

★ ★ ★
DC GOVERNMENT

ELECTRONIC RECORDS, TEXT MESSAGES, AND AI: MODERN FOIA CHALLENGES

TRAINING FOR FOIA OFFICERS
& AGENCY DIRECTORS



RECORDS
MATTER



COMMUNICATIONS
ARE RECORDS



AI CREATES
NEW RISKS



TRANSPARENCY
BUILDS TRUST



FOR FOIA OFFICERS
& AGENCY LEADERSHIP

Director Niquelle Allen
August 7, 2026

INFORM.
PRESERVE.
DISCLOSE.
SERVE.

AGENDA



Defining Electronic Records



Text Messages & Personal Devices



Messaging Platforms & Retention



AI-Generated Records



AI Risks



AI Litigation

Agency Practices are evolving faster than Public records laws.

Key themes:

- Mobile-first communications
- Hybrid work environments
- AI-assisted workflows
- Public distrust and transparency expectations
- Litigation and reputational risk



WHY THIS
MATTERS

WHAT COUNTS AS A
“RECORD”?

DC CODE DEFINITION OF A RECORD

- D.C. FOIA is title II of the District of Columbia Administrative Procedure Act (“D.C. APA”), but incorporates certain global definitions from Title I of the D.C.APA, including that of “public record.”
- For purposes of D.C. FOIA, “[t]he term ‘public record’ includes all . . . documentary materials, *regardless of physical form or characteristics*[,] prepared, owned, used, in the possession of, or retained by a public body. *Public records include information stored in an electronic format.*”

CONTENT
MATTERS MORE
THAN FORMAT

Potential electronic records include:

Emails

Text messages

Teams chats

Slack messages

Shared documents

Calendar entries

AI-generated drafts

Metadata

DC FOIA FRAMEWORK

Key concepts:

Broad presumption of disclosure

Technology-neutral definitions

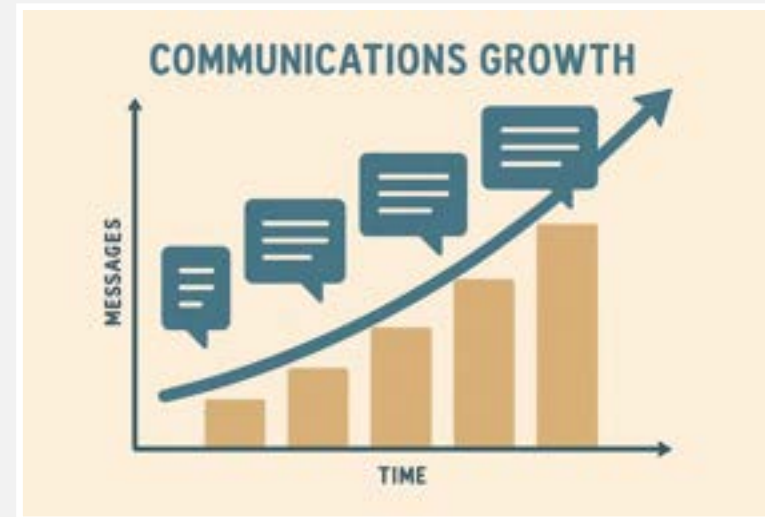
Retention obligations

Agency control and possession

ELECTRONIC RECORDS EXPLOSION

Modern government agencies generate:

- Thousands of emails daily
- Continuous Teams chats
- Text-based workflows
- Shared cloud documents
- AI-assisted outputs



- New and emerging technologies have become a routine method of conducting government business.
- Government employees are no longer communicating only through memoranda, letters, and official email. They are also using SMS messages, multimedia messages, WhatsApp, Signal, Facebook Messenger, Microsoft Teams, and other third-party applications.
- If government business is moved from an official email system to a personal cellphone or new application, does the public's right of access depend on the technology selected by the government employee? NO
- Public access cannot turn on whether a DC Gov employee chooses email, text messaging, or a third-party application.



THE PERCEIVED NEW TECHNOLOGY PROBLEM

TEXT MESSAGES & PERSONAL DEVICES

If government business is discussed the platform may not matter.





PUBLIC RECORD?

ARE TEXT MESSAGES PUBLIC RECORDS?

- Key question: Was the message created or retained in connection with public business?

Potential sources of records:

- SMS
- iMessage
- WhatsApp
- Signal
- Group chats

CASE LAW SUPPORTING TEXT MESSAGES ARE PUBLIC RECORDS

- Under federal FOIA, a record may exist in any format, including an electronic format. 5 U.S.C. § 552(f)(2)
- In *Citizens for Responsibility and Ethics in Washington v. Department of Justice*, the federal court treated a text-message conversation as a record and emphasized the importance of preserving the context of the conversation rather than viewing each individual message in isolation. *Citizens for Resp. & Ethics in Wash. v. U.S. Dep't of Just.*, No. 18-cv-0007 (TSC), 2020 WL 2735570, at *3–5 (D.D.C. May 26, 2020).
- In *Flagg v. City of Detroit*, a federal court applying Michigan law concluded that text messages exchanged by city officials in the performance of official functions could be public records. *Flagg v. City of Detroit*, 252 F.R.D. 346, 355 (E.D. Mich. 2008)
- In *Nissen v. Pierce County*, the Washington Supreme Court held that work-related text messages could be public records even when they were stored on a public employee's personal telephone. *Nissen v. Pierce County*, 357 P.3d 45, 53, 55–56 (Wash. 2015)
- Similarly, in *Toensing v. Attorney General of Vermont*, the Vermont Supreme Court concluded that public records stored in private accounts remained subject to the state's public-records law. *Toensing v. Attorney General of Vermont*, 178 A.3d 1000, 1004, 1009–13 (Vt. 2017).

Although these authorities are not binding interpretations of D.C. FOIA, they reinforce the same principle: government officials cannot place the public's business beyond public access merely by moving it to an electronic device, including private equipment or private accounts.

RISK: PERSONAL PHONES USED FOR GOVERNMENT BUSINESS

Legal concerns:

- Agency custody/control
- Preservation obligations
- Discovery risks
- Employee privacy conflicts



RISK: SIGNAL, SLACK & TEAMS CHALLENGES

Issues include:

Auto-delete functions

Informal communication culture

Ephemeral messaging

Fragmented retention systems

AUTO-DELETION RISKS

Auto-delete settings may conflict with:

- (1) Records retention laws;
- (2) Litigation holds; and
- (3) FOIA preservation duties.



MESSAGES: WHAT IS AND WHAT IS NOT A PUBLIC RECORD

<u>Message</u>	<u>D.C. FOIA treatment</u>
Text discussing an agency decision, program, contract, investigation, meeting, personnel action, or other official matter	Public record
Government-business text on a personal phone	Public record
Government-business WhatsApp, Signal, Teams, or direct message	Potential public record
Purely personal conversation unrelated to District business on a personal device	Not a government public record
Personal content stored on a government device	May be within District custody, but could be nonresponsive or protected by the privacy exemption
Government-business text containing exempt information	Public record, but exempt portions may be redacted or withheld

WHEN DO
TEXT
MESSAGES
BECOME
RECORDS?

Hypothetical:
Senior official coordinates policy decisions through text messages on her personal phone. She has deleted some of the messages. What should the FOIA Officer do when the agency received a request for those messages?

WHEN DO TEXT MESSAGES BECOME RECORDS?

If a D.C. employee or official texts about District business, the message is potentially subject to D.C. FOIA even when sent from a personal phone. The agency must search for it, review it, release the nonexempt material, and justify any redactions or withholding.

HELP TO ANSWER WHEN TEXT MESSAGES BECOME RECORDS

GOVERNING RULE:

Whether information is a Government Record is content-based, not device-based.

A text about District business can be a public record even on a personal phone, while a purely personal text is not made public merely because a government employee sent it.

Government officials should be advised of their record retention obligations when conducting government business via text messages on government and private devices.

EMPLOYEE'S PERSONAL DEVICE:

The agency ordinarily should not seize or indiscriminately search an employee's entire personal phone.

Where there is reason to believe responsive government-business texts are on a personal device, the FOIA Officer should direct the employee to

- Conduct a good-faith search using the relevant names, dates, and search terms;
- Provide the responsive government records to the agency.

The statutory obligation is to conduct a reasonable electronic search. The FOIA Officer should provide a declaration or affirmation describing the search that meets this standard.

WHAT THE FOIA STATUE SAYS

D.C. FOIA does not expressly list “text messages.” Instead, it uses a technology-neutral definition. Under [D.C. Code §§ 2-539\(a\)\(10\) and 2-502\(18\)](#), a “public record” includes:

“documentary materials, regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body.”

The statute expressly adds: “Public records include information stored in an electronic format.”

HOW D.C. FOIA LAW APPLIES TO TEXT MESSAGES

In a formal 2022 advisory opinion, the Office of Open Government concluded that:

- A text created, received, or used by a District official or employee within the scope of government employment is a public record.
- The result does not change because the message is stored on a personally owned phone.
- Government personnel cannot avoid FOIA by conducting government business through private devices or private messaging accounts.
- SMS, MMS, WhatsApp, Signal, instant messages, direct messages, and similar platforms can all generate public records.

https://www.open-dc.gov/FOIA_AdvisoryOpinion_TextMessages

PRACTICAL GUIDANCE FOR FOIA OFFICERS

When a FOIA request may encompass text messages, the FOIA officer should begin by identifying the likely custodians of the records. Ask whether those individuals used:

- District-issued cellphones;
- Personal cellphones;
- Microsoft Teams or another internal messaging platform;
- WhatsApp, Signal, or another third-party application;
- Personal email or cloud accounts; or
- Any application with an automatic-deletion feature.

The FOIA officer should coordinate with the agency's Office of General Counsel, records management officer, and information-technology personnel.

Search instructions should be documented. Employees should be told not to delete potentially responsive messages, and the agency should maintain records of who searched, what was searched, what search terms were used, and what results were produced.

The agency should preserve enough of the conversation to provide context. After collection, the FOIA officer should determine responsiveness, apply any lawful exemptions, redact protected information, and release all reasonably segregable nonexempt portions.

Most importantly, the agency should not assume that a search of official email accounts constitutes a complete search when there is reason to believe that government business was conducted through text messaging.

RECORDS RETENTION RESPONSIBILITIES

D.C. FOIA and the Public Records Management Act perform different but related functions.

D.C. FOIA governs public access to existing records.

The Public Records Management Act governs how government records must be maintained, preserved, and lawfully disposed of.

D.C. FOIA does not require every government record to be retained permanently. The applicable records-retention schedule determines how long a particular category of record must be kept.

However, records cannot be destroyed merely because they may later become the subject of a FOIA request. Destruction must be authorized by an applicable retention schedule or other lawful records-disposition authority.

Once an agency receives a FOIA request—or reasonably anticipates litigation, an investigation, an audit, or another preservation obligation—it must ensure that potentially responsive records are not destroyed while the matter remains pending.

RECORDS RETENTION RESPONSIBILITIES

For Records Retention, here are the Questions agencies should answer:

- What platforms are approved?
 - Who preserves records?
 - How are chats archived?
 - What happens after employee departure?
- The Public Records Management Act independently provides that records documenting public business are public records regardless of the medium. [D.C. Code § 2-1701\(13\)](#). It also provides that records created or received in the course of official business are District property and cannot be destroyed except as authorized by law or an approved retention schedule. [D.C. Code § 2-1706](#).

The District has since modernized its records-retention guidance.

The Office of Public Records' General Records Schedule 20, updated August 1, 2024, now expressly covers electronic correspondence, including email, text messages, chat messages, Microsoft Teams messages, and attachments that qualify as District records.

The schedule generally provides:

- Permanent retention for qualifying electronic correspondence of senior District officials;
- Seven-year retention for messages of most nonsenior officials, staff, and contractors;
- Three-year retention for messages of designated support or administrative personnel; and
- Shorter retention for properly classified transitory records.

For senior officials, official business conducted through a personal or nonofficial messaging account must be copied or forwarded to an official electronic-messaging account within 20 days.

This development reinforces the opinion's central principle: text messages are not a separate or lesser category of government records. They must be identified, managed, and preserved according to their content and the applicable retention schedule.

LINK: https://os.dc.gov/sites/default/files/dc/sites/os/publication/attachments/GS-20%20Retention%20Schedule_2.pdf



2024 REVISIONS TO RETENTION SCHEDULE TO REFLECT NEW TECHNOLOGIES

AI-GENERATED RECORDS, AI RISKS, & AI LITIGATION

THE EMERGING
LANDSCAPE:
WHY AI IS DIFFERENT

AI prompts

AI-generated reports

Large language model outputs

Risk scores

Predictive recommendations

Training datasets

Bias evaluations

Validation testing

Human review documentation

Model governance records

ARTIFICIAL INTELLIGENCE IS ALREADY TRANSFORMING GOVERNMENT

Artificial intelligence is no longer a future technology. AI is increasingly being used by government agencies to improve efficiency, analyze information, automate routine tasks, and enhance public services.

As AI becomes integrated into government operations, it also creates new challenges for transparency, records management, and public access under the Freedom of Information Act (FOIA).

Many agencies are already experimenting with AI, while others have implemented AI in limited operational areas. FOIA officers may not even realize AI is being used within their agency. As AI adoption expands, FOIA professionals must understand both the opportunities and the legal implications associated with AI-generated information and AI-assisted decision-making.

WHY EVERY FOIA OFFICER NEEDS TO UNDERSTAND AI

- FOIA professionals are uniquely positioned at the intersection of transparency, records management, and technology. They do not need to become AI engineers, but they should understand enough about AI to ask the right questions, evaluate agency practices, and recognize potential legal and operational risks.

THE TECHNOLOGY IS NEW
THE PRINCIPLES ARE NOT

Artificial intelligence changes how government creates and manages information.

D.C. FOIA ensures that government remains accountable for that information.

FOIA-RELATED ARTIFICIAL INTELLIGENCE LITIGATION

There are a few federal FOIA cases yet involving AI.

No DC Specific case, YET...

DEMOCRACY FORWARD V. STATE & HUD (D.D.C. 2025)

- *Democracy Forward Foundation v. State Dept, et. Al.* (Case: 1:25-cv-2020) is a FOIA case alleging these government agencies failed to timely issue determinations or produce responsive records.
- From the Complaint: Plaintiff sought records due to the government's "use of generative AI across the government to eliminate programs, surveil viewpoints of private individuals and federal employees, review and rewrite agency regulations and cancel contracts."
- Requests for AI use in visa evaluation, performance reviews, personnel recommendations
- Records sought: prompts, chats, AI recommendations, emails, notes, memos
- Key legal questions: Are prompts deliberative? Are AI outputs records?

DEMOCRACY FORWARD V. OPM, GSA, HUD, OMB (D.D.C. 2025)

- *Democracy Forward Foundation v. OPM, GSA, HUD, OMB* (Case 1:25-cv-03517) is a FOIA lawsuit filed in the D.C. District Court on October 1, 2025, against several federal agencies regarding their use of artificial intelligence.
- The complaint alleges that the Trump-Vance Administration is pushing a deregulation agenda using artificial intelligence. Plaintiff filed several FOIA requests for records regarding the AI Core issue: Were searches adequate?
- AI records may exist in Copilot, ChatGPT, Claude, Gemini, Teams, Slack
- Searching email only is increasingly unreasonable

ACLU V. NATIONAL SECURITY AGENCY (S.D.N.Y. 2024)

- ACLU sought records on NSA AI governance, civil liberties reviews, bias assessments
- Possible exemptions: Federal FOIA Exemption I (Classified Information), Exemption 3 (Federal Statute other than FOIA), Exemption 5 (Deliberative Process), Exemption 7 (Law Enforcement)
- Litigation examines whether AI governance documents can be withheld

ACLU Complaint: <https://www.aclu.org/documents/nsa-ai-foia-complaint>

EPIC v. National Security Commission on Artificial Intelligence

419 F. Supp. 3d 82 (D.D.C. 2019)

When an AI policy body must answer to FOIA



FOIA coverage turned on what Congress created, not what the Commission studied.

Congress gave the AI Commission governmental form and function

National Security Commission on Artificial Intelligence

A temporary 15-member body charged with reviewing AI advances and national-security needs.

Its reports would carry findings and recommendations for action by Congress and the executive branch.

Location	Executive branch
Status	Independent establishment
Output	Three public reports; classified annexes permitted
Duration	Temporary statutory commission

EPIC sought access before the Commission's recommendations hardened

FEB. 22, 2019

Request to DOD

Commission records, required reports, meeting notice, and access under FOIA and the Federal Advisory Committee Act (FACA).

SEPT. 11, 2019

Request to NSCAI

Records plus contemporaneous access to upcoming Commission and subcomponent meetings.

SEPT. 27, 2019

Suit filed

EPIC sued NSCAI, its chair, and DOD after records and expedited relief were not provided.

The FOIA complaint raised four questions; agency status came first

Agency status

Does FOIA's definition of "agency" reach the Commission?

Deadlines

Did NSCAI comply with FOIA's statutory response requirements?

Expedited processing

Did EPIC qualify for accelerated treatment under FOIA?

Withholding

Did NSCAI improperly withhold responsive agency records?

Agency status turned on two statutory texts

FOIA — 5 U.S.C. § 552(f)(1)

“Agency” includes any executive department, military department, government corporation, government-controlled corporation, or other establishment in the executive branch.

NSCAI's organic statute

Congress established NSCAI “in the executive branch” and said it “shall be considered an independent establishment of the Federal Government” under 5 U.S.C. § 104.

**Congress could
“hardly have been clearer.”**

The Government's narrowing theories did not overcome the enacted text

The Government's position

NSCAI was advisory, did not exercise substantial independent authority, and presented separation-of-powers concerns because most members were congressional appointees.

The court rejected each route as a basis for ignoring unambiguous text.



Functional test

Soucie v. David chiefly protects the President's immediate staff and EOP units whose sole function is to advise and assist.



Constitutional avoidance

The canon cannot displace statutory text unless genuine ambiguity exists.



Appointments concerns

The Commission's constitutional structure was a separate question not before the court.

The court denied dismissal but did not order blanket disclosure

Holding

NSCAI is an “agency” subject to FOIA. The Government's partial motion to dismiss was denied. The opinion did not decide exemptions, segregability, or whether every requested record must be released.

Agency status	YES
Deadline count	Not dismissed
Expedition count	Not dismissed
Withholding	Remained pending

The ruling converted a novel AI commission into an operating FOIA program

First production

NSCAI produced 105 pages in January 2020, including internal email concerning language in its interim report.

Rolling disclosure

Fourteen Commission productions followed through February 2021, alongside DOD productions and agency referrals.

Case closure

After public meetings and thousands of pages of records, the parties resolved the attorney-fee claim in July 2021.

JAN. 2020

2020–2021

JULY 2021

Functional analysis pointed to the same result

Text first; function as confirmation

The court treated the statutory language as dispositive, then explained that the Government would lose under its preferred functional approach too.

The Commission did the kind of governmental evaluative work precedent had treated as agency activity.

Investigates • Evaluates • Recommends

- Reviews advances and receives agency briefings
- Develops findings and recommendations
- Matches Energy Research's functional rationale

Not merely personal presidential staff

- Located outside the White House
- President did not control its functioning
- Reported to both Congress and the President

The court denied dismissal but did not order blanket disclosure

Holding

NSCAI is an “agency” subject to FOIA. The Government's partial motion to dismiss was denied. The opinion did not decide exemptions, segregability, or whether every requested record must be released.

Agency status	YES
Deadline count	Not dismissed
Expedition count	Not dismissed
Withholding	Remained pending

The disclosed records showed why AI-policy process records matter

Drafts + emails

Show how report language, judgments, and public positions evolved.

Working-group files

Agendas, conclusions, status reports, and preliminary recommendations preserve the decision trail.

External briefings

Materials addressed social scoring, surveillance, AI threats, and workplace screening technologies.

Governance records

Best-practices briefings, delegations, organizational files, and ethics disclosures reveal accountability structure.

D.C. lessons: persuasive, not controlling

Different statute; transferable discipline

Federal FOIA's definition governed a federal commission. D.C. FOIA has its own text, coverage, exemptions, procedures, and case law.

The operational questions about authority, custody, retrieval, and public functions remain highly relevant.

What carries over

- Read the enabling law
- Identify the responsible public body
- Test custody, control, and retrievability

What D.C. FOIA adds

- Reasonable efforts to search electronic systems
- Access in requested electronic formats when available
- Contractor records for public functions remain reachable

EPIC v. Department of Justice

320 F. Supp. 3d 110 (D.D.C. 2018) • Appeal No. 18-5307 (D.C. Cir. 2020)

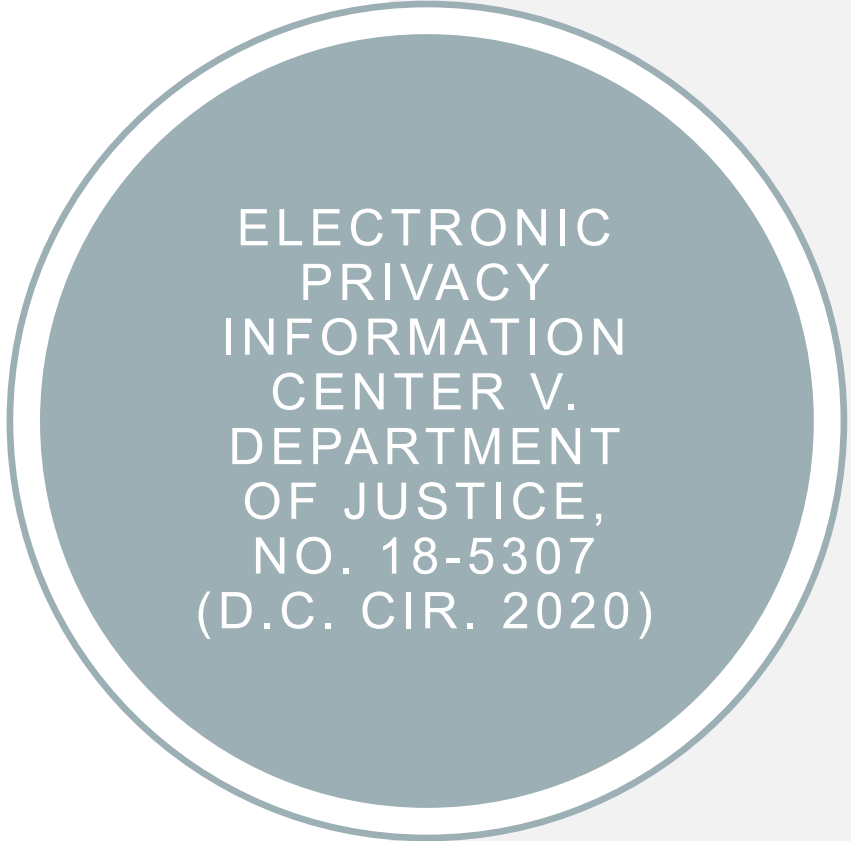
How FOIA exposed DOJ's predictive-policing analysis



Federal FOIA action brought by the Electronic Privacy Information Center ("EPIC") seeking records regarding the Department of Justice's use of algorithmic decision-making in the criminal justice system. The lawsuit arose after DOJ allegedly failed to make a timely determination and failed to produce responsive records following EPIC's FOIA request.

Specifically, EPIC sought records concerning:

- predictive policing;
- evidence-based risk assessment tools;
- sentencing algorithms;
- recidivism prediction models; and
- DOJ policy regarding artificial intelligence and algorithmic criminal justice technologies.



ELECTRONIC
PRIVACY
INFORMATION
CENTER V.
DEPARTMENT
OF JUSTICE,
NO. 18-5307
(D.C. CIR. 2020)

FACTS OF THE CASE

FACTS: Beginning around 2015 - 2016, federal and state governments increasingly relied upon ***statistical algorithms*** to assist criminal justice decision-making.

Examples included: pretrial release recommendations; sentencing recommendations; recidivism predictions; predictive policing; and resource allocation.

FOIA REQUEST FOR INFORMATION ON ALGORITHMS

Civil liberties organizations questioned whether these systems: contained racial bias; lacked transparency; relied upon proprietary software; violated due process; and were scientifically reliable.

To understand DOJ's role in developing these systems, EPIC submitted a FOIA request seeking agency records. DOJ did not provide the requested records within FOIA's statutory deadlines. EPIC therefore filed suit.

ISSUE THE CASE CONSIDERED

Whether DOJ improperly withheld agency records concerning predictive policing and criminal justice algorithms in violation of FOIA.

The Court found DOJ improperly withheld records and the litigation resulted in disclosure of:

- hundreds of pages of DOJ records;
- internal policy documents;
- research regarding predictive policing;
- algorithmic criminal justice materials; and
- the report: **Predictive Analytics in Law Enforcement: A Report by the Department of Justice** (This report reportedly had not previously been made public.)

WHY THE CASE MATTERS

Although this case did not establish a groundbreaking new interpretation of FOIA exemptions, it is significant because it demonstrated that FOIA can be used to obtain records concerning government use of artificial intelligence and algorithmic decision-making. It is one of the earliest cases to consider government use of AI and predictive analytics.

The litigation established that:

- AI-related government records are subject to FOIA like other agency records;
- public interest in algorithmic transparency can justify aggressive pursuit of agency records;
- litigation may be necessary where agencies possess emerging technology records not routinely disclosed; and
- FOIA can uncover previously unknown government reports concerning AI policy.

AI LITIGATION THEMES

- Is the AI output a record?
- Was it retained?
- Did officials rely upon it?
- Is it deliberative?
- Can factual material be segregated?
- Was the search adequate?
- Does contractor possession defeat control?
- Security vs transparency vs trade secrets

PRACTICAL GUIDANCE FOR FOIA OFFICERS

Develop AI governance now

Prompt retention

Record preservation

AI inventories

Validation documents

Procurement records

Human review

Bias testing

Search protocols

Vendor contracts

Employee guidance

LOOKING
AHEAD:
UNRESOLVED
QUESTIONS

- Are prompts agency records?
- Are chats discoverable?
- Must prompt histories be preserved?
- Can the Deliberative Process Exemption cover AI recommendations?
- Are hallucinations responsive records?
- When is AI output adopted as policy?
- Must agencies explain algorithmic reasoning?

KEY TAKEAWAYS:
ADVANCES IN
TECHNOLOGY **DO NOT**
CHANGE FOIA PRINCIPLES

It changes where records exist

It changes how agencies search

It changes preservation methods

It affects exemption analysis

It changes how courts define records



CONTACT INFORMATION

Niquelle M. Allen, Esq.,
Director
Niquelle.Allen@dc.gov
(202) 481-3406

Louis L. Neal, Jr., Esq.,
Chief Counsel
Louis.Neal@dc.gov
(202) 384-2945

Joan Lelma, Esq.
Attorney Advisor
Joan.lelma@dc.gov
(202) 948-3623

Anthony J. Scerbo, Esq.
Attorney Advisor
Anthony.Scerbo1@dc.gov
(202) 731-2926

Brandon W. Lewis, Esq.
Trial Attorney
Brandon.lewis@dc.gov
(202) 579-1043

Kevin Brown
IT Specialist
Kevin.Brown@dc.gov
(202) 579-3756

Kimberly Brown
Paralegal Specialist
Kimberly.brown6@dc.gov
(202) 893-3902

THANK YOU!