engaging the controlling authority that categorically forecloses that result. The district court adopted the recommendation, and the Fifth Circuit resolved the case on other grounds, leaving this error uncorrected.

Third, the Fifth Circuit expressly declined to reach the exemption questions, leaving intact the district court ruling without appellate review. App. 9 n.3. The result is an unreversed district court determination — entered on behalf of an agency that never sought it, without engaging this Court's unanimous precedent — that is now available as authority for future courts and agencies.

C. The Uncorrected Ruling Threatens Recurring Harm

The district court's ruling carries forward-looking significance beyond this case. Future FOIA requesters in the Eastern District of Texas seeking corporate IP addresses from law enforcement files now face a district court precedent permitting withholding under Exemption 7(C). Courts in other districts may cite it. The Fifth Circuit's resolution on an alternative ground immunized this error from correction in the one case where it was squarely presented.

The recurring danger is real. Federal criminal investigations routinely involve email communications routed through corporate servers — Microsoft, Google, Amazon, and countless others. The IP addresses associated with those servers belong to corporations, not individuals. Under FCC v. AT&T Inc., Exemption 7(C) is categorically inapplicable to them. But the unreversed district court ruling creates a path for agencies to obtain judicial protection for corporate IP addresses through courts acting sua sponte — without the agency claiming the exemption, without meeting the statutory burden, and without engaging this Court's unanimous precedent. This precisely inverts FOIA's scheme: the agency need not justify its withholding if the court will do so on the agency's behalf.

The binding-component doctrine's logic does not stop at the email's visible content, Center for Public Integrity v. United States Dep't of Energy, 287 F. Supp. 3d 50, 68 (D.D.C. 2018); ACLU v. CIA, 710 F.3d 422, 429 n.7 (D.C. Cir. 2013); Marino v. DEA, 685 F.3d 1076, 1082 (D.C. Cir. 2012); Dean v. United States DOJ, 87 F. Supp. 3d 318, 321 n.3 (D.D.C. 2015) — applied by the Fifth Circuit to moot the "To" line claim based on the EOUSA's unredacted release, App. 7 — should have required the court to address the same doctrine's application to the electronic file and the header metadata. Once the EOUSA released the underlying email without asserting any exemption, the government's ability to claim Exemption 7(C) for embedded components of the electronic record requires re-examination. A doctrine sufficient to moot the "To" line claim should be equally applicable to embedded components of the same file. The Fifth Circuit did not address this question. Neither did any court below.

Additionally, the Department of Justice's own Office of Information Policy determined that the EOUSA's operative response date was November 23, 2021 — before the FBI withheld anything, before Petitioner filed his complaint, and before any judgment. App. 47. The FBI cannot simultaneously assert, as a component of the DOJ, that exemptions shield corporate IP addresses while its parent agency's OIP has determined the underlying email was publicly available more than four months before any complaint was filed.

This Court should grant certiorari to confirm that FCC v. AT&T Inc.'s prohibition on applying personal privacy exemptions to corporations encompasses corporate server IP addresses; that courts may not apply exemptions agencies have not claimed; and that the sua sponte application of an exemption — without the agency's invocation, without engaging controlling authority, and in direct conflict with that authority — is inconsistent with FOIA's burden-allocation framework, and that the binding-component doctrine precludes exemption claims for embedded components of an electronic record once the record itself has been publicly released.

III. The Court Decided This Case Without Petitioner's Timely Reply Brief and Failed to Notify Petitioner of the Rejection Despite Having His Address and Actively Corresponding with the Government.

A third, independent ground arises from two failures that together prevented Petitioner from having any meaningful opportunity to respond once his timely-filed brief was erroneously rejected.

A. The Reply Brief Was Timely Under Houston v. Lack

In Houston v. Lack, 487 U.S. 266 (1988), this Court held that a pro se prisoner's filing is deemed filed on the date the prisoner delivers it to prison authorities for mailing. The rule exists because incarcerated litigants have no control over institutional mail systems, cannot hand-deliver filings, and cannot track or resend submissions. Id. at 270-72.

The government filed its response brief on September 10, 2025. The 21-day reply deadline under Fed. R. App. P. 31(a)(1) was October 1, 2025. Petitioner deposited his reply brief in FCC Pollock's institutional mail system on September 29, 2025 — two days before the deadline. His certificate of service establishes this date under penalty of perjury. App. 30. Petitioner was still incarcerated at FCC Pollock on September 29; he was not released until October 21, 2025. Under Houston v. Lack, September 29 is the filing date. The brief was timely.

The clerk's office applied a receipt-based rather than deposit-based rule, rejected the brief on October 16, 2025, and sent a rejection letter to Petitioner at FCC Pollock — five days before his release. The clerk did not apply Houston v. Lack.

B. The Court's Failure to Notify Petitioner Compounded the Error into a Structural Denial

The rejection alone was error. What followed transformed it into a structural denial of the opportunity to be heard.

On October 21, 2025, Petitioner was released to Oriana House in Cleveland. He mailed address-change notices to both courts in late October. The district court docketed his notice on November 3, 2025. App. 37-38. The Fifth Circuit obtained his Oriana House address — evidenced by correspondence addressed to him there (App. 39) and the carbon copy of the February 3, 2026 clerk's letter (App. 40).

On February 3, 2026, the Fifth Circuit clerk sent AUSA Gillingham a letter directing him to file six paper copies of the government's brief within five days, and carbon-copied that letter to "Mr. Michael A. Hagar." App. 40. The court took affirmative steps to ensure the government's record was complete — sending a reminder letter to experienced federal prosecutors about paper-copy requirements — while making no corresponding effort to notify Petitioner that his timely-filed brief had been rejected due to a misapplication of the prison mailbox rule.

The asymmetry is stark. The government, represented by experienced federal prosecutors with full access to the docket, received affirmative assistance from the court to keep its filings in order. Petitioner, a pro se litigant who had diligently filed within the deadline, updated his address, and remained reachable — received nothing. He never received the February 3 letter. The first communication about this appeal he received after his release was the opinion itself on March 26, 2026. By then, the window for any curative motion had closed. He had no notice, at any point, that his reply brief had been rejected.

C. The Rejected Brief Contained the Fully Developed Versions of Petitioner's Strongest Arguments

The panel decided the appeal without the brief that contained the most fully developed versions of Petitioner's arguments. The rejected reply brief contained: the complete FRA framework showing the FBI possesses the header metadata by operation of law, with reference to the NARA regulations defining electronic records and embedded metadata; the direct citation to Center for Investigative Reporting identifying the Ninth Circuit conflict; the argument that the FBI forfeited its no-creation defense by failing to object to the Magistrate Judge's sua sponte application of exemptions; the waiver argument arising from the FBI's explicit admission that it had not claimed any exemption for the header; the designee argument under Sample v. Bureau of Prisons establishing that the BOP restriction does not extinguish Petitioner's FOIA rights; and the detailed § 552(a)(3)(B) readily-reproducible analysis. None of these arguments were before the panel.

This Court should grant certiorari and direct the Fifth Circuit to accept the reply brief as timely filed under Houston v. Lack and reconsider the appeal with that brief in the record. In the alternative, this Court should address all three questions on the merits, as they are pure questions of law on an undisputed factual record requiring no further development below.

IV. The Questions Presented Are Important, Recurring, and Appropriate for This Court's Resolution.

Each question is of national significance and presents a clean vehicle for resolution.

The no-creation question affects the entire landscape of FOIA access to electronic records. Government agencies operate on electronic platforms that embed metadata within files rather than maintaining it separately. Email header data, document version histories, embedded GPS coordinates, transmission logs, and audit trails are all routinely embedded in records agencies possess and are required by the FRA and NARA regulations to maintain. Under 36 C.F.R. § 1236.2, all such data constitutes "embedded metadata" — textual components that exist alongside the content within the file. The Fifth Circuit's rule — that any extraction step constitutes creation — provides agencies across the circuit a broad, low-threshold tool to withhold embedded electronic information regardless of how readily accessible that information is. The Ninth Circuit conflict means a FOIA requester in California gets what a requester in Texas does not, from the same agency, for identical information. This Court's resolution is necessary to restore uniformity to a federal transparency statute enacted to hold "the governors accountable to the governed." N.L.R.B. v. Robbins Tire & Rubber Co., 437 U.S. 214, 242 (1978).

The incarcerated-requester dimension adds urgency. The Fifth Circuit's rule, combined with the government's BOP-restriction argument — neither of which was corrected below — creates a systematic barrier under which incarcerated persons cannot obtain embedded electronic records from agencies in the Fifth Circuit, regardless of whether those records could be produced to a designee under Sample v. BOP. Thousands of incarcerated persons file FOIA requests each year. This structural barrier operates silently and categorically, foreclosing an entire class of records without the agency ever claiming an exemption or meeting any statutory burden.

The FCC v. AT&T Inc. question recurs wherever government investigations involve corporate email infrastructure — which is to say, virtually every federal investigation involving electronic communications. Commercial email platforms route all messages through corporate servers. IP addresses associated with those servers belong to those corporations. FCC v. AT&T Inc.'s categorical holding should foreclose Exemption 7(C) for all such addresses. But the uncorrected district court ruling, reached without engaging that holding and on behalf of an agency that never invoked the exemption, creates a precedent that future requesters will face. This Court's confirmation that FCC v. AT&T Inc. applies to corporate IP addresses and that courts cannot apply exemptions on agencies' behalf would resolve recurring confusion at the district court level throughout the circuit.

The mailbox rule question affects every incarcerated pro se litigant in the federal courts. The faithful application of Houston v. Lack to every filing, at every stage, by every clerk's office is essential to ensuring that incarcerated individuals can meaningfully participate in federal proceedings. This case presents the additional dimension that the court had the petitioner's address, was actively administering the appeal, ensured the government's filings were complete — and took no step to notify him that his timely-filed brief had been rejected. This Court's supervisory authority over the uniform application of its own precedents warrants review.

The case presents a clean vehicle. The facts are undisputed. The FBI possessed the complete Outlook file, including header metadata, from June 7, 2016. Petitioner's FOIA request described that specific file. The FBI confirmed the file is a Microsoft Outlook file on a jump drive. NARA regulations define the header as embedded metadata existing within the file. The IP addresses in the header belong to Microsoft Corporation and Eaton Corporation. The FBI never claimed any exemption for the header. The Magistrate Judge applied the exemption sua sponte without engaging FCC v. AT&T Inc. Petitioner deposited his reply brief on September 29, 2025, while incarcerated at FCC Pollock. The clerk rejected the brief without applying Houston v. Lack. Petitioner filed an address-change notice in late October 2025; the district court received it November 3, 2025. The court corresponded with the government in February 2026 without notifying Petitioner. Petitioner received only the final opinion. The legal questions are pure questions of statutory interpretation and application of this Court's precedents.

CONCLUSION

The Fifth Circuit's decision conflicts with the Ninth Circuit on a recurring and important question of FOIA law, leaves intact an erroneous district court ruling applying a personal privacy exemption to corporate entities in direct conflict with this Court's unanimous decision in FCC v. AT&T Inc., creates a structural barrier to FOIA access for incarcerated requesters throughout the circuit by foreclosing an entire category of embedded electronic records without any agency exemption claim; and was rendered without Petitioner's timely-filed reply brief due to the clerk's erroneous failure to apply Houston v. Lack — compounded by the court's failure to notify Petitioner of the rejection despite actively administering the appeal and corresponding with the government at the same time. Any one of these grounds independently warrants this Court's review. Together they require it.

The petition for a writ of certiorari should be granted.

Respectfully submitted,

Michael A. Hagar

Michael A. Hagar
Oriana House, Inc.
Cleveland, Ohio
1829 East 55th Street
Cleveland, OH 44103