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-8: MICROSOFT CORPORATION (THIRD-PARTY CUSTODIAN)

INTRODUCTION

Microsoft Corporation is served as a third-party custodian under Federal Rule of Civil Procedure 45. Plaintiff is not presently asserting any claim against Microsoft. The records sought are in Microsoft's exclusive possession because they are generated and retained by Microsoft's server-side infrastructure (`augloop.svc.cloud.microsoft`, Outlook telemetry pipelines, and Microsoft 365 diagnostic data service).

The records are material to two distinct categories of Plaintiff's claims:

(i) **Categories A through C** — Plaintiff's First Amendment Petition Clause claim arising from the March 28, 2026 RST-termination of Plaintiff's connections to Microsoft's real-time

draft-sync service during composition of First Amendment-protected correspondence to: (a) Move to Amend's Law and Research Committee concerning *Trump v. Barbara*, Nos. 25-364, 25-365 (U.S.); and (b) Matthew McGuire of the Minnesota Attorney General's office, opposing counsel in *Kirchner v. Ellison*, No. 0:26-cv-00726-PJS-ECW (D. Minn.). Pleading reference: TAC ¶ 108 (Compl. ¶ 110); Exhibit K-1 (redacted Move to Amend correspondence — content of the Petition-Clause communication that was the target of the RST attack); Ex. D-30 at p. 160, l. 7.[1]

(ii) **Category D** — Plaintiff's Counts V (§ 1985(3) Conspiracy), VI (RICO), XII (ECPA), and XIV (CCPA) claims arising from the Datadog / Datadog Israel Ltd. sub-processor architecture pleaded at TAC ¶¶ 5–6, 21, 82–83 (Compl. ¶ 5, Compl. ¶ 6, Compl. ¶ 21, Compl. ¶ 84, Compl. ¶ 85) and at App. P §§ II.B, V.A, V.D. Microsoft Corporation operates Microsoft Azure, on which a portion of Datadog's ingestion infrastructure runs and through which Apple Inc. sub-processes data for Apple Intelligence, IDELanguageModelKit, ExternalModelService, iCloud, and adjacent services. Microsoft holds the Azure-side records of (a) Datadog's Azure tenant configurations and contracts, (b) Apple's Azure sub-processing of Plaintiff's data, and (c) any intersection between Apple's Azure sub-processing and Datadog's Azure ingestion — none of which is in any defendant's exclusive possession.

RELEVANT PERIOD

For Categories A through C (the March 28, 2026 Augloop / Outlook incident), the relevant period is **March 1, 2026 through May 1, 2026**, covering the composition period, the

1 Plaintiff's complete forensic analysis of the March 28, 2026 Microsoft Outlook draft-sync RST attack is preserved at `DDC_EVIDENCE/6_outlook_forensics/`, comprising: incident report (`01_incident_report/`); hex/opcode binary analysis (`02_hx_binary_analysis/`); controlled re-test (`03_controlled_test/`); telemetry-recovery records (`04_tm_recovery/`); diagnostic logs (`05_diagnostic_logs/`); the Move to Amend Outlook email forensics package (`MTA Outlook Email Forensics/`); and SHA-256 manifest (`SHA256SUMS.txt`). Master index at `DDC_EVIDENCE/6_outlook_forensics/INDEX.md`.

incident itself, the immediate remediation window, and subsequent reconnection events material to the forensic analysis.

For Category D (Datadog-Azure infrastructure integration and Apple Inc. sub-processing), the relevant period is **January 1, 2025 through the date of production**, capturing the full Datadog-Anthropic data-flow window and the Apple Intelligence deployment cycle.

PLAINTIFF'S ACCOUNT IDENTIFIERS

For Categories A through C, the Microsoft account-side identifiers for which records are sought include:

- Plaintiff's primary Outlook / Microsoft 365 account associated with email `legal@lawsofexistence.com`
- Any Microsoft 365 account, mailbox, or alias bound to any email address on the domains `lawsofexistence.com` or `lawofsupremacism.com` — both of which are domains owned and operated by Plaintiff and the Laws of Existence LLC organization — including (without limitation) `legal@lawsofexistence.com`, `info@lawofsupremacism.com`, `partnership@lawofsupremacism.com`, `contact@lawofsupremacism.com`, and every other address ever provisioned on either domain
- Any Microsoft account bearing Plaintiff's name "Joseph Kirchner" with a registered mailing address in Edina, Minnesota
- Each such account's Object ID, Tenant ID, and any long-lived device-identity tokens (Windows Hello device identifier, Microsoft Account CID, Azure AD UPN)

For Category D, additional identifiers required for cross-pipeline correlation include:

- Plaintiff's Apple ID(s) and iCloud account identifier(s)
- Plaintiff's Apple hardware device identifiers (UDID, hardware serial numbers, IOPlatformUUID where surfaced)
- All accountUUIDs in Plaintiff's accountUUID Roster (DISCOVERY-5 §A.0)
- Plaintiff's Anthropic-derived `device_id` SHA-256 values (four canonical values): (i) `bc3614c8483b91d9a192d80acc5c38f26d188b1f476950ad0d33050928328a26` (gravity Linux work-station — primary); (ii) `b4ccb1859fd328ded4bea410ea182954d230287fe88b74a8b838ce3bcda10834` (gravity Linux work-station — alternate); (iii) `0fe8f24d334ad40a7cb00d828fabdef7a0400c3f012cfad1d87309732095fe17` (Mac

Mini); and (iv) `f355afa03b7a54118822bdeed397671e524e85c4cd72963264630bf352d4cb09` (MacBook work-station)

• Plaintiff's OpenAI account identifier(s) associated with the email surface listed above

CATEGORY A: AUGLOOP SERVER-SIDE RECORDS

REQUEST NO. 1: Complete server-side logs for `augloop.svc.cloud.microsoft` attributable to Plaintiff's Microsoft account(s) for the relevant period, including:

(a) Every TCP connection, with source IP, source port, connection establishment timestamp, termination timestamp, and termination reason

(b) Every RST, FIN, or error-coded connection closure observed server-side

(c) Every `SettingSyncEditorServiceError` event and analogous diagnostic event

(d) Every draft-content snapshot (pre- and post-change) transmitted to or from Plaintiff's clients

(e) The specific connection events on March 28, 2026 at 07:50:51 UTC and 07:52:34–07:52:37 UTC documented in Plaintiff's client-side capture

REQUEST NO. 2: Complete telemetry records from the Augloop real-time co-authoring service concerning Plaintiff's draft content sessions, including:

(a) Operational-transform ("OT") operation logs

(b) Conflict-resolution records

(c) Content-checksum entries

(d) Any anomaly flags, rate-limit events, or service-side mitigation actions applied to Plaintiff's session

REQUEST NO. 3: Complete logs of any Augloop-side action, mitigation, or inspection performed in response to Plaintiff's March 28, 2026 connections,

including any abuse-detection, malware-detection, or DDoS-mitigation response, together with the authorizing criterion for each.

CATEGORY B: OUTLOOK AND MICROSOFT 365 DIAGNOSTICS

REQUEST NO. 4: Complete Outlook diagnostic logs for Plaintiff's Microsoft account(s) for the period March 27, 2026 through March 30, 2026, including:

(a) All `SettingSyncEditorServiceError` events

(b) All `augloop` and `draft-sync` client-side events transmitted to Microsoft's diagnostic-data service

(c) All Outlook crash reports, ASSERT events, and error reports

(d) All local-cache-corruption events for the user's Drafts folder

REQUEST NO. 5: Complete Microsoft 365 audit-log records for Plaintiff's tenant for the relevant period, including all administrative actions, policy applications, and service-side configuration changes affecting Plaintiff's account.

REQUEST NO. 6: All records of Plaintiff's account receiving conditional-access policy, data-loss-prevention (DLP) policy, or Microsoft Defender for Office 365 action during the relevant period, with for each action: (a) the policy name; (b) the triggering condition; (c) the imposing administrator or automated process identifier; (d) the effect on Plaintiff's ability to compose, save, or transmit draft content.

CATEGORY C: COMMUNICATIONS AND PRESERVATION

REQUEST NO. 7: All communications, law-enforcement requests, National Security Letters, FISA orders, preservation demands, subpoenas, or administrative requests directed to Microsoft concerning Plaintiff's Microsoft account during the relevant period.

REQUEST NO. 8: All communications between Microsoft and Comcast Cable Communications, LLC concerning the `augloop.svc.cloud.microsoft` service, its routing path, or any deep-packet-inspection-based mitigation applied by any carrier to traffic bound for that service.

REQUEST NO. 9: Complete documentation of every preservation hold, litigation hold, or legal hold Microsoft has issued or received concerning Plaintiff's Microsoft account, including the issuing authority, effective date, scope, and any partial or conditional release.

CATEGORY D: DATADOG-AZURE INFRASTRUCTURE INTEGRATION AND APPLE INC. SUB-PROCESSING

REQUEST NO. 10: All records in Microsoft Corporation's possession concerning any Datadog (Datadog, Inc., and Datadog Israel Ltd., Israeli Company ID 516464922) integration with Microsoft Azure during the Category D relevant period (January 1, 2025 through the date of production), including but not limited to Datadog's role as a sub-processor of Apple Inc. data routed through Microsoft Azure infrastructure. Production shall include:

(a) **Datadog's Azure footprint.** Every Azure subscription, tenant, resource group, and region operated by or for the benefit of Datadog, Inc. or Datadog Israel Ltd., with the data-residency, peering, and inter-region replication architecture for each.

(b) **Microsoft–Datadog contractual record.** Every contract, master service agreement, data processing addendum, sub-processor disclosure, side letter, and amendment between Microsoft Corporation and Datadog, Inc. or Datadog Israel Ltd. governing Azure use during the Category D relevant period.

(c) **Apple sub-processing through Azure.** Every contract, sub-processor disclosure, and Azure tenant configuration governing Apple Inc.'s use of Microsoft Azure (including for Apple Intelligence, IDELanguageModelKit, ExternalModelService, iCloud, the Floodgate proxy, and any Xcode-Intelligence-adjacent service); together with every Microsoft–Apple communication addressing per-customer sub-processor disclosure, data-residency commitments, or telemetry-pipeline routing across Azure infrastructure.

(d) **Apple-Datadog intersection on Azure.** Every record showing whether Apple's Azure-routed data flowed through any Datadog ingestion pipeline operating on Microsoft Azure during the Category D relevant period — including any joint Apple-Datadog tenant, any customer of both Apple and Datadog whose data traversed Azure, and any Azure-side audit record of the intersection.

(e) **Plaintiff's data on Azure.** Every record of data attributable to Plaintiff (under the Apple, Anthropic, OpenAI, and Microsoft account and device identifiers enumerated under PLAINTIFF'S ACCOUNT IDENTIFIERS for Category D, supra) that traversed any Datadog-on-Azure or Apple-on-Azure pipeline during the Category D relevant period.

(f) **Israeli-personnel access to Azure-hosted data.** Every Azure-side audit record of Datadog Israel Ltd. personnel access to Apple, Anthropic, or OpenAI customer data routed through Azure, with the access-control posture (read-only, read-write, query-only, model-training-eligible) for each named individual at Datadog Israel Ltd.

(g) **Microsoft–Datadog communications.** All communications between Microsoft Corporation and Datadog, Inc. (or Datadog Israel Ltd.) concerning per-customer routing, per-tenant configuration, Israeli-personnel access, or Israeli-government legal process directed to Datadog's Azure tenant during the Category D relevant period.

Evidentiary predicate: Pleading ¶¶ 5, 6, 21, 82, 83, 108 (Compl. ¶ 5, Compl. ¶ 6, Compl. ¶ 21, Compl. ¶ 84, Compl. ¶ 85, Compl. ¶ 110); App. P, §§ II.B, II.E, V.A, V.D; Ex. E-34, Finding SC-9; Ex. E-35, Finding NF-36; Ex. E-39, Finding NF-47; Ex. F-6 at p. 33, l. 2; Ex. F-16 at p. 72, l. 2; Ex. F-2 at p. 10, l. 2; cross-reference DISCOVERY-6 (Apple), DISCOVERY-9 § A (Datadog), and DISCOVERY-11 §§ A, K (Datadog Israel Ltd. as direct custodian and Israeli intelligence coordination).

PRESERVATION NOTICE

This subpoena serves as express notice under Federal Rule of Civil Procedure 37(e) that Microsoft Corporation is on notice of the preservation obligation. Routine destruction of any category of record identified in this subpoena is expressly prohibited pending completion of production. This includes:

1. All `augloop.svc.cloud.microsoft` server logs for connections from Plaintiff's IP range during the Categories A–C relevant period, notwithstanding any ordinary retention schedule that would shorten the preservation period.

2. All Outlook diagnostic data for Plaintiff's account, including data routed to third-party or successor diagnostic endpoints.

3. All communications with carriers (including Comcast) concerning routing, mitigation, or interception of Augloop traffic.

4. All Azure-side records of Datadog (Datadog, Inc. and Datadog Israel Ltd.) tenant activity during the Category D relevant period, including Datadog tenant configurations, per-tenant audit logs, Datadog-Israel personnel access events to Apple/Anthropic/OpenAI customer data routed through Azure, and Microsoft-Datadog and Microsoft-Apple contracts and sub-processor disclosures.

FORMAT AND MECHANICS

Production format shall comply with Microsoft's standard litigation-response specifications, including encrypted transport and production via Microsoft's compliance portal or an equivalent secure mechanism mutually agreed.

Plaintiff is prepared to meet and confer on scope, form, and cost under Rule 45(d), and will engage a technical consultant under confidentiality undertaking for review of any highly-sensitive production.

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