

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

JOSEPH KIRCHNER,

Plaintiff,

v.

MIKE JOHNSON, in his individual and official
capacity as Speaker of the United States House of
Representatives;
DONALD J. TRUMP, in his individual capacity as
former and current President of the United States;
PAMELA J. BONDI, in her individual and official
capacity as Attorney General of the United States;
BRENDAN T. CARR, in his individual and
official capacity as Chairman of the Federal
Communications Commission;
THE UNITED STATES HOUSE OF
REPRESENTATIVES;
ANTHROPIC PBC;
OPENAI, INC.;
APPLE INC.;
COMCAST CABLE COMMUNICATIONS, LLC;
METR (MODEL EVALUATION & THREAT
RESEARCH);
and DOES 1-20, unknown co-conspirators,
Defendants.

Case No. 1:25-cv-02735-ACR

**DISCOVERY-5: GENERAL
REQUIREMENTS**

INTRODUCTION

This document is the umbrella protocol governing Plaintiff's expedited discovery in this case. It sets forth:

- Cross-custodian preservation and production obligations
- ESI specifications and native-format requirements
- Privilege-logging protocol
- Redaction protocol for unrelated customer or third-party data
- Deposition scheduling and priority
- Protective-order preconditions

This document is read in conjunction with — and does not displace — the substantive request blocks in DISCOVERY-1 through DISCOVERY-13. The substantive requests control; this document governs mechanics.

A. CUSTODIAN LIST AND PRESERVATION ORDER

All custodians identified below are subject to litigation-hold obligations and must preserve and search for responsive documents. The custodian list is set per-defendant; cross-defendant coordination custodians appear in more than one list.

A.0 PLAINTIFF'S ACCOUNTUUID ROSTER (ANTHROPIC ORGANIZATION "LAWS OF EXISTENCE")

This Section A.0 enumerates the canonical roster of Plaintiff's Anthropic `account\_uuid` values once. Every other discovery document and every other section of this document referring to "Plaintiff's accountUUIDs," "Plaintiff's accountUUID Roster," or "Plaintiff's accounts" refers to the roster set out here. The Roster is established by Exhibit E-39 §H wire-capture roster, Exhibit H-12 §C account-by-account table, and Exhibit H-4 §A0 account inventory.

All five Plaintiff accountUUIDs share the same Anthropic `organization\_uuid` `2e997389-cf99-41ee-8ee3-764442034332` (the operator's `Laws of Existence` organization). Plaintiff owns and operates both email domains (`lawsofexistence.com` and `lawofsupremacism.com`); discovery as to "Plaintiff's accounts" reaches every account ever provisioned on either domain whether or not enumerated below.

#	accountUID D	Email	Notes
1	`08bdec7f-1ed1-48c9-	`joseph@lawsofexistence.com`	Primary testing account during 2026-04-21 → 2026-04-25 wire-capture

	8a93-210eb8052d0e`		window (Exhibit H-4 §A0 row 1)
2	`61343ae3-fd33-403f-897e-6edf3c368c37`	`joseph@lawofsupremacism.com` (also surfaces as `info@lawofsupremacism.com`)	Federal-litigation-active account named in this Court's docket (Appendix P NF-47); subject of the H-12 TTFB-throttle evidence and the wire-capture classifier-firing evidence (Exhibit E-39 §I; Exhibit H-12 §C; Exhibit H-4 §A0 row 2)
3	`e4161cc6-d505-40dc-bbae-10c60276120c`	`contact@lawofsupremacism.com`	Captured during 2026-04-21 → 2026-04-25 testing window (Exhibit H-4 §A0 row 3; Exhibit H-12 §C)
4	`e35353be-f92f-4025-a4e1-222fbd2930ee`	`partnership@lawofsupremacism.com`	Documented at Exhibit E-39 §I OAuth-capture (Session 3); Exhibit H-12 §C account-by-account table
5	`6b6dc58d-7434-463e-a668-c0a613f93d00`	`joseph@lawofsupremacism.com` (separate OAuth session bound to operator's workstation MacBook)	Cross-machine corroboration captured 2026-04-25 (Exhibit H-4 §A0 row 4; preserved at Exhibit H-5 §G `evidence/macbook_workstation_settings_variants/dot_claude_json.json`)

Cross-references that resolve to this Roster: "Plaintiff's accountUUIDs" / "Plaintiff's account identifiers" / "Plaintiff's accounts" / "the operator's accountUUIDs" as those terms appear in DISCOVERY-2 (Anthropic), DISCOVERY-8 (Microsoft), DISCOVERY-9 (Sub-processors), and DISCOVERY-11 (Foreign Influence).

A.1 METR Custodians (See DISCOVERY-1)

1. Paul Christiano (co-founder, METR; trustee, Anthropic Long-Term Benefit Trust; US NIST AI Safety Institute role addressed via DISCOVERY-4 Phase E)

2. Beth Barnes (CEO, METR; prior DeepMind / OpenAI / ARC Evals — produced via Barnes's personal records and METR's institutional possession only, not DeepMind / OpenAI company-side files)
3. All METR officers, directors, and advisory-board members during the relevant period
4. All METR personnel involved in framework development, evaluation conduct, financial administration, or Project Canary coordination

A.1.a TED Foundation Custodians (See DISCOVERY-12)

5. The TED Foundation, Inc. as institutional custodian for Form 990-PF working papers, donor schedules, METR grant disbursements, and Audacious Project records (see DISCOVERY-12)

A.1.b RAND Corporation Custodians (See DISCOVERY-13)

6. RAND Corporation as institutional custodian for non-classified Project Canary governance, RAND-METR coordination, and Project Canary methodology records — narrowly limited to non-classified material; no FFRDC / IC contract production sought (see DISCOVERY-13)

A.2 Anthropic PBC Custodians (See DISCOVERY-2)

1. Dario Amodei (CEO)
2. Daniela Amodei (President)
3. Jared Kaplan (Chief Scientist)
4. Jason Matheny (in relevant capacity)
5. All authors of code referenced in the Leaked Source, including authors of:
`sessionIngress.ts`, `undercover.ts`, `gitBundle.ts`, `datadog.ts`, `claude.ts`, `withRetry.ts`,

`extractMemories` / `autoDream`, any `DANGEROUS\_uncachedSystemPromptSection` site, any `tengu\_`*` flag configuration

6. All reviewers / approvers of the code changes in Item 5
7. All personnel responsible for incident response for inc-3694, inc-4029, inc-4258, inc-4549, inc-4788, inc-4829
8. All participants in Anthropic Slack channel `#briarpatch-cc` during the relevant period
9. All personnel responsible for RSP framework development and amendment
10. All personnel involved in the March 31, 2026 source-code release, including release-engineering, QA, and post-incident review
11. All personnel with responsibility for government relations or regulatory compliance
12. All personnel involved in session-continuity removal (v2.1.20)
13. All personnel involved in October 2025 documentation destruction and partial restoration
14. All personnel involved in post-leak code or policy modifications

A.3 OpenAI, Inc. Custodians (See DISCOVERY-3)

1. Sam Altman (CEO)
2. All personnel involved in Preparedness Framework development (2023 Beta, 2025 v2)
3. All personnel involved in coordination with Anthropic PBC
4. All personnel involved in METR coordination
5. All personnel involved in the Apple-OpenAI partnership integration
6. All personnel responsible for ChatGPT Atlas, ChatGPT Desktop, and ChatGPT iOS engineering

7. All personnel with responsibility for cross-provider fingerprinting or shared-identifier coordination

8. All authors and reviewers of App Store Privacy Nutrition Label filings

A.4 Apple Inc. Custodians (See DISCOVERY-6)

1. Tim Cook (CEO)

2. Craig Federighi (SVP, Software Engineering)

3. Katherine Adams (SVP, General Counsel)

4. All personnel responsible for IDELanguageModelKit and ExternalModelService engineering

5. All personnel responsible for Apple Intelligence engineering and policy

6. All personnel responsible for Floodgate proxy infrastructure

7. All personnel responsible for Biome database and crash-log pipeline

8. All personnel responsible for SmootML analytics

9. All personnel responsible for Messages container retention and deletion semantics

10. All authors of hidden system-prompt instructions injected via IDELanguageModelKit

11. All personnel responsible for certificate-pinning deployment and policy

12. All personnel responsible for the Apple-OpenAI and Apple-Anthropic partnerships

A.5 Government Custodians (See DISCOVERY-4)

1. Mike Johnson (Speaker of the House) — in individual and official capacity

2. Donald J. Trump (President) — in individual capacity

3. Pamela J. Bondi (Attorney General) — in individual and official capacity

4. Brendan T. Carr (Chairman, FCC) — in individual and official capacity

5. United States House of Representatives — institutional custodian

6. Paul Christiano — in his US NIST AI Safety Institute capacity
7. All NIST AI Safety Institute personnel involved in framework evaluation, Christiano conflict management, and US-UK coordination
8. All FCC personnel involved in ISP coordination, content-related enforcement, and complaints regarding ISP RST injection or DNS manipulation
9. All Executive Office personnel involved in inter-agency coordination, AI-project authorization, or communications with any other defendant in this case

4.6 Comcast / Network-Tier Custodians (See DISCOVERY-7)

1. All Comcast Cable Communications, LLC personnel responsible for TR-069 ACS backend operations
2. All Comcast LESRC (Law Enforcement Support Resource Center) personnel
3. All Comcast personnel responsible for JUMPSTART-2 network operations and equipment at injection point `68.85.201.221`
4. All Comcast personnel responsible for peering with Level 3 / Lumen Technologies
5. All Comcast personnel responsible for DNS-over-HTTPS infrastructure (`cloud-doh-ch-az2-prod-16p-877085.sys.comcast.net`)
6. All Level 3 / Lumen Technologies personnel (served as Doe defendant upon identification) responsible for IP `8.40.222.134` and associated backbone injection
7. All VMware, Inc. / Broadcom, Inc. personnel (served as third-party custodian) responsible for the MAC-address allocation `00:0c:29:50:89:f1` and any coordination with Comcast regarding that allocation

A.7 Microsoft Custodians (See DISCOVERY-8)

1. All Microsoft Corporation personnel responsible for `augloop.svc.cloud.microsoft` real-time draft-sync server operations during the March 28, 2026 incident window
2. All Microsoft Azure personnel responsible for Datadog, Inc. and Datadog Israel Ltd. tenant configurations during the relevant period
3. All Microsoft Azure personnel responsible for Apple Inc. tenant configurations and Apple-Intelligence sub-processing through Azure during the relevant period
4. All Microsoft personnel involved in Microsoft-Datadog and Microsoft-Apple contract negotiation, sub-processor disclosure, and per-customer-routing configuration

A.8 Sub-Processor Custodians (See DISCOVERY-9)

1. Datadog, Inc. (and Datadog Israel Ltd.) — sub-processor records under Federal Rule of Civil Procedure 45
2. GrowthBook, Inc. — sub-processor records under Federal Rule of Civil Procedure 45
3. Statsig, Inc. — sub-processor records under Federal Rule of Civil Procedure 45
4. Functional Software, Inc. d/b/a Sentry — sub-processor records under Federal Rule of Civil Procedure 45
5. Cloudflare, Inc. — edge-layer differential-treatment records under Federal Rule of Civil Procedure 45
6. Hound Technology, Inc. d/b/a Honeycomb — distributed-tracing-tenant records under Federal Rule of Civil Procedure 45
7. Twilio Inc. d/b/a Segment — event-stream and downstream-destination records under Federal Rule of Civil Procedure 45

A.9 Federal Contractor Custodians (See DISCOVERY-10)

1. General Services Administration (GSA), Federal Acquisition Service, and Office of Management and Budget — Claude-for-Government partnership records
2. Department of Defense Chief Digital and AI Office (CDAO); DOD Office of Inspector General; House Armed Services and Appropriations Committees — \$800M AI contracts and Section 20005 records
3. Office of the Secretary of the Treasury; Board of Governors of the Federal Reserve System; Financial Stability Oversight Council — Bessent-Powell convocation records

A.10 Foreign-Influence Custodians (See DISCOVERY-11)

1. Datadog Israel Ltd. (Israeli Company ID 516464922) as direct custodian — Israeli-government legal-process records, named-personnel access logs, OzCode patent-family records
2. OzCode Ltd. and Seekret Software Security Ltd. (acquired by Datadog) — pre- and post-acquisition records
3. Elron Ventures Ltd., Rafael Development Corporation Ltd., Rafael Advanced Defense Systems Ltd. — joint-venture, portfolio-company, and customer-relationship records
4. Israel Innovation Authority and Israeli Tax Authority — Sponsored Knowledge grant and tax-treatment records
5. Named Israeli individuals — Omer Raviv (IDF Unit 8200; Datadog Israel Engineering Manager), Alon Mordechai Fliess (Microsoft Regional Director / Azure MVP at OzCode founding), Yair Cohen (Sentra co-founder)

B. PRESERVATION OBLIGATION

B.1 Universal Preservation Notice

Each defendant is on express notice under Federal Rule of Civil Procedure 37(e) of the obligation to preserve electronically stored information (ESI) responsive to the requests in DISCOVERY-1 through DISCOVERY-13. Routine destruction of any responsive category is expressly prohibited pending completion of production.

Each defendant shall:

1. Issue a litigation hold to every custodian identified in Section A above within seven (7) calendar days of service of this document.
2. Provide Plaintiff with a copy of the litigation hold text (with custodian-specific details reasonably redacted for privilege, provided no substantive scope information is removed).
3. Verify litigation-hold compliance by the thirtieth (30th) calendar day of service and quarterly thereafter until production is complete.
4. Suspend automated deletion, retention-expiration, and purge procedures for every category of ESI identified in the defendant's corresponding DISCOVERY document.
5. Preserve all messaging-platform content, including ephemeral-messaging content (Signal, Wickr, Telegram disappearing-message mode) used by custodians for work-related communication.

B.2 Enhanced Preservation for Post-Service Conduct

Each defendant shall preserve, with enhanced care, all records of:

1. Any source-code change, policy change, public statement, or disclosure revision made after the date of service of this discovery.

2. Any rotation, invalidation, or replacement of credentials, tokens, endpoints, or identifiers referenced in the Leaked Source or in any forensic exhibit of record.
3. Any employment termination, leave, or reassignment of a custodian identified in Section A during the period from service through completion of production.

Post-service conduct is directly probative of responsiveness to a court-order obligation and is separately discoverable as an element of Compl., Count X (Consumer Protection / Deceptive Trade Practices) and under Rule 37(e).

B.3 CRITICAL Preservation Categories

The following categories, as identified in the SMF Correlation Matrix's Preservation Priorities section, require immediate and explicit preservation orders:

Custodian	Category
Anthropic	Git history for Leaked-Source-referenced files; session-continuity removal records; post-leak code/policy modifications; `#briarpatch-cc` Slack
Comcast	TR-069 ACS backend logs for Plaintiff's router (Serial `21V4H5FHDA00031`); NSL / FISA records
Government (Bondi)	December 4 2025 memorandum drafting records, including AI-invocation logs

C. PRODUCTION SPECIFICATIONS

C.1 Native Format

All ESI shall be produced in native format wherever feasible, including:

1. Source code in its original file format (TypeScript, `.ts`; JavaScript, `.js`; Python, `.py`; etc.), with Git-tracked files accompanied by `.git` history as specified in per-document requests.
2. Database contents in native format (`.sqlite`, `.db`, `.mdb`, or exportable SQL dump).
3. Network captures in `.pcap` or `.pcapng` format.

4. System logs in native binary format or structured-text format (e.g., macOS `.tracev3`, Linux journal binary, Windows `.evtx`), not as rendered text extracts.
5. Messaging-platform content with complete metadata (sender, receiver, timestamp, edit history, reactions, attachments, thread context).
6. Office documents in native format with every embedded object and revision history preserved.

C.2 De-NIST and Container Handling

Standard NIST-reference file deduplication (de-NISTing) is permitted. Custodian-level deduplication across devices is permitted provided Plaintiff can request per-custodian copies upon request. Container-file contents (`.zip`, `.tar`, `.mbox`) shall be expanded and indexed.

C.3 Metadata Preservation

All produced ESI shall retain original metadata, including:

- File-system metadata (creation, modification, access, size, owner)
- Application-level metadata (author, last editor, revision count, template)
- Email metadata (complete headers including DKIM, routing)
- Source-control metadata (commit SHAs, author/committer, timestamps, signed-off-by)

C.4 Load-File and Index Format

Productions shall include:

- A Concordance-compatible `.DAT` load file or equivalent
- A per-document metadata index including Bates number, custodian, original path, source file, and privilege designation
- An index of Bates ranges mapped to DISCOVERY request numbers

C.5 Encryption

Productions shall be encrypted in transit and at rest. Decryption keys shall be shared via separate channel from the encrypted payload.

D. PRIVILEGE LOGGING

D.1 Privilege Log Requirements

For every document or ESI item withheld on a claim of privilege, the privilege log shall include:

1. Document identifier (Bates stub, internal identifier, or filename)
2. Date of document
3. Author(s) and recipient(s)
4. Privilege asserted (attorney-client, work-product, executive privilege, deliberative-process, state-secrets)
5. Subject matter sufficient for Plaintiff to evaluate the claim (general topic, not a waiver-triggering summary)
6. The specific factual basis for the privilege claim as applied to the document
7. The name of the attorney or agency to whom the privilege belongs

D.2 Categorical Privilege Logs

Categorical privilege logs are permitted for: (a) communications among outside counsel identified in the Certificate of Service; and (b) communications among in-house counsel regarding specifically identified litigation holds. All other privilege claims shall be logged on a document-by-document basis.

D.3 Classified or Controlled-Unclassified Information

For government custodians asserting classification-based withholding, the privilege log shall identify:

1. The classification level
2. The classification authority (Executive Order, statute)
3. The specific authority under which declassification-review procedures apply
4. Plaintiff's willingness to accept in-camera review or to proceed under a CIPA-analog protective procedure

E. REDACTION PROTOCOL

E.1 Permissible Redactions

Redactions for the following are permitted without specific pre-approval, subject to a redaction log:

1. Individual social-security numbers, financial-account numbers, and healthcare identifiers of non-party natural persons
2. Unrelated third-party customer data not responsive to any request in DISCOVERY-1 through DISCOVERY-13
3. Information specifically identified in an effective protective order entered in this case

E.2 Impermissible Redactions

The following categories of redaction are prohibited unless specifically agreed by the parties or ordered by the Court:

1. Redaction of file paths, function names, or identifiers contained in source code

2. Redaction of endpoint URLs, IP addresses, or credentials in telemetry, network-capture, or billing records
3. Redaction of participant identities in Slack, email, and messaging-platform records where the participant is a named custodian
4. Redaction of incident numbers, internal ticket numbers, or document identifiers referenced in the Leaked Source
5. Redaction for "relevance" that is not also covered by a separate, supportable privilege

E.3 Redaction Log

Every redaction shall be logged with: (a) Bates identifier; (b) redaction location within the document; (c) redaction basis; (d) a subject-matter description sufficient for Plaintiff to evaluate the claim.

F. DEPOSITIONS

F.1 Deposition Priority Order

Plaintiff intends to notice depositions upon receipt of initial document production.

Priority order:

1. Rule 30(b)(6) corporate representative of each corporate defendant
2. Custodians with direct knowledge of each defendant's CRITICAL-category preservation items
3. Custodians named in `#briarpatch-cc` participation (Anthropic) and in Bondi Memo drafting (government)
4. Third-party custodians named in per-defendant discovery (Christiano, Barnes, Matheny)
5. Expert witnesses identified in the defendant's Rule 26(a)(2) disclosures

F.2 Deposition Scope

Each deposition will address the DISCOVERY-N Phases within that custodian's scope of knowledge. Plaintiff reserves the right to redepose any custodian upon production of substantial additional material.

F.3 Deposition Logistics

Remote depositions via video conference are permitted for all witnesses. In-person depositions will occur at a location mutually agreed upon, with default District of Columbia for federal custodians and Plaintiff's choice of mutually convenient location for corporate custodians.

G. PROTECTIVE ORDER PRECONDITIONS

G.1 Stipulated Protective Order

Plaintiff and each defendant shall negotiate in good faith a stipulated protective order addressing:

1. Designation levels (CONFIDENTIAL, HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY, SOURCE CODE)
2. Authorized recipients per level
3. Source-code review protocol (secure computer, annotation restrictions, printout controls)
4. Clawback procedure for inadvertently produced privileged material under Fed. R. Evid. 502(d)
5. Destruction or return of materials at conclusion of the case

G.2 Plaintiff's Pro Se Status

As a pro se litigant, Plaintiff will personally review material under designations adequate to permit that review. Source-code review may be conducted on a designated workstation under mutually agreed terms. Plaintiff's retention of a technical consultant or testifying expert under a confidentiality undertaking is permitted without defendant consent.

G.3 No Blanket Designations

Defendants shall not designate entire productions as HIGHLY CONFIDENTIAL without a document-level basis. Over-designation will be challenged under Local Civil Rule 26.2.

H. DISCOVERY DISPUTE RESOLUTION

H.1 Meet-and-Confer

Before filing any motion to compel or motion for protective order, the parties shall meet and confer by video conference within ten (10) calendar days of the dispute's crystallization. Plaintiff will provide a written summary of the dispute in advance of the conference; each defendant shall respond with a written position within three (3) business days.

H.2 Joint Status Conference

Plaintiff reserves the right to request a joint status conference with the Court within thirty (30) days of completion of initial production to address any unresolved production, privilege, or preservation disputes.

I. ROLLING PRODUCTION AND PRODUCTION DEADLINES

I.1 Rolling Production

Rolling production is encouraged and preferred. Defendants shall produce non-privileged responsive material in batches as it becomes available, without waiting for completion of the entire review.

I.2 Production Deadlines

Per-Phase production deadlines are set out in each DISCOVERY-N document. Absent a specific per-Phase deadline, responsive material shall be produced within the following periods:

- **Immediate:** production within 21 days of service (applies to CRITICAL preservation categories and to any request bearing a 14-day Phase deadline)
- **Expedited:** production within 30 days of service (applies to any request bearing a 21-day Phase deadline)
- **Standard:** production within 45 days of service (applies to requests bearing a 30-day Phase deadline)

J. CERTIFICATION

Each defendant's response to each request in DISCOVERY-1 through DISCOVERY-13 shall be accompanied by a certification under Federal Rule of Civil Procedure 26(g) that the response is complete and correct as of the date of the certification. The certification shall identify the responding attorney and shall specifically address the scope of the search performed.

For any request to which the response is "no responsive documents exist," the certification shall identify the search methodology applied and shall affirm under penalty of perjury that no responsive documents exist as of the date of certification.

Respectfully submitted,

/s/ Joseph Kirchner

Joseph Kirchner

Pro Se Plaintiff

4440 Parklawn Avenue #203

Edina, MN 55435

Telephone: (612) 552-2122

Email: legal@lawsofexistence.com

Dated: May 5, 2026

CERTIFICATE OF SERVICE

I hereby certify that on the date shown above, a true and correct copy of the foregoing was served on counsel of record by the Court's CM/ECF electronic filing system. Those who have not appeared will be served by United States certified mail, return receipt requested, same day or on the next business day, at the addresses on file with the Court.

/s/ Joseph Kirchner

Joseph Kirchner

Pro Se Plaintiff